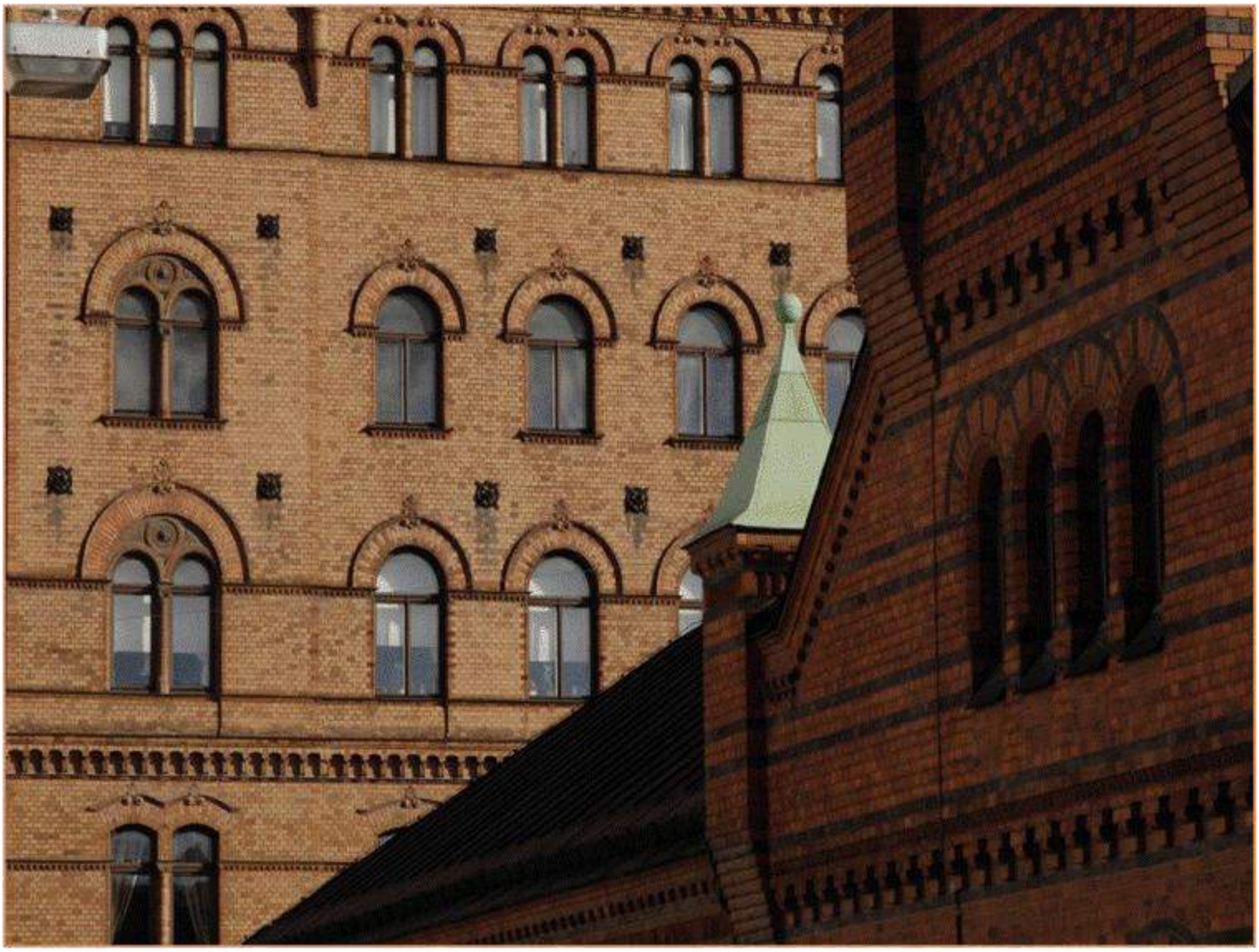
Nepal e-Government Interoperability Framework (NeGIF) - Main Report



pwc

Jan 2011

Document History

Date	Version	Author	Description
November , 2010	Draft	PwC India	Nepal e-Government Interoperability Framework (NeGIF) Main Report - Draft version
January , 2011	Final	PwC India	Nepal e-Government Interoperability Framework (NeGIF) Main Report - Final version

Distribution

Title	No. of Copies
HLCIT: **Primary**: Mr. Juddha B. Gurung **Secondary**: HLCIT to decide	1

1 Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Expansion
ACID	Atomicity, Consistency, Isolation, and Durability
ASCII	American Standard Code for Information Interchange
ADSL	Asymmetric Digital Subscriber Line
AMQP	Advanced Message Queuing Protocol
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Automatic Teller Machine
AVI	Audio Video Interleave
B2B	Business-to-Business
BGP	Border Gateway protocol
BI	Business Intelligence
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
BPR	Business Process Re-Engineering
Cat 6	Category 6 UTP cable
CDB	Common Database
CDMA	Code Division Multi Access
CGM	Computer Graphics Metafile
CoBIT	Control Objectives for Information and related Technology
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off the Shelve
CSS	Cascading Style Sheet
CSV	Comma Separated Values
DBA	Data Base Administrator
DBMS	Data Base Management System
DCCP	Datagram Congestion Control Protocol
DCOM	Distributed Component Object Model
DES	Data Encryption Algorithm
3DES	Triple Data Encryption Algorithm
DHCP	Dynamic Host Configuration Host protocol
DNS	Domain Name Services
DOM	Document Object Model
DRM	Digital Rights Management
DTD	Document Type Definition

Abbreviation	Expansion
EA	Enterprise Architecture
ebXML	E-business XML
ECN	Explicit Congestion Notification
EDI	Electronic Data Interchange
eGIF	e-Government Interoperability Framework
NeGIF	Nepal e-Government Interoperability Framework
NGoT	Nepal Government Thesaurus
HLCIT	High Level Commission for Information Technology
ERD	Entity-Relationship Diagram
EVDO	Evolution Data Optimized
FDDI	Fiber Distributed Data interface
FTP	File Transfer Protocol
FTPS	Secure File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GIF	Graphics Interchange Format
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	Global System for Mobile communications Association
GTP	GPRS Tunneling Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
HSPA	High Speed Packet Access
ICA	International Compliance Association
ICT	Information and Communication Technology
ICMP	Internet Control Message Protocol
IDL	Interface Description Language
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol

Abbreviation	Expansion
IPsec	IP Security Authentication Header
IRC	Inter Relay Chat
ISBN	International Standard Book Number
IS-IS	Intermediate System to Intermediate System
ISO	International Standards Organisation
ISSN	International Standard Serial Number
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JDBC	Java Database Connectivity
JMS	Java Message Service
JPEG	Joint Photographic Experts Group
JVM	Java Virtual Machine
KPI	Key Performance Indicators
LDAP	Lightweight Directory Access Protocol
L2TP	Layer 2 Tunneling Protocol
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
MIX	Metadata for Images in XML
MP-BGP	Multi Protocol-Border Gateway Protocol
MPEG	Moving Picture Experts Group
MPLS	Multi Protocol Label Switching
MPLS-OAM	Multi Protocol Label Switching – Operation Administration and Maintenance
MPLS-TE	Multi Protocol Label Switching -Traffic Engineering
MS	Microsoft
MSAG	Multi Service Access Gateway
MSDP	Multi Source Discovery Protocol
MSMQ	Microsoft Message Queuing
MTA	Message Transfer Agent
NAS	Network –Attached Storage
NDA	Non-Disclosure Agreement
GIDC	Government Information Data Centre
NDP	Neighbor Discovery Protocol
NISO	National Information Standards Organization
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OAI-PMH	Open Archives Initiative - Protocol for Metadata Harvesting
OASIS	Organization for the Advancement of Structured Information Standards

Abbreviation	Expansion
ODBC	Open Database Connectivity
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
OLEDB	Object Linking and Embedding Database
ORB	Object Request Broker
OSPF	Open Shortest Path First
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format
POP	Post Office Protocol
POSIX	Portable Operating System Interface
PPP	Point to Point Protocol
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PST	Personal Storage Table
P3P	Platform for Privacy preferences
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RARP	Reverse Address Resolution Protocol
RDBMS	Relational Data Base Management System
RDF	Resource Description Framework
RFC	Request for Comments
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RPC	Remote Procedure Calls
RSTP	Rapid Spanning Tree protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
RSVP	Resource Reservation protocol
RSVP-TE	Resource Reservation protocol-Traffic Engineering
SAM	Self-service Automated Machine
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCTP	Stream Control Transmission protocol
SCM	Software Configuration Management
SCP	Session Control Protocol

Abbreviation	Expansion
SDLC	Software Development Life Cycle
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
STP	Spanning Tree Protocol
SSH	Secure Shell
SSM	Source Specific Multicast
SVG	Scalable Vector Graphics
S/MIME	Secure/Multipurpose Internet Mail Extensions
TA	Transport Authority
TC	Trust Computing
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
Telnet	Teletype Network
TFTP	Trivial File Transfer Protocol
TIA	Telecommunication Industry Association
TIFF	Tagged Image File Format
UBL	Universal business Language
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling language
UTP	Unshielded Twisted Pair
URN	Uniform Resource Name
VDSL	Video Digital Subscribers Line
VRRP	Virtual Router Redundancy Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAI	Web Access Initiative
WCAG	Web Content Access Guidelines
WCDMA	Wide Band Code Division Multiple Access
WIMAX	Worldwide Interoperability for Microwave Access
WFS	Web Feature Services
WML	Wireless Markup Language

Abbreviation	Expansion
WMS	Web Map Service
WSDL	Web Service Definition Language
WSRP	Web Service for Remote Portlets
WSRM	Web Services Reliable Messaging
WSS	Web Services Security
WS-I	Web Services-Interoperability
W3C	World Wide Web Consortium
XHTML	Extensible Hypertext Markup Language
XMPP	Extensible Messaging and Presence Protocol
XCIL	Extensible Customer Information Language
XLS	Excel Worksheets
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XNAL	Extensible Name and Address Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformation
XTP	Xpress Transport protocol

Structure of the Report

Structure of this report

The report is structured as follows:

Section 1 – Executive summary

This section summarises the background, intent of the project and provides the overview of the proposed Nepal eGIF.

Section 2– Introduction

This section covers the key purpose of e-Governance and how eGIF will help towards better governance. In order to provide a basic understanding, an introduction on eGIF, its importance, key challenges in implementation and its different dimensions are discussed. This section also covers the approach and stages of this eGIF project to understand the set of activities and deliverables (as per the contract) that has helped to draft this report.

Section 3 – Nepal eGIF (NeGIF) Meta Model

The thrust of this report is the design of the Nepal e-Governance Interoperability framework version 1.0 (NeGIF v1.0). This section describes the Meta model (conceptual framework) of Nepal's eGIF which comprises of the scope, purpose, principles, policies, standards, and assumed national enterprise architecture and governance mechanism.

Section 4 – NeGIF Technical Standards

This section provides the definition, structure, importance of standards and the summary of nine technical standard areas identified under NeGIF v1.0 namely Interconnection, Data Integration, Access, Collaboration, Application Design and Development, Application Integration, System Standards, Security, business area specification.

Section 5 – NeGIF Data Standards

For the government data to be truly interoperable defining the standards and rules governing the data and the metadata used across the eGovernance applications and services is very much essential. The Government Data Standards sets out the rationale, approach and rules for setting and agreeing at the set of Government Data Standards (GDS) to be used in the Govt. Data Schemas and other electronic interchanges of data involving the public sector, developed to support the e-GIF

Section 6 - Reference

This contains references to the various source of data/information and literature survey used in writing this report.

1. Executive Summary

1. Executive Summary

1.1 Background & Introduction

Nepal recognises the potential of Information and Communication Technology (ICT) to enhance competitiveness, facilitate economic diversification and increase productivity as well as to improve the efficiency and capability of government institutions. Nepal is working towards a plan of transforming the governance by using ICT for increased citizen participation and attempting to create an open, transparent environment through integration of different government information systems and services.

As part of achieving this end objective, the High Level Commission for Information Technology (HLCIT) has taken up the development and implementation of ICT standards and Preparation of Nepal e-Government Interoperability Framework (NeGIF). HLCIT aims to create an environment which will help government information systems to work together successfully and in an integrated and seamless manner regardless of the underlying technology or application in use, or regardless of which vendor the system or technology has been procured from. Towards this objective HLCIT has developed the first version of the NeGIF. This eGIF would serve the following objectives of HLCIT eGovernment implementations:

- Enable proprietary and open source systems in different Government information systems, both within Government and external to Government, to communicate and inter-operate efficiently and effectively;
- Promote and foster the adoption of open source solutions within the Government, by emphasising the need for openness, transparency and competitiveness for all implementation of information systems;
- Promote and foster the adoption of open standards that enables the exchange of data between applications;
- Promote vendor-neutral and technology-neutral implementations, with the adoption of open standards, for all Government information systems; and
- Reduce the total cost of ownership of Government information systems, with the adoption of open standards.

M/s PricewaterhouseCoopers Pvt Ltd. (PwC) India was entrusted the assignment of developing the NeGIF. This report is the compilation of the various phases of the assignment through consultative process of arriving at the standards to be adopted by HLCIT. The various highlights of the entire report are summarized below:

1.2 Scope and coverage of the report

The scope of the engagement for NeGIF was the following:

- Understand the existing GIF / practises prevailing in Nepal
- Arrive at the current As-Is Scenario
- Conduct a study on the leading eGIF practises
- Identify the Gaps
- Define the NeGIF

Based on the above, the PwC have provided the various detailed deliverables at each phase of the engagement. This report provides in brief the various phases and approach of PwC towards the completion of this engagement and also the first version of the NeGIF proposed to HLCIT. The snapshot of the proposed eGIF is provided below.

1.3 Nepal e-Government Interoperability Framework (NeGIF)

eGIF provides a framework to share, collaborate and integrate information and organisation processes by use of common standards. Increasingly the use of open standards to enable such interoperability is the key for success of any eGIF framework and choosing the right set of technical standards and policies that are suitable to the environment.

To achieve this level of interoperability it requires a holistic approach covering different dimensions of interoperability standards at various levels such as, business process or organizational interoperability, information or semantic interoperability, and technical interoperability.

During the engagement, we have identified the suitable framework for NeGIF. Since Nepal has taken a step towards defining interoperability standard (eGIF) along with EA, the following eGIF Meta Model has been proposed. ***The following diagram represents the NeGIF Meta Model.***

The core of eGIF is the Preamble (covering purpose and scope), Principles, Policies and Standards. Governance and Architecture are aspects that will aid eGIF implementation, interrelationship, management and success.

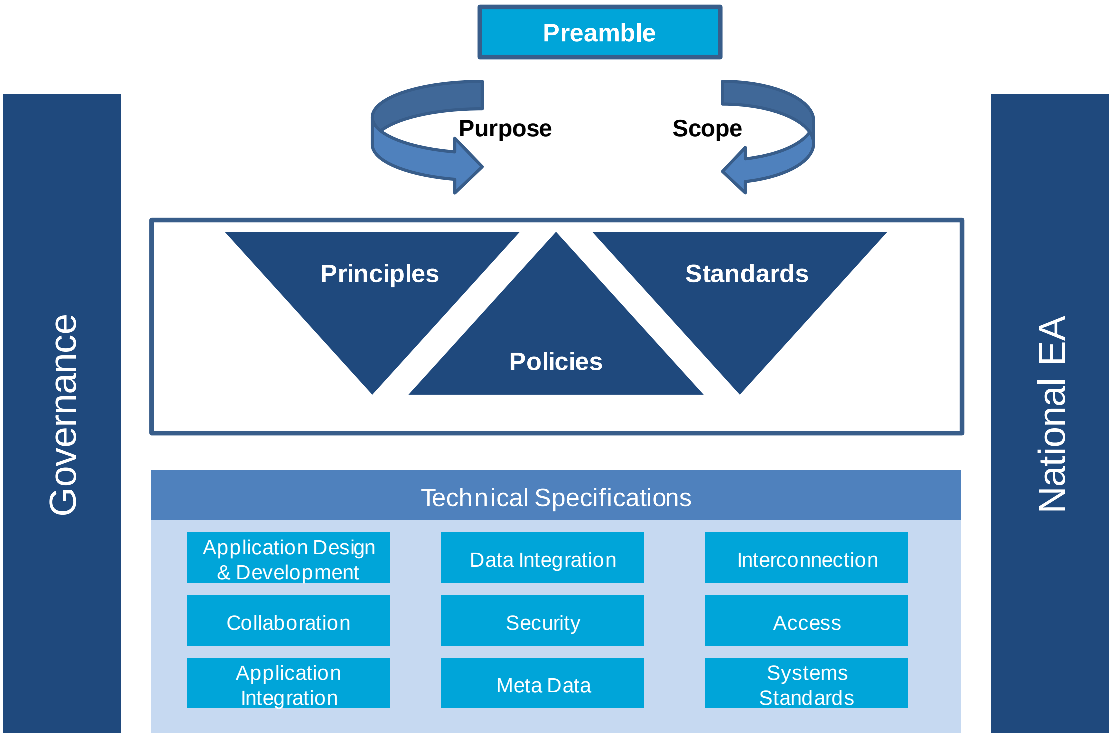


Figure 0-1: NeGIF Meta Model

1.3.1 Guiding Principles & Policies

The key drivers guiding the recommendations of NeGIF are based on the assessment of current environment in Nepal and based on leading practices of various countries. The following key principles have been suggested.

- **Interoperability -** Standards and specifications recommended be relevant to recommended use of OSS applications and the use of open standards for Information Access.
- **Share, Re-Use and Collaborate -**The standards proposed may be shared, reused and collaborative in nature for entire government to use
- **Scalability -** The proposed standards be scalable for future needs as well.
- **Adherence to open standards -** The standards, where available, be recognised and adopted by internationally recognised bodies.

1.3.2 Policies

Policies establish direction and define technical requirements that govern the acquisition, use and management of IT resources. Overall the policies drive successful implementation, maintenance and governance of eGIF.

The success of an e-Government initiative depends on effective enforcement of these policies along with the applicable standards. They ensure that principles on which eGIF are based are achieved and assessed for compliance as well. Policies should apply to all the initiatives of the ministries without any exceptions. The governing body must ensure access to the standards and policies so that ministries and vendors are aware of the policies that need to be enforced.

As a part of the successful implementation of NeGIF, suitable policies have been defined under the below mentioned categories. These policies will guide the NeGIF governance body to ensure adherence and compliance to eGIF.

- Overall Governing Policies
- Application and Technology Policies
- Data and Meta data Policies
- Security Policies
- Data Protection Policies

1.3.3 NeGIF Scope of use and applicability*:*

The various dimensions of NeGIF covered in this report are:

- Business process or organizational interoperability;
- Information or semantic interoperability; and
- Technical interoperability

The NeGIF scope of use and applicability is prescribed to the following categories:

1. Government-to-Government (G2G) - Within Nepal Government i.e. between Government agencies and departments.
2. Government-to-Citizens (G2C) - Between Nepal Government and its citizens.
3. Government-to-Businesses (G2B) - Between Nepal Government and businesses in the private sector, i.e. suppliers and contractors to the Government.
4. Government-to-Employees(G2E) – Between Nepal Government and its govt. employees

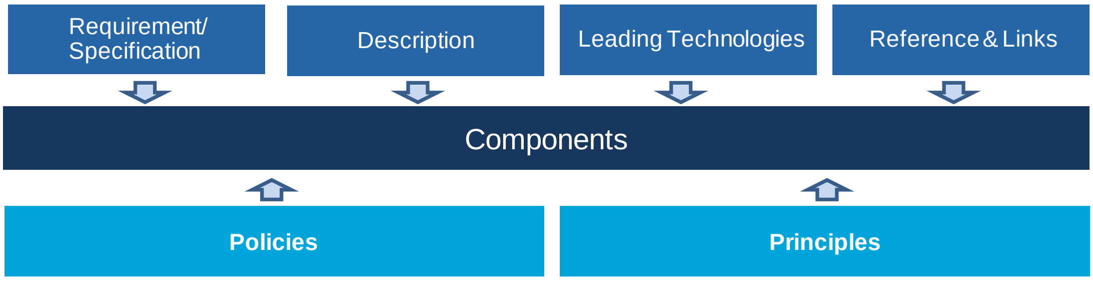
1.3.4 NeGIF Standards Coverage

There are 9 technical standards areas covered under the first version of NeGIF - namely Interconnection, Data Integration, Access, Collaboration, Application Design and Development, Application Integration, System Standards, Meta Data and Security. The 9 areas were identified based on the:

- As-Is assessment wherein the baseline technologies of various ministries / agencies were studied, and the contextual requirements were analysed
- Understanding of maturity level and transformational values of existing and emerging technologies through technology trends by leading analyst, PwC technology research reports etc.
- Best practice review to get an idea of the leading practice industry standards
- Information on Standards organisation such as w3c, Dublin core, ISO etc.

The details of the standards are provided in the subsequent sections of this report.

1.3.5 NeGIF Standards Structure:



F

Figure 0-2: NeGIF Standards Structure

- The defined Policies will act as enforcement guidelines for implementing these standards.
- The standards proposed table will have multiple ‘Components’ and each of the component will have:
  - One or more requirement/specification that needs to be followed to ensure interoperability.
  - These requirement /specification can be mandatory or recommendatory.
  - Based on the baseline information collected during the As-Is phase the status of the standards adoption is indicated, whether the standards are currently Adopted, Partially Adopted or Not Adopted.
  - The standards table briefly represents the standards/requirements/ status and enforcement rules.

1.3.6 Governance Structure:

Success of any eGIF is dependent on the adherence and adoption of the standards by the stakeholders. This is ensured through appropriate governance mechanism. As a part of the engagement PwC has proposed a suitable governance mechanism for NeGIF. The governance structure, roles and responsibilities, process of governance are detailed in the report.

1.4 Implementation plan

The final section of the report defines the various stages for adoption of the eGIF in Nepal. This includes the creation, maintenance and update of the eGIF and life cycle management of the NeGIF. One of the key points to be noted is that NeGIF is a living document of standards and therefore each version of the document has a definitive life time, beyond which the eGIF needs to be updated and enhanced based on the business needs and changing technologies. PwC has proposed a clear Life Cycle Management approach to NeGIF.

2. Introduction

2. Introduction

2.1 e-Governance

e-Governance in simple terms is a mechanism to use/leverage Information and Communication Technologies (ICTs) in the working of the Government. The world has seen a sea change in governance across the globe. Especially in Asia many governments have moved towards eGovernance, where in the role of government to take control has moved towards citizen centric participative governance. This is due to the demand that is already being made and will be made by the citizens with increasing urgency, to directly participate in the governance. e-Governance is a pragmatic way to achieve the above.

The delivery of e-Goverment services involves interaction between actors, citizens, businesses and administrations, in a diverse setting, not only in terms of technology, but also in terms of how the relationships and the processes are organized and of how the necessary data and information are structured and handled. The challenge of eGovernment lies in integrating the various stakeholder needs (automation needs) both at the business level and technology level. Here lies the importance of a common framework, rules and regulations, policies and standards that needs to be adopted for integration between and among the various stakeholders. Such an integration framework is derived by applying some common minimum standards which in technology terms is referred to as **Interoperability Frameworks**.

2.2 What is e-Government Interoperability Framework (eGIF)

Interoperability, like technology, is not an end but a means to an end. eGIF provides a framework to the government to share, collaborate and integrate information and organisation processes by use of common standards.

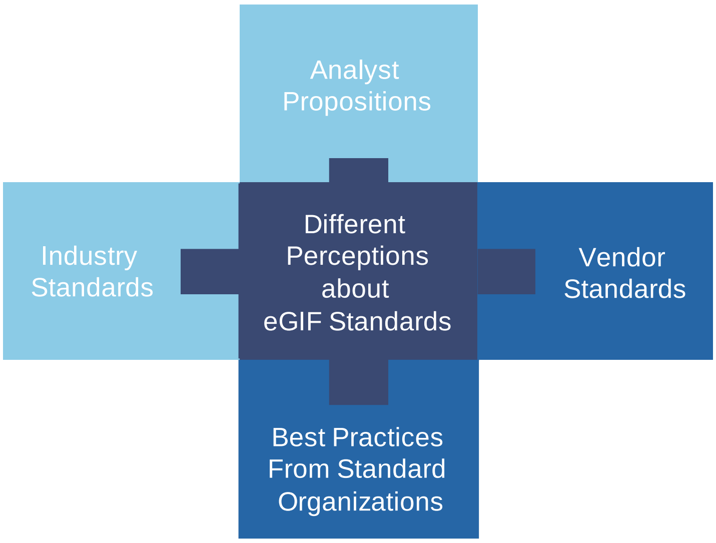

Analyst Propositions
Industry Standards
Different Perceptions about eGIF Standards
Vendor Standards
Best Practices From Standard Organizations

Figure 0-3: eGIF Standards

Source: PwC adapted from external sources eGIF provides the know how to achieve interoperability of data and information within and outside the government. It enables any ministry/agency to provide and receive information and integrate its processes with other agencies using a predetermined framework. Increasingly, the use of open standards to enable such interoperability is emerging to be the key in eGIF frameworks. Many people and bodies (industries, standards organisations, software and hardware vendors, analysts etc.) have different views on standards for ensuring interoperability. The success depends on choosing the right set of technical standards and policies that are suitable to the environment. However technical standards in eGIF alone cannot ensure interoperability. Each organisation's process, collaborative environment, common applications, development of semantics are other key factors to ensure interoperability. An analogy to eGIF is the road /traffic rules. It would be inefficient and cumbersome to adhere and agree to road/traffic rules every time a vehicle encounters another vehicle. Standards like traffic rules will set the base to achieve common understanding and uniformity.

2.3 Benefits of NeGIF

Every government functions by collaborating closely with its departments, regions etc. and the government tries to use technology (e-Governance) to help citizens, government departments and businesses at large to effectively manage information and improve the governance mechanism.

To develop a successful e-Governance requires sound technical integration between government agencies, service providers and other stakeholders/participants. Providing services online to citizens will require substantial collaboration between several agencies at the back-end for it to be delivered effectively.

eGIF will provide the Nepal government the ability to share information and integrate information and business processes by use of common standards.

Over the years the government would have accumulated a lot of data on paper, building complex repositories for everything from personnel details to the holdings of a large museum. Access to these data has been restricted to a select few, with a wall of paperwork and bureaucracy separating them and their data from those who might wish access. For anyone intending to integrate data from different locations, there has often been no alternative than to manually translate and re-key data off printouts from incompatible systems.

Nepal has embarked upon an ambitious program for leveraging ICT for development and for providing public services to citizens/business (e-Government). One of the aims of the e-Government programme is to integrate various departments in the government, in order that citizens/businesses deal with one face of the government rather than individual departments/agencies for availing services. This is possible to achieve given the power of ICT. However, this does require making ICT systems and the processes they support interoperable, which is only possible when all systems and subsystems are developed and operate on well accepted policies and standards – which is the core aim of NeGIF.

There are multiple benefits that can be expected from the Interoperability Framework.

- Every single component of the IT Technology infrastructure utilized by the ministries across the departments will comply with the technical and data standards catalogue to promote inter-operability
- It will enable better decision by allowing data compiled by different agencies to be used together
- It will also eliminate patchwork of ICT solutions in different government offices that are unable to 'talk' or exchange data.
- It will improve coordination between various government and non-government agencies. It will enable prudent utilization of government resources by preempting redundancy and waste of resources due lack of coordination.

- It will enable the government service delivery to become more citizen-centric. To be truly citizen-centric we need to break down the silos and allow seamless flow of information through various departments.
- It will lead to dramatic cost savings by the virtue of obviating the need for new systems by improving the current systems, reducing reliance on single vendors and making systems, knowledge and experience reusable from one agency to another.
- Overall e-Government Interoperability Framework is expected to result in better governance for the citizens of Nepal.

One of the crucial requirements for eGIF to work in Nepal will be to have nationwide infrastructure, so that the information governed by eGIF flows across the government and the public sector. *The good news is Nepal is taking effort to develop and enhance the infrastructure through various initiatives such as building a nationwide network infrastructure.* We believe that NeGIF will aid the success of these projects and will also be vital element for managing e-Gov interconnectivity, data integration, e-Services access and content management. It will also need to facilitate exchange of information effectively with other equally interoperable bodies, changing internal systems and practices, to make them interoperable. So a structured customized approach to design and implement eGIF is critical.

Thus the Nepal e-Government Interoperability framework (NeGIF) will be one of the key components of Nepal e-Governance transformation process.

2.4 Dimensions of eGIF

To achieve interoperability it requires a global approach that takes into account issues like types of interactions, the interoperability chain, standards, common infrastructure services and conditions for sharing, re-use and collaboration. These aspects are covered in the various dimensions of interoperability standards that are adopted globally, namely:

- Business process or organizational interoperability;
- Information or semantic interoperability; and
- Technical interoperability.

These dimensions are also the capabilities of eGIF. These capabilities are required to improve the interoperability. The improvement is achieved through the right mix of policy, structure, standards, process, management and technology across all capabilities (organisation, semantic, and technology). These will also improve the ability of government organisations to deliver coordinated government programs and services and share information across stakeholders/agencies.

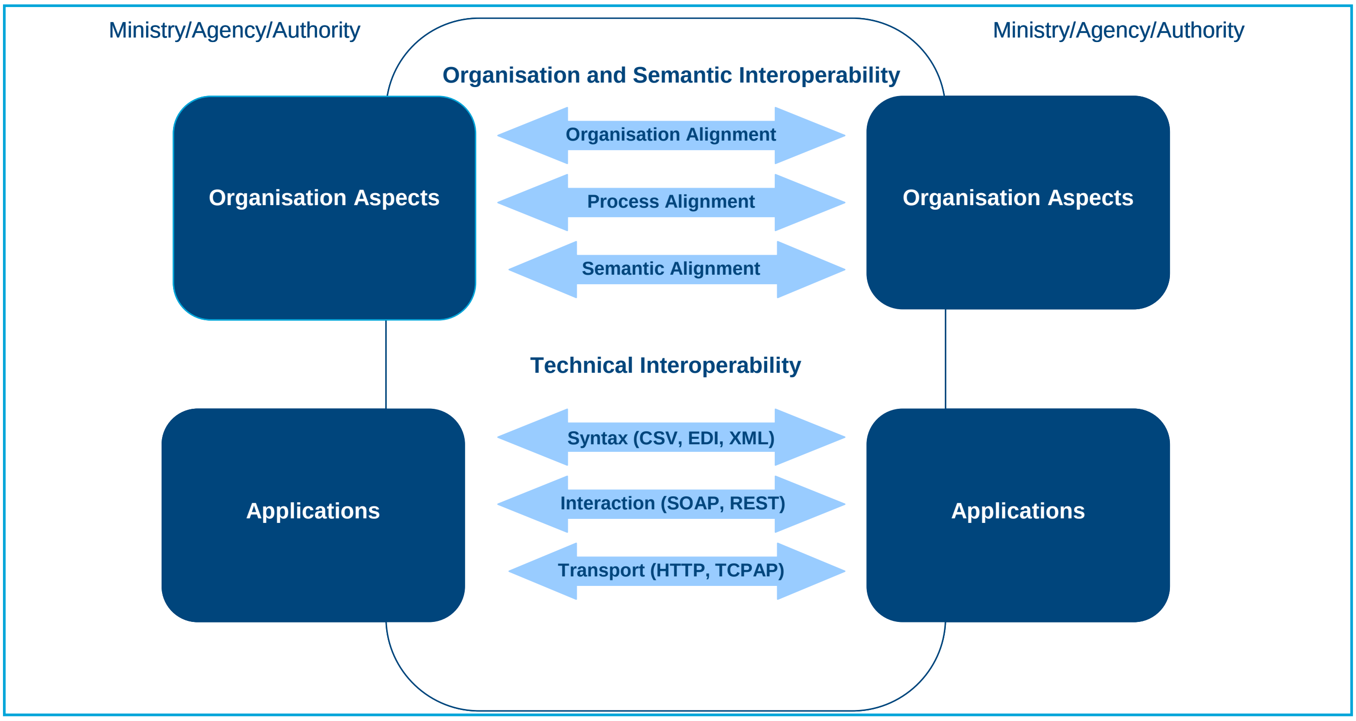


Figure 0-4: Interoperability Reference Model

Source: PwC adapted from external sources

Business Process or Organizational interoperability:

It is concerned with collaboration between entities in the development, deployment and delivery of e-Government services, and to the interaction between services, and supporting processes. Specifically, business process or organizational interoperability deals with defining organisation goals, common methods, modeling business processes, defining shared services etc. For example, in many countries infrastructure industry needs the cooperation of the social security department and the construction department. The social security department helps monitor payment of social security, medical insurance, accident insurance and endowment insurance for the workers of the company. Meanwhile, the infrastructure department is given charge of examining, approving and supervising the construction projects including how companies hire and manage their employees. If there is an organisational interoperability, the infrastructure department can keep a record of each construction project including location, construction schedule and number of workers. These records can then be sent to the Social Security department to monitor if the companies are providing insurance for their workers. The social security department can then examine the labour insurance payment of each construction company periodically and inform the construction department accordingly and the construction department can take these factors into consideration while examining and approving the projects. This kind of cooperation across departments results in each department being granted access to more information and is therefore better able to supervise and provide services.

Information or semantic interoperability:

Semantic interoperability is concerned with the communities of practice and to the negotiation of meaning that occurs within them. It is also concerned with ensuring that the exact meaning of information from various applications are understandable by any application even though if the application was not developed for this purpose'. For e.g. semantic interoperability services can be used when a citizen relocates his home and business from one city to another by means of a single interaction. Linking the user's name to their business and retrieving residential and business addresses, telephone numbers etc. will ensure interoperability. In some countries they prepare a common words thesaurus for commonly used terms, for example in accounting and administration functions all ministries and agencies make use of terms such as Acquisitions, Contracting out, e-Procurement, Outsourcing, Procurement and Tendering. These terms are defined clearly and standard connotations are provided. The effort is in first identifying the area, then defining the semantics and lastly institutionalising the usage. Interoperability at this level can fail if different users, or groups of users, use different terms for similar concepts, or use similar terms to mean different things.

Technical interoperability:

Technical interoperability is the most common and basic aspect of interoperability. This is necessary to ensure that all the hardware and software components of the network and information system can physically communicate and transfer information successfully. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services etc. System of Systems Interoperability (SoSI) Model, developed by the Carnegie Mellon Software Engineering Institute (SEI) as part of an independent research and development project have also developed three types of interoperability such as:

- Programmatic: interoperability between different program offices or organizations tasked with the development of a system
- Constructive: interoperability between the organizations that are responsible for the construction(and maintenance) of a system
- Operational: interoperability between the fielded systems.

The interaction among elements that correspond to various technological waves, particularly relevant in relation to preservation and access of information on the electronic media need to be considered in technical interoperability.

2.5 Challenge in design and implementation of eGIF

Based on our understanding and analysis of practices on design of eGIF implementation across the world and our assessment of Nepal, we found some major challenges that countries need to handle while designing and implementing eGIF:

- Lack of capacity is a key issue in a developing economy, even in developed economy this does exist but the magnitude however is lesser. The ability of the economy to absorb skills, knowledge and creating a learning framework (ecosystem not just education) with a mixed strategy of self learn, learning through sourcing and incentivising is key to build capacity.
- Choice of appropriate mechanism for eGIF governance - This is a critical issue that needs to be dealt carefully. eGIF is usually managed centrally but it should not be a case wherein a central agency dictates rules. It should be a participative framework wherein a right mix of standardisation and localization/customization at the agency level is crucial. Solving the trade-off between widespread buy-in by involving larger participation in development of standards vs agility by involving select key people is also a key challenge to be addressed. The choice of the right governance model is a country specific challenge which needs to be addressed by the leaders of the government through discussion and mandates.
- One size fits all – 'One solution and everything is solved' is not the role of eGIF. Every eGIF has specific purpose and every version of a country's eGIF evolves. Trying to get everything right at the first go and making it comprehensive in the first version will not help. Starting with minimum implementable framework and evolving it further will be a better approach
- Scoping of eGIF that defines the relationship between various initiatives and coherence between them is crucial as redundancy may creep with more and more initiatives, e.g. Identification of Enterprise architecture (EA) and e-Governance strategy which the eGIF can support should be analysed first.

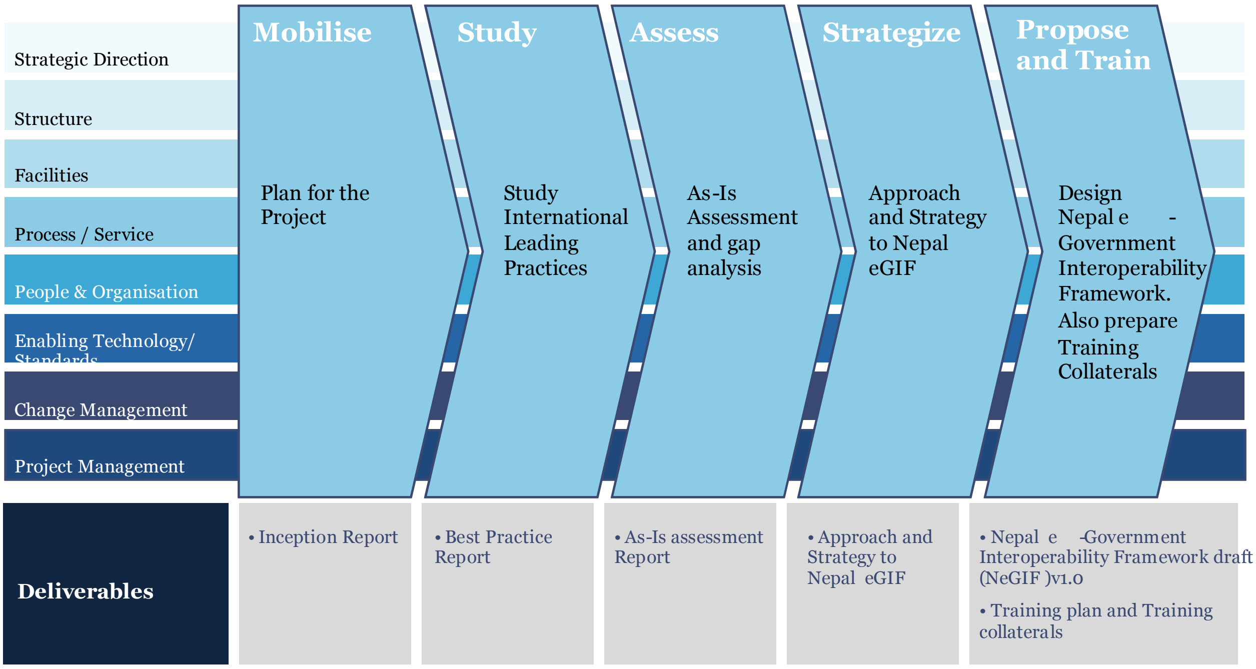
- Awareness and communication of eGIF is a crucial challenge as many concepts, convention, tools practice have to be conceived and perceived in the same way by everyone.
- Lack of source funds – These are fundamental issues concerning many developing nations, many countries have postponed/delayed their e-Governance initiatives due to lack of ability managing funds, this is a long term economic issue that needs to be handled first before embarking on any e-Governance initiative.

The above challenges the NeGIF has taken into account and we propose an appropriate solution in this report.

2.6 Project Stages and Approach

2.6.1 Stages

The following diagram summarizes the different stages and deliverables of the eGIF project.



Strategic Direction
Structure
Facilities
Process / Service
People & Organisation
Enabling Technology/ Standards
Change Management
Project Management

Mobilise
Plan for the Project

Study
Study International Leading Practices

Assess
As-Is Assessment and gap analysis

Strategize
Approach and Strategy to Nepal eGIF

Propose and Train
Design Nepal e - Government Interoperability Framework. Also prepare Training Collaterals

Deliverables
- Inception Report
- Best Practice Report
- As-Is assessment Report
- Approach and Strategy to Nepal eGIF
- Nepal e -Government Interoperability Framework draft (NeGIF)v1.0
- Training plan and Training collaterals

Figure 0-5: Stages and Deliverables of the eGIF Project

The essence of this project taken up by M/s PricewaterhouseCoopers, India for Nepal ICT Development Agency (HLCIT) is to provide meaningful alignment of e-Government Interoperability Framework (eGIf) towards Nepal's e-Governance strategy and increase the ability of Nepal government to share information and integrate information and business processes by use of common standards as it moves forward on an ambitious eGovernment Programme.

The following deliverables (as per the contract) have helped to reach the milestone of drafting the eGIF for Nepal.

- Inception Report
- Best Practice Report
- As-Is assessment Report

- Approach and Strategy to Nepal eGIF.
- Nepal e-Government Interoperability Framework draft (NeGIF)v1.0
- Training plan
- Training collaterals namely - Standards CD and Power points presentations deck of all the workshop/training sessions

2.6.2 Approach

The following diagram summarises the approach towards delivering NeGIF. A detailed description is provided below the diagram.

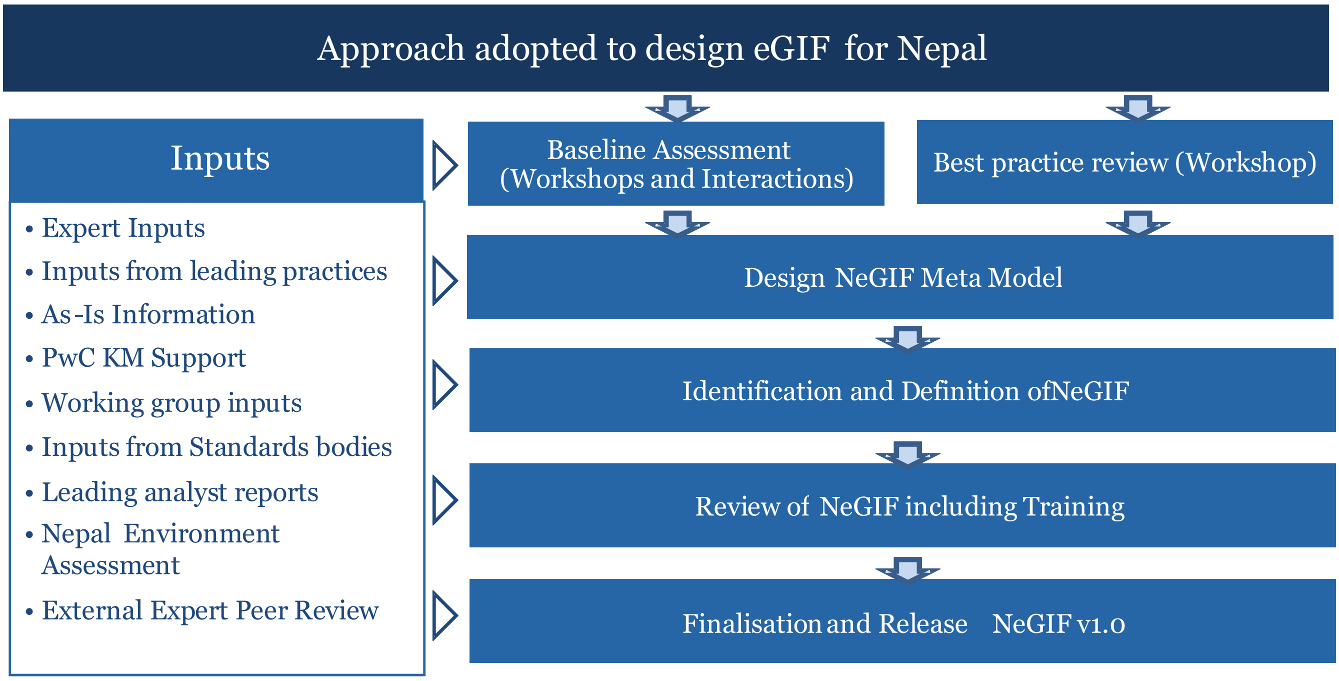

Approach adopted to design eGIF for Nepal
Inputs
• Expert Inputs
• Inputs from leading practices
• As-Is Information
• PwC KM Support
• Working group inputs
• Inputs from Standards bodies
• Leading analyst reports
• Nepal Environment Assessment
• External Expert Peer Review
Baseline Assessment (Workshops and Interactions)
Best practice review (Workshop)
Design NeGIF Meta Model
Identification and Definition ofNeGIF
Review of NeGIF including Training
Finalisation and Release NeGIF v1.0

Figure 0-6: Approach towards delivering NeGIF

a. **Baseline Assessment**

Baseline assessment includes the following activities

- **Kick-off and Inception Report**

The assessment phase started with the kick off meeting of the project. PwC presented to HLCIT the detailed objectives, scope, deliverable project plan, approach and HLCIT agreed to the same.

i. Inception report

This report contained detailed information on the objective, scope, approach, deliverables, finalized work plan, activities and timelines of this project.

ii. Questionnaires

Three Questionnaires were prepared namely Organisation and Process Questionnaire, Application Information Questionnaire and Technology Information Questionnaire. Each of these questionnaires were designed to assess various aspects/components such as:

- Service
- Application
- Enterprise Architecture
- Technology
- Organisation
- Security and
- Best Practices, Policies & Standards.

- **Administration of Questionnaire**

Three Questionnaires containing qualitative and data collection questions to assess the current state of NeGIF were circulated to the respective ministries. The objective and the details of the 3 questionnaires are as follows:

i. Organisation and Process Questionnaire for NeGIF v1.0

The purpose of this questionnaire is to understand:

- the nature and functions of the Organisation, its priorities and target by knowing its goals and objectives
- the baseline (As-Is) processes
- the different roles, and skills required to perform functions in addition to the responsibilities of each role
- the services offered by the Organisation, the information for which is essential inorder to understand the type and kind of data that will be generated from each ministry and to identify commonalities and areas of standardisation across various ministries etc.

ii. Application Information Questionnaire for NeGIF v1.0

The purpose of this questionnaire is to:

- to assess the maturity of application against application management, application functionality/performance and security aspects
- to assess the sufficiency of transactional/reporting application meeting the business need
- to assess the maturity of interactions between various application.

iii. Technology Information Questionnaire for NeGIF v1.0

The purpose of this questionnaire is to:

- assess the existing capacity and baseline IT infrastructure resource
- assess the IT Roles and responsibility and skill sufficiency and requirements
- assess the maturity of technology in meeting the business need.

The above aspects/components are dealt in detail in the analysis and findings section of the Assessment Report (As-Is).

- **Meeting with Stakeholders (20 Ministries/Agencies)**

  After the Questionnaires were circulated, PwC team along with help from HLCIT conducted meeting with 16 ministries/departments explaining the importance, scope and details of the assessment and a walk through for filling the information required in the questionnaire. Each ministry was given a date of submission for responding to the questionnaire.

- **Workshop 1 and Follow-up Meetings**

  After the questionnaires were circulated PwC conducted a workshop on introduction to eGIF, application standards and introduction to Enterprise Architecture (EA) and the relationship between eGIF and EA. Subsequent to the workshop PwC team visited each ministry for providing clarification on questionnaires and also to help them complete the responses to the questionnaire.

- **Analysis, Findings and Workshop 2 and 3**

  On receipt of responses to the questionnaires, PwC sorted the information and analyzed the maturity of the organisation, application and technology across seven components such as:

  1. Service
  2. Application
  3. Enterprise Architecture
  4. Technology
  5. Organisation
  6. Security and
  7. Best Practices, Policies & Standards.

  for 15 ministries/agencies. The assessment of data centre (both NDC and other ministry ministries which have data centre) was done with respect to data centre criteria defined additionally over and above these seven components.

  Each component may have one or more parameters contributing to the evaluation of the component as a whole for e.g. application, application interface and common application may be some of the parameters under the application component.

  The overall baseline architecture, assessment of all ministries /agencies are provided in the As-Is report. This was presented to the stakeholders during workshop 2 and 3. The Assessment was based on the information provided by the ministry and it was with respect to the time of collection of baseline data. The assessment report also contains root cause for challenges/issues and recommendations. The challenges /issues combined with the leading practices across the eGIF of candidate countries have been considered closely to prepare the NeGIF.

b. Best Practice assessment

An important imperative of this project is to use inputs from the leading practices in eGIF of various countries and their experience in designing the Nepal eGIF. The document submitted by PwC reviewed each candidate country and derived the leading practices that can be adopted/used in NeGIF.

PwC reviewed the eGIF of various candidate countries that had a matured eGIF and identified the collective and individual country's leading practices. The key outcome was to encapsulate and elaborate key learnings of leading practices in eGIF based on the other country's practices. This involved studying who were involved in eGIF; making direct contacts with the agencies for detailed information, why an eGIF was developed, the context, scope etc; how GIFs were produced and revised; and what were the critical success factors essential to make eGIF successful in the country.

c. Formation of working groups

As it is important to increase the participation and contribution from various ministries/agencies to make this initiative a success we identified working groups for each of the 9 technical areas of interoperability standards namely Interconnection, Data Integration, Access, Collaboration, Application Design and Development, Application Integration, System Standards, Meta Data and Security. These working groups will work along with the experts and contribute in the design and implementation of the eGIF. Going forward, these working groups will provide the technical expertise to maintain and manage the standards lifecycle.

d. Approach and Strategy to Nepal eGIF

After assessing the current environment based on the Baseline information, we identified key challenges and issues pertaining to Nepal that will need to be addressed to improve the eGIF maturity. We have also reviewed eGIF for various countries and their experience in designing and implementing it, to take key learnings of practices in eGIF in those countries that will be relevant to Nepal.

Hence based on the understanding of Nepal's current environment, leading practices of eGIF across the world and with the objective to

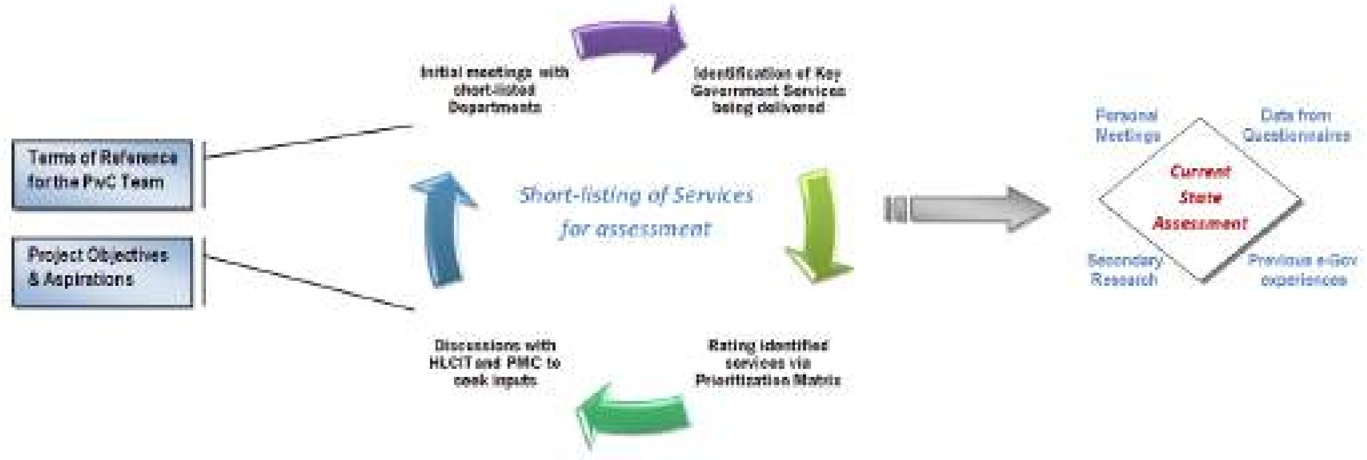
- ensure that resources are expended in the right direction without reinventing the proverbial wheel and circumventing the mistakes that others have made
- improve the effectiveness of the implementation of eGIF in Nepal by adopting latest practices
- facilitate information standards that will such as e-Government architecture framework (eGAF)

an NeGIF Meta Model and the approach and strategy for NeGIF was proposed which will assist Nepal to improve their interoperability maturity.

3. Summary of As-Is Assessment

3. Summary of As-Is Assessment

The overall approach that has been adopted for Current State Assessment of short-listed Government Services is shown below:


Terms of Reference for the PwC Team
Project Objectives & Aspirations
Initial meetings with short-listed Departments
Identification of Key Government Services being delivered
Short-listing of Services for assessment
Rating identified services via Prioritization Matrix
Discussions with HLCIT and PMC to seek inputs
Personal Meetings
Data from Questionnaires
Current State Assessment
Secondary Research
Previous e-Gov experiences

PwC Team began the current state assessment by first short-listing the Government Services that would be assessed from GEA's perspective. This particular exercise was based on the Terms of Reference as provided at the time of award of the contract and the Core Objectives & Aspirations of the Project as understood by the PwC team. It comprised of 4 main tasks:

- Discussions with HLCIT and the Project Management Committee to understand their Vision pertaining to the GEA and to finalize the coverage of the assessment in terms of the Ministries and Departments to be covered

- Holding initial meetings with short-listed Ministries / Departments to understand their mandates, responsibilities and structures

- Identifying the Key Government Services that are being delivered by these Ministries and Departments and the methodologies that are used to do the same

- Evaluation of these Government Services via a Parameterized Prioritization Matrix to determine their readiness, importance and relevance for final inclusion in the Assessment exercise (see Annexure for the list of parameters on which the prioritization of services has been done)

The end-result of these 4 tasks was the final list of Government Services that were an appropriate mix Citizen-facing Services (G2C), Business-facing Services (G2G) and Government-facing Services (G2G) across the following Ministries / Departments / Agencies:

Inland Revenue Department (IRD)	Supreme Court of Nepal
Department of Transport Management (DoTM)	Nepal Police
Ministry of Foreign Affairs (MoFA)	Municipalities
Election Commission (EC)	Financial Comptroller General Office (FCGO)

Department of Roads (DoR)	Nepal Telecom Authority (NTA)
Ministry of General Administration (MoGA)	Department of Land Reform & Management (DoLRM)
Tele-Center Network (under Department of Post)	Public Service Commission (PSC)
National ID Management Committee (NIDMC)	Nepal Rastra Bank (NRB)

Services short-listed from these Ministries / Departments / Agencies were thereafter fully assessed in their "As-Is" State utilizing a combination of Personal Meetings (with various Officers and Technology Partners in concerned Departments), Questionnaires (that captured the details pertaining to a particular Government Service along with the Ministry / Department / Agency delivering the same) and Secondary Research (from the Official Websites, Rule Books, Manuals, Documentation of Applications currently being used, etc.). It was further ensured that PwC's previous experiences from across the World are referred to during Current State Assessment and Learning from such assignments are also factored in while understanding the Core Governance Principles on which the Short-listed Services are based upon.

This entire study is divided into 15 Sections (for each of the 15 Ministry / Department / Agency except NRB as listed in the Table) and each of these Sections are further divided Service-wise into Sub-sections. Each Sub-section refers to an individual Government Service and broadly has following 7 parts:

i. Service Overview: provides a broad overview of the S Government ervice being assessed and also gives an insight into the flow of delivery that is currently being used

ii. Broad Description: provides the service-type (G2C, G2B or G2G), names of the Participants and the lists the pre-conditions that need to be ensured for successful delivery of the Service being assessed

iii. Detailed Flow: provides the Cross-Functional Flow of the Government Service's delivery and also provides the details regarding various Enablers / Essentials (such as Supporting Documents and IT Systems that exist)

iv. Input Matrix: lists the data-items that are have to inputted for successfully delivering the Government Service at present and the Sources of all such data-items

v. Output Matrix: lists the data-items that are outputted / generated while delivering the Government Service and the Recipients of all such data-items

vi. Current State Assessment: provides "first-look" analysis of the entire flow pertaining to the delivery of the Government Service and identifies the Design Considerations for suggesting BPR Recommendations.

vii. List of Web Services: that can be extracted from the current delivery-flow of the Government Service and the potential consumers of such Web Services

Overall Qualitative Assessment

The following table summarises the assessment of Baseline Organisation & Process, Application and technology environment of Nepal across all the components that have been defined.

Table 0-1: Qualitative Assessment

Component	Assessment description

Component	Assessment description
Service	- Across most of the ministries the Service automation level is low. - Lack of standard frameworks for service prioritization. - No formal infrastructure for integration of services with other government agencies. - The information reusability in service delivery is not achieved. - Little documentation is available on services.
Applications	- Availability & usage of application within or throughout departments is low, post BPR this will be a prime focus area as business process /transactional/reporting need to be addressed through an application - Application level roles and responsibilities though exists in some departments but in most of the departments are not defined clearly - Individual applications are built independently to align with business functionalities. Changes in the common business functionalities handled by these applications will have an impact on their maintenance. - No well defined application integration architecture to allow applications to integrate across different govt. ministries - Common application reusable components across enterprises are not defined - Software development life cycle process and implementation framework are not defined for implementation at enterprise level, some projects are delayed - Application non-functional requirements such as availability, performance, application maintenance SLAs and No compliance process are not defined
Technology	- Even though availability is medium, technology is not adequate enough and is also not scalable. - No proper standards for hardware is defined - Data centre maturity is low and needs to improve to scale up for future needs - At the data level, roles and responsibilities are not defined to design, develop and deploy the database and changes as per requirement. - Components used in IT infrastructure design are modular, however no document/information has been observed to standardize re-usability across the organisation. - No tools are used for monitoring and managing infrastructure and benchmarks and SLAs are not defined. Getting technology Inventory is tough. In the future, due to proliferation of application, there will be more technology and data to be managed which will increase the overall technology capacity.
Architecture	- No standard architectural guidelines & principles defined at enterprise level - Application design framework is not defined at enterprise level. - Though network is defined as layers, a framework for IT infrastructure integration within the organisation is not documented and adopted. - There is need to define and document the design, model, and data view.
Security	- Though there are no common standards for security available - No disaster recovery plans yet - Enterprise level security framework is not defined for Standardization of security products, technologies and its integration with application at enterprise level - There is no information sharing policy like NDA being implemented by the ministry - Lack of comprehensive policy on data management and technology usage. Though in bits and pieces, there are policies in specific ministries for desktop, password, email etc. - The classification of business information as per the sensitivity to business continuity is not done
Policies	- Lack in adoption of adequate policies or standards for technology, application process and architecture. - Processes such as change management, asset management, and vendor management have not been properly defined and documented. - There is no plan for data governance for data policy management Process and compliance process for data lifecycle.

Component	Assessment description
	- Application, technology and data guidelines and templates are not standardized. In some departments it is not available, this in turn will result in increase in project timelines - There is no standard auditing process for monitoring the service. - Lack of standard processes to communicate changes/ enhancements in standards or policies would lead to inconsistencies in understanding and incorporating the changes.

4. Learning from leading practices

4. Learning from leading practices

An important imperative of this project is to use inputs from the leading practices in eGIF of various countries and their experience, in designing the Nepal eGIF. The document submitted by PwC reviewed each candidate country and derived the leading practices that can be adopted/used in NeGIF.

The GIF of various candidate countries with a matured eGIF were reviewed and the collective and individual country's leading practices were identified. The key outcome was to encapsulate and elaborate key learnings of leading practices in eGIF based on the other country's practices. This involved studying who were involved in eGIF; making direct contacts with the agencies for detailed information, why an eGIF was developed, the context, scope etc; how GIFs were produced and revised; and what were the critical success factors essential to make eGIF successful in the country. The key learning from the leading practices review is given in the following paragraphs.

The following countries were considered for the study:

Sl.No	Countries	eGIF/GIF framework
1	UK	United Kingdom e-Government Interoperability Framework (UK e-GIF) v 6.1
2	New Zealand	New Zealand e-Government Interoperability Framework (NZ e-GIF)v 3.3
3	Australia	Australian Government Technical Interoperability Framework
4	Canada	Treasury Board information or technology standard (TBITS) and CLF 2.0 Standards and Guidelines
5	European Union	European Interoperability Framework for Pan-European e-Government services v 1.0
6	Germany	Standards and Architectures for e-Government Applications v 2.0
7	Brazil	e-PING Standards of Interoperability for Electronic Government v 2.0.1
8	Malaysia	Standards, Policies and Guidelines - Malaysian Government Interoperability Framework (MyGIF) v 1.0

4.1 Leading Practices

4.1.1 Structure

	Structure
A	Each country has defined interoperability based on the scope and extent of coverage. Most of them start as a set of 'minimum technical standards' and then evolve broader and deeper. Countries like Germany and Canada have more comprehensive coverage as they have included interoperability in their architecture.

Structure	
B	“The reality in most e-Government settings is that there is a complex goal structure and strict legal norms, while interoperable services must still be delivered in a secure and transparent way.” Many countries use interoperability differently for e.g. UK, New Zealand, Brazil, Malaysia make it mandatory to define, maintain eGIF standards for interoperability whereas countries like Canada, Germany have imbibed the interoperability aspects in their enterprise/federated architecture. There are no better approaches; it is based on the need, scope and objective; while countries that have mandated eGIF aim to achieve technical interoperability through eGIF, while countries using interoperability standards as guidelines use it to reduce the effort on multiple initiatives, multiple standards and governance. Depending on a government’s objective, capabilities and available resources, interoperability scope and objective are decided. The architecture of a system may enhance or reduce the ability of the system’s Components to interoperate with each other. Some architecture may facilitate interoperability, while others may inhibit it. Therefore, whatever architectural paradigm is adopted, assumed, or inherited should be provided in eGIF. As GIF is a set of rules that specify what standards are to be used, architecture should provide common resources. Best practice suggests that countries should concentrate on architectural aspects while developing an eGIF. Some eGIF may include a discussion of its relationships and linkages with other related efforts, such as national EAs. Alternatively after eGIF and EA are developed, both the artifacts may be converged to include architecture and standards in one document to rationalize both.

4.1.2 Scope

Scope	
C	Most pure play eGIF initiative focus on technical interoperability as this is quintessential to define standards for different parties in a government to interact and exchange data /information Some of the Organization and semantic interoperability aspects are imbibed in the principles and policies. Countries like Germany, Canada and European Union who have highly evolved e-Services and architecture have incorporated organization and semantic aspect in through their architecture initiatives and technical interoperability is usually covered in the architecture principles, policies and standards. ‘The reason for most candidate countries in our sample to have gone for technical interoperability could be that it is easier and fundamental to have technical interoperability before embarking on the other types of interoperability. Interoperability covered through architecture focuses on defining standards based on service e.g. job search, application for visa, income tax declaration etc. Generally, all government agencies are bound by GIF, but the definition for ‘government agency’ varies. Australia does not specify name of agencies that are covered. The UK Government, on the other hand, includes central government departments and their agencies, local government, and the wider public sector. Some countries like Malaysia extend the limits to cover local authorities as well. In New Zealand, it includes all public service departments, Police, Defence Force, Security Intelligence Service etc

4.1.3 Principles

Principles	
D	All eGIF initiative have defined key principles as the basis for defining and managing the standards and specification. Countries, such as Germany, Canada, which have covered interoperability through other initiatives have also inculcated the architectural principles. The selection of the principles is based on the scope and objective of the initiatives as the eGIF evolves principles may also be enhanced. Also definition of the principles in each country may be different based on the context, scope and objectives. Open

	Principles
	standards are an important principle of any interoperability framework that is common across all the candidate countries and even other top countries who have initiated eGIF. Apart from these principles there are certain aspects that are also considered such as Universal Access and Security and defining Intellectual Property Rights to support a global competitive market and the compatibility of new technologies within growing interdependent systems and to prevent manipulation of standards for rent-seeking and market domain.

4.1.4 Policy and Standards Coverage

	Policy and Standards Coverage
E	Technical standards area against which the review for breadth and depth has been done refers to different aspects of interoperability. Various eGIF initiatives have defined standards across the different technical areas. The point of integration between various candidate countries on the technical standard areas in terms of breadth and depth of coverage are Interconnection/Communication, Data management, Access and Collaboration, Security and Meta Data. Other standard areas such as Process, Architecture, Hardware System Software and Web services are important to countries that have embarked on eGIF initiatives coupled with their architecture. Some countries along with their standards have also focused on Legal or legislative considerations, Semantics etc. From a Nepal context these areas are important because interconnection, data management and access and collaboration are mandatory standard areas for interoperability to happen at technical level. In advent of initiatives like smart cards there will be huge requirements for Meta data of citizens for many initiatives to come which requires Meta data standards. For an emerging country like Nepal it is important to look at all the Technical standard areas that have been identified. Each country may call the technical standard area in different names, however they cover the one or more aspects of technical standard areas defined. Malaysia has used proprietary standards, Australia has couple of them, New Zealand has provided links to some vendor websites for standards and Brazil has used few proprietary production their standards, Nevertheless all the frameworks stress on adoption of open standards. Australia, Germany, Malaysia and New Zealand have explicitly mentioned the preference for open standards. Standards also have lifecycle; any new standard will be considered/recommended, or rejected. The recommended standard will be maintained and with the change in the version the maintained standards can be phased out or deleted. Broadly the standards defined are classified as under consideration, Recommended, Mandatory, Adopted and Deleted. Hence it is important to make the eGIF framework 'flexible' to anticipate and accommodate change. The classification of standards usually depends on the level of maturity of the countries implementing the GIF. An emerging eGIF may not have the same mandatory standards of a matured eGIF. Though the selection of standards are based on the principles defined, it should be **flexible** to accommodate aspects like supporting backward compatibility with older systems , to consider historical, technological and cultural heterogeneity, constant change, and the reality that different agencies implement technology differently.

4.1.5 Governance

	Governance
F	The Best practice structure of eGIF governance usually comprises of the following authorities. **Lead Agency/Authority**: Is a lead body providing personnel, budget and other administrative requirements. Apart from organizational support, the lead agency could also have a final say in the approval of standards in the eGIF. **Execution Unit:** Usually this is a unit established under the lead agency by picking up skills from across different agencies to manage the operations of the GIF document from development to approval to revision, etc. It also coordinates with the different stakeholders involved in the GIF development process **Working committee or Groups:** These are several technical groups that do the actual work on the technical policies. Usually these groups comprise of experts from various government agencies and is the technical body that works on standards selection. **Independent Groups:** These are usually pool of expert outside the working group countries like Germany, Australia and UK .These countries have hired individual experts/counting firms for specific areas of contribution. In some countries like Germany, Canada and Denmark the Architecture group serves as the working group and execution body, so the roles and responsibilities of each of the authority is quintessential to understand how governance is organized. Citizens have also contributed their perspectives in some of the GIF, this was used to evaluate the impact and the usability of the specifications in the GIF to the end user.
G	The process for development and updation of eGIF standards is almost similar. Countries like Malaysia, New Zealand, UK, and Australia have similar processes. Whereas, countries like Germany and Canada does have similar processes to define standards, but within their architecture process. Generally, the process for changing a standard is the same as that of developing it. Compliance to policies and standards is usually defined both in terms of specific requirements to support standards, protocols, and paradigms, and in terms of higher-level requirements to meet the goals of interoperability. There are monitoring and evaluation processes defined to ensure compliance. Countries like UK and Germany have also defined adverse mechanisms in case of non-compliance such as withholding funds and approvals for projects of those who are not complying with eGIF.

4.2 Key Learnings from eGIF Leading Practices

Achieving interoperability in 'one go' is a big leap. It is a process of many incremental activities over time. Hence, it was observed that significant infrastructure of people, technology and knowledge needed to be in place to create, use and revise the e-Government interoperability document. Each candidate country's eGIF differed from one another based on challenges, scope and objective of their government strategy and environment.

The review has exhibited the common leading practices across the various criteria which were similar between the candidate countries.

The table below summarises good practices followed by candidate countries in relation to various aspects of eGIF. Some of the relevant leading practices have been incorporated in the Nepal eGIF as well as identified for Nepal to consider.

Scope, Coverage and Principles

- Sound principles, goals for interoperability, clear scope should be the basis of defining standards rather than defining standards independently for e.g.
    - Goal: Improve private sector and personal interactions (G2B, G2C etc.)
    - Interoperability policy: encourage use of open standards and (possibly) open-source software, include semantics for private sector and personal interactions and emphasize personal and enterprise portals. Interoperability must therefore be:
        - Reflected in the conceptual design of government, system architecture
        - Supported by infrastructure.

- To be truly interoperable it is important to concentrate on Organisational and Semantic interoperability after ensuring the implementation of technical interoperability. Data-sharing and cooperation across agencies with each agency granting more access will help better governance, providing services faster and above all reducing redundancy of information.

Governance, Compliance and management of eGIF

- Ability of the Lead Agency and Execution unit to independently operate with good span of control, clear funding mechanism and limited number of key stakeholders

- The process of developing and revising the eGIF should involve participation from the stakeholders. This will ensure support for the document among those who will eventually implement it. Also, scoping appropriately can help, for example
    - having the eGIF apply to new systems first and then move to incorporate older systems
    - incentivising the adoption may result in effective compliance of eGIF by the agency e.g. only GIF compliant e-Government projects will receive funding preference.

- Enforcement, capacity building and monitoring & evaluation are critical to the success of eGIF. Not investing in these will be the only cause of failure of eGIF. Typically the following are evaluated, monitored and enforced:
    - The status of completion of the eGIF
    - The degree of adoption of the eGIF
    - The effectiveness of the various processes specified within the eGIF
    - The degree of achievement of various goals
    - The perceived impact of the eGIF
    - The cost-effectiveness of specific e-Services or overall e-Government delivery that are the expected outcomes of implementing and using the eGIF.

Policy/ Standards Coverage

- All standards are selected based on the objective, scope and principles of eGIF, coherently and not loosely coupled.

- Adoption of Open standards is widespread. 'A recommendation for effective support for interoperability must start with the sole 'compatibility' criterion for new software being software from multiple vendors'. This being very relevant to Nepal currently because many departments such as Transport authority which are spread across different regions may decide to implement smart cards for Driving Licenses and Vehicle Registration. To make the smart card interoperable with hardware/software being used by different regions in Nepal and compliant with the National Vehicle Rules one need to define open standards. This will result in more number of vendors available to provide cards /card readers, ensure better interoperability, reduce prices and increase bargaining power for the government.

- Also main thrust of some of the e-GIFs is adoption of Internet and World Wide Web standards for all government systems (UK for e.g. made a strategic decision to adopt XML and XSL as the core standards for data integration and presentation. This includes the definition and central provision of XML schemes for use throughout the public sector).Such standards/policies will move the eGIF towards latest technology advancements. Countries like Ethiopia where the interoperability between applications are normally low across ministries, can embark on such policy to facilitate effective interoperability while developing new applications

Implementation of eGIF

- For Effective and successful eGIF Implementation the candidate countries have practiced the following:
  - adaptation of eGIF specifications as respective ministry/agency's policies
  - defining enforcement and monitoring process by the execution unit
  - providing appropriate tools or service for IT officials who will design IT projects; and
  - Recommending/preferences to eGIF compliance in the bidding process.
  - adverse stance like withholding funds and approvals for projects of those who are not complying with eGIF (countries like Germany and UK have these penalties).

5. Nepal e-Government Interoperability Framework (NeGIF)

5. Nepal e-Government Interoperability Framework (NeGIF)

5.1 NeGIF Meta Model Rationale

For any government, improving government interoperability can be a complex effort and resource intensive initiative. We have observed from our experience with various governments around the world, that a government while differing in their specific political structures and even degrees of civil society and rule of law, tend to share at least one similarity, they struggle in their efforts to effectively share authority, resources, and information across the organizational boundaries within those governments to become interoperable. While the extent of complexity varies, the challenge of working together across the Government interoperability is the mix of policy, management, and technology capabilities needed by a network of organizations to deliver coordinated government programs and services across boundaries remains intense. By implementing the NeGIF the technical interoperability will be strengthened to enable the semantic and organisational dimensions of interoperability.

Technical interoperability can be achieved either:

- through the adoption of eGIF standards and guidelines that a government specifies to its ministries/agencies and business to interact/collaborate with each other or
- through Enterprise architecture(EA) whereby defining each component of the government, how they are related and designing sub architecture of each component to gain interoperability through architecture.

Many countries use interoperability differently, for e.g. UK, New Zealand, Brazil, Malaysia make it mandatory to define, maintain eGIF standards for interoperability whereas countries like Canada, Germany have imbibed the interoperability aspects in their enterprise/federated architecture. There are no better approaches; it is based on the need, scope and objective; while countries that have mandated eGIF aim to achieve technical interoperability through eGIF, while countries using interoperability standards as guidelines use it to reduce the effort on multiple initiatives, multiple standards and governance. Depending on a government's objective, capabilities and available resources, interoperability scope and objective are decided.

Sometimes the EA may enhance or diminish the ability of each component in the EA to interoperate with each other. Some architecture may facilitate interoperability, while others may inhibit it.

Nepal has taken a step towards defining interoperability standard (eGIF) along with EA. Hence, the underlying approach taken is whatever architectural initiative adopted, designed or inherited in the future should on one hand be supported by eGIF and on the other hand must provide guidelines to the architectural effort. Based on this understanding, we have proposed the following eGIF Meta Model which comprises of various aspects/components that are interrelated and by design will coexist. However the success of the interrelation will depend on the scope, interrelationship and management of the initiatives.

The following diagram represents the NeGIF Meta Model:

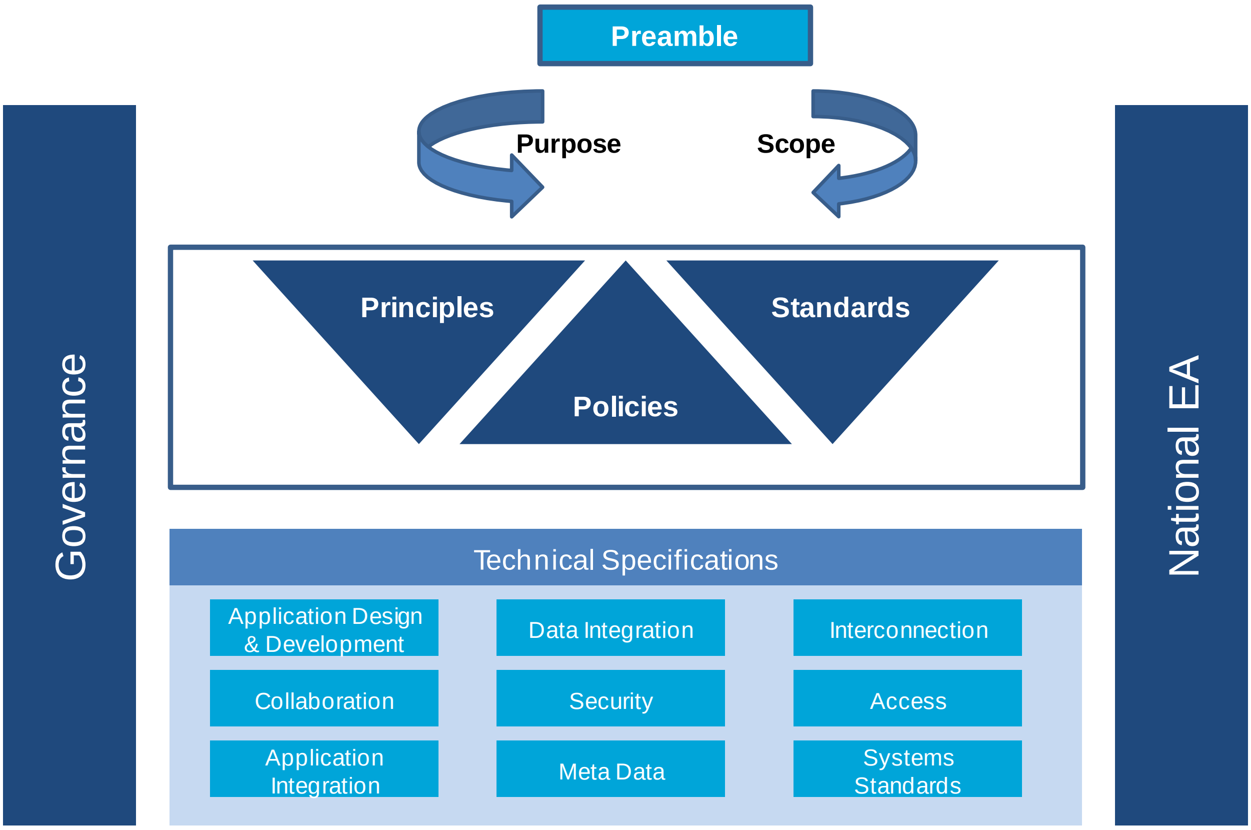


Figure 3-1: NeGIF Meta Model

The core of eGIF is the Preamble (covering purpose and scope), Principles, Policies and Standards. Governance and Architecture are aspects that will aid eGIF implementation, interrelationship, management and success.

The rational for having such Meta Models for NeGIF are:

- Principles defined, would serve as the guiding basis for defining the standards.
- Policies will act as enforcement guidelines for implementing these principles and standards.
- Standards are foundations upon which to develop new technologies and an opportunity to share and enhance existing practices.
- Architecture should coexist with eGIF coherently, so that both the initiatives complement each other and reduce redundancy through shared principles, artifacts etc.
- Governance is the key to implement and maintain such initiatives. Leading practice suggests clearly, that all successful eGIF have a clearly defined governance mechanism.

5.2 *Preamble*

Preamble covers the purpose and scope of Nepal eGIF.

a. Purpose

The overarching purpose of eGIF in Nepal should be to improve economic growth and equity by enhancing access to information and its effective use, thereby improving delivery of services to benefit stakeholders – citizens, businesses and also Government (intra and inter).

To enable interoperability across government in Nepal, starting with a solid strategic framework for e-Governance and aligning with the vision and goals of its leaders should precede the technology initiatives. Reason being, Nepal has already committed to key development goals and are striving to fight social and economic priorities like poverty and enhanced good governance in the short and medium term. In short, Interoperability in digital public services cannot be achieved without process re-organisation, legal system re-structuring and data re-work.

The key is networked resources – sharing and collaboration to improve transparency and participation. The eGIF framework suggested takes into account the Nepal environment and should be suitably adopted further.

This first version of NeGIF interoperability focuses primarily on the technical ability of ministry/agency's ICT systems or components to exchange information and to use the information that has been exchanged to improve overall governance. The key objectives to be targeted in NeGIF towards effective e-Governance are:

- Ensure elimination of patchwork of ICT solutions in different government offices that are unable to 'talk' or exchange data.
- Transform government to become more citizen rather than government focused in delivering public services.
- Reduce cost and enhance capacity building through standardization
- Improve coordination and information flow for faster decision making
- Develop a coherent mechanism (environment and infrastructure) for exchange of information and services between government agencies electronically.

b. Scope of Applicability

In general, all ministries/agencies/authorities in Nepal must be encouraged to comply with the NeGIF. The exchange of information between the following organizations should be made mandatory:

- Government-to-Government (G2G)
- Within Nepal Government i.e. between Government agencies and departments.
- Government-to-Citizens (G2C)
- Between Nepal Government and its citizens.
- Government-to-Businesses (G2B)
- Between Nepal Government and businesses in the private sector, i.e. suppliers and contractors to the Government.

The compliance with the NeGIF cannot be imposed on citizens, private businesses and foreign governments, but the Government of Nepal can make it available to all.

5.3 Principles

Every government has priorities for ICT plans. Based on these priorities and goals, a set of directions are required to define the kind of policies and for selection of appropriate standards. The principles cover parameters for selection of standards and also cover the limitations of the organization, anticipated outcomes of the eGIF, requirements for project and operational management, and governance. Principles typically provide the basis of policies/standards (why this policy, what standards to use) and also reflects concerns, risks, issues of eGIF. They can be used to guide future versions of the initiative. Principles are applicable and essential to interoperability or architecture.

Based on the assessment of Nepal's current environment, estimation of future requirements, and leading practices of Government Interoperability Framework of the various countries, the following key principles have been suggested for NeGIF:

a. Interoperability:

The basic premise of this principle is to ensure that policies should reinforce and standards selected should facilitate interoperability by:

- eliminating patchwork of ICT solutions in different government offices those are unable to 'talk' or exchange data
- bringing in the ability to effectively interconnect, collaborate, access and facilitate data integration in order to communicate between different government organizations (G2G, G2C, and G2B etc.).

b. Share, Re-Use and Collaborate

This principle propagates sharing, re-use and collaboration and essentially highlights the importance of:

- Identifying common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and defining policies, standards, and procedures to ensure reusability of artifacts. For e.g. defining data structure, data sets at a national level etc.
- Choosing standards that will enable more choice and reduce the administrative burden.

c. **Scalability**

The principle suggests that the standards chosen should meet the changing and growing ministry and agency's needs and requirements and the applications and technologies should essentially scale up, adapt and respond to such requirement changes and demand fluctuations. Thus the maintenance and development of standards are a key element in the choice of such standards.

d. Confidentiality

Despite its considerable benefits, interoperability does have some potentially negative side-effects if privacy is compromised. Guaranteeing the privacy of information with regard to citizens (e.g. health records), business (e.g. organization statistics) and government (e.g. confidentiality agreements) can help to enforce the legally-defined restrictions on access & dissemination of information. This will ensure that the confidential information and data are properly classified and adequately protected. Privacy cannot be guaranteed by technical standards alone, it has to have process, inter-organisational agreements, cyber laws etc. in place to enforce it. However fundamental tenet of this is to protect the integrity of government information and information held by various agencies.

e. Adherence to open standards

Adherence to standard that will provide for choice of vendor will promote competitiveness and opportunity to look at cross platforms. The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are what will allow for sustainable information exchange, interoperability and flexibility.

Open standards could include open source as well but it is not necessary that all open standards are open source. Open source will suit few areas like server end products, Operating systems, Integrated Development

Environment etc. It may not be appropriate to have open source enterprise application to be pervasive in government; also Open source is not free in totality. Open Source Initiatives (http://www.opensource.org) have defined the criteria to be met by any software to become an open source software. While selecting standards, open source can be considered ensuring adequate support and training.

The crux of this principle is to ensure that the standards chosen are Open standards. Certain exemption to choice of open standards can be considered due to the following factors influencing the decision towards proprietary:

- excessive user base of proprietary applications/product which makes migration to new open standards difficult in the short term. Gradual discontinuation of old proprietary technology should be considered
- market leadership of a product which dominates the market which through its favourable prices bracket and availability of skilled resources could influence the decision towards open standards
- less competitive choices available in open standards may make the decision in favour of proprietary standards.

However we recommend putting in place a suitable approval mechanism for use of such proprietary standards.

5.4 Policies

Technology standards and policies establish direction and technical requirements which govern the acquisition, use and management of IT resources for the IT initiatives undertaken by the ministries. Overall the policies give direction and guidelines to successfully implement, maintain and govern eGIF. The success of the initiative depends on the enforcement of these policies along with the standards. Each policy is based on or aid one or more of the principles. They ensure that principles on which eGIF is based are achieved and they can be qualitatively assessed for compliance or adherence.

Policies should apply to all the initiatives of the ministries with exceptions. The governing body must ensure access to the standards and policies so that ministries and vendors are aware of the required standards. The ministries should refer to these standards and policies when planning or making changes to their IT landscape. Standards and policies will have to be regularly reviewed to keep them up to date with the latest technology developments.

The following are some key policies covering various aspects of NeGIF which are to be followed to make this initiative a perennial success. These policies are based on increasing the e-Readiness in Nepal which will trigger effective usage of ICT and in turn effective e-Governance. These policies include both organizational level policies and even those relating to different technical standard areas.

a. Overall Policies

- Adopt objective, principles, policies and standards as a respective ministry/agency's policies and institutionalize the same across all government departments through passing a mandate in the cabinet/parliament.
- All selected standards should be based on the objective, scope and principles of NeGIF.
- Any policy and standard defined in NeGIF should be consistent and compliant with the existing Government policies and standards wherever relevant. Existing published Government policies and standards that are relevant to be observed and complied as of now are Language localization, Digitization standards, local language key board layout standard and transliteration standard.

- The use of open standards should be given preference over proprietary standards wherever appropriate. In the event of choosing proprietary standards the NeGIF principles should be considered as the basic requirement.
- The institution-based approach should be replaced by a service-center one closely aligned with e-Governance strategy and adherence to the eGIF should be mandated throughout all government ministries, agencies and authorities.
- In case of private public partnership, the standards for information exchange between the private partner and the government should comply with the NeGIFv1.0 but flexibility may be allowed in the information exchange between the partner and the distribution network of the partner reaching the citizens/consumers.
- Whenever a new version of NeGIF is released or enhanced/revised, it is mandatory to train the working group committee members who should in turn be mandated to train the concerned/identified IT resource in each government department across all ministries/agencies/authorities.
- All ministries/agencies /departments should review their technology implementations with the NeGIF, whenever:
    - a new/enhanced /revised version of the eGIF is released
    - they are looking out for new implementations, upgrade of older systems and reviewing their e-Governance/e- Services strategy.
- All ministries/agencies /authorities should recommend compliance to NeGIF in their bidding process for any technology product/service procurement.
- All standards should first apply to new systems and then move on to incorporate older systems.
- The systems in each ministry/agency that are built to support a given access device should comply with the specification given in the NeGIF standards.
- Going forward the eGIF working groups should be responsible for the development and evolution of eGIF standards and HLCIT should ensure the adoption of the standards.
- HLCIT to put in place a process in such a way that no IT investment should be made without an approved architecture and compliance to eGIF.

b. Application and Technology Policies

- The standards should as far as possible be aligned with the World Wide Web for all public sector information systems.
- The development of applications or e-Services should provide services to the users who do not have the access to latest technologies and to those who may not be aware of using such technologies.
- While developing applications, special accessibility needs have to be considered including the provision of more sophisticated and user-specific resources.
- Current applications may not need to comply immediately with NeGIF, however, any new information system/change/upgrade must be compliant. A given version of eGIF should apply over the lifecycle of a specific, discrete system. It is desirable to move upgrade/re-engineer the system up to the most recent version of the framework. In case it is not possible to comply, an appeal for exemption must be approved by the Governing council. The exemption can be only on the following grounds:

  - a current standard that is going to be interoperating with another agency does not comply with the eGIF
  - there is no suitable open or accepted standard for a new system that is proposed
  - the current version of the eGIF cannot meet a ministry/agency's requirements
  - an alternative approach to achieving interoperability has been agreed amongst all the parties exchanging data and a change is requested in the specification/requirement as an amendment.

- All future application and migration of legacy application should be web based(browser based interface).
- Email communication should be recognized as the official communication and Email should be the preferred medium of official communication.

c. Data and Meta data Policies

- XML should be the primary standard for data integration and data management for all application in every ministry, agency and authority in Nepal. The Nepal Meta data standards should be primarily based on the international Dublin Core model (ISO 15836).
- Development of national level data set and centralization of Meta data of the country should be done in compliance with the interoperability standards on meta data.
- The working groups and experts should develop guidelines for XML Schemas that will be used for all new applications. These guidelines should include mandatory requirements for XML Schema structure and content.
- Data standards, data exchange standards, integration standards are interrelated, their compatibility and technical requirements should be considered.

d. Security Policies

- In order to ensure:
  - Confidentiality/privacy of Nepal government held information
  - to continue to exercise control of Nepal government data and computing environments
  - Protect confidentiality rights accorded to personnels who use government systems
  - Ensure privacy of personal information.

  Nepal should have process, principles, policies, technology and control mechanism to achieve fair maturity in Trusted Computing and Digital Rights Management (DRM).
- Security is a process that should be present at all stages of application development, the security working group should document systems, security controls, and the environment topologies, educate every ministry/agency IT department on their responsibilities for the security and the correct use of the access means and update policy and procedures
- The security requirements for the information, the services, and the infrastructure should be identified and treated in accordance to the type of information, SLA's, and the outcome of the risk analysis.
- To start with, internal network security policy should be enforced across all ministries. The policy document should be updated and maintained eventually. Concerned authority should also set out a

framework to assure the availability, integrity and confidentiality of e-Government services, specifically lay out procedures for identity registration, enrollment and authentication processes which are important for citizens to access e-Service. Adding to that, key procedures pertaining to the following areas should be implemented and enforced.

  - Application Acquisition, Development and Maintenance Procedure
  - Audit Logging Procedure Version
  - Backup and Restore Management
  - Capacity Management
  - Change Management
  - Incident Management Procedure
  - Information Labelling and Handling
  - Physical Access Process
  - Physical Access To Secure Areas Process
  - Physical Zoning Guidelines
  - Risk Assessment Methodology
  - User account management.

- The security policies, procedures and standards should be enforced to protect the privacy of data. Suitable media should be used to store/transport/process in providing the adequate level of protection needed.

e. Data Protection Policies

- Data-protection policy and process should be in place before introduction of any smart card scheme. The policy should clearly highlight the requirements, the roles and responsibility of all parties involved (card issuer, application developer, authority etc.) in the smart card
- Data must be controlled, defined and have integrity so that they are fit for the purpose for which it was collected/collated. Data should be created into a one institutionalized data source once and maintain. Then using it several times for different purposes becomes easier
- Whenever data and information flows into or out of critical systems (to be defined by each ministry) the agency should ensure they monitor:
  - such flow whenever they occur,
  - the content of the information transmitted,
  - the purpose of such information/data flow,
  - parties involved in exchange and collection of such information
  - for how long the information is going to be held and under what circumstances.

To reap the benefit of eGIF, effective use of the standards, policies and governance mechanism is crucial.

6. NeGIF Technical Standards

6. NeGIF Technical Standards

It is to be noted that the NeGIF technical standards provided in this section and the subsequent sub-sections are the general standards adopted by countries world-wide as necessary. However it is advisable for Govt. of Nepal to adopt these standards judiciously on a case-by-case basic wherever applicable and permitted based on legal validity of the standard in the country.

Use of these standards will bring Leading Practices, Interoperability, reuse and collaboration to bear upon e-Governance efforts to develop and deploy services.

These standards are chosen from internationally available and accessible standards which are widely in use. ICT Products are designed and developed in conformity with the standards. Since eGIF is aimed to facilitate the ability of government organisations to share information and to integrate information and business processes it is quintessential to agree to use common standards.

It should be noted that these standards evolve as innovations drive new technologies, products and improvements to existing products (e.g. IPv4, IPv6). Interoperability Framework sets out the government's guidelines, standards, policies and technical specifications describing the way in which government ministries/departments can link their business processes and deliver 'joined-up' services.

There must be a mandatory compliance with the accepted standard, interface and architecture at all levels to be interoperable, so that data and information can be exchanged and processed seamlessly across government. The framework should cover policies and standards for achieving technical, semantic, and syntactical process interoperability.

Moreover, incompatible data at different departments will hinder government efforts to detect fraud. It is also found that the benefits of e-Governance initiatives within an isolated department are sub-optimal and finally result in no substantial speed or efficiency gain.

There are nine technical standards areas namely Interconnection, Data Integration, Access, Collaboration, Application Design and Development, Application Integration, System Standards, Meta Data and Security identified under NeGIF v1.0. The nine areas were identified based on the:

- As-Is assessment wherein the baseline technologies of various ministries / agencies were studied, and the contextual requirements were analysed
- Understanding of maturity level and transformational values of existing and emerging technologies through technology trends by leading analyst, PwC technology research reports etc.
- Leading practice review to get an idea of the leading practice industry standards
- Information on Standards organisation such as W3C, Dublin core, ISO etc.

The structure of the standards for NeGIF is given below:

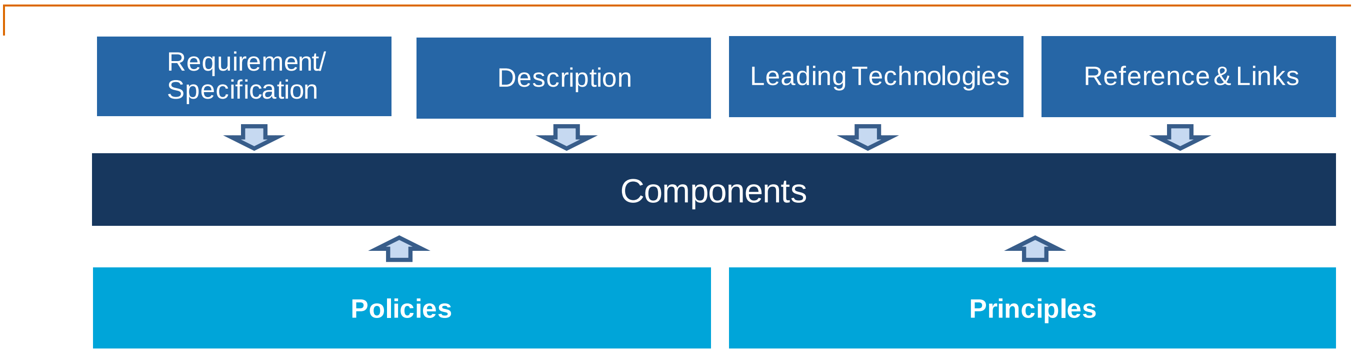


Figure 6-1: Structure of NeGIF Standards

- Principles would serve as guidelines selection and recommendation of standards.
- Policies will act as the enforcement guidelines for implementing these standards.
- Standards table for each technical area. The standards table will have many 'Components'. Each component will have:
    - One or more requirement/specification that needs to be followed to ensure interoperability.
    - These requirement /specification can be mandatory or Recommendatory. Requirements/specification that uses words such as should, shall and will is construed as mandatory. Requirements/specification that uses words such as may and can is construed as Recommendatory.
    - Based on the baseline information collected during the As-Is phase the status of the standard's adoption is indicated, whether the standards are currently Adopted, Partially Adopted or Not Adopted.
    - The standards table briefly represents the standards/requirements/ status and enforcement rules. For additional information on each component/standard, the details of the standards with resource locator (source) to the relevant standard are provided in a section below. However the hyperlinks for the detailed standards/requirement for each component are provided in the Reference and Links column in the standards table.

The brief overview of the nine technical areas and the respective components are given below.

Table 6-1: Technical Areas

Technical Areas	Components
Interconnection	- Interconnection –Telecom • Access Transmission Network • Fixed Line Next Generation Network • Next Generation Mobile Network Standards - Interconnection- Enterprise • Physical Layer Infrastructure • Application Layer Protocols • Transport Layer Protocols

Technical Areas	Components
	• Internet Layer Protocols • Link Layer Protocols - Interconnection- Integrated (Telecom + Enterprise) • Internet Service Provider Standards • Financial Interconnectivity System Standards
Data Integration	• Character and encoding for information interchange • Data description • Data exchange & Transformation • Data exchange Formats • Ontology-based information exchange • Data modelling language • Data integration meta language • Minimum interoperable character set • Digitization • Data Definition for Smart Cards
Security	• Access management • Anti Spam • Anti Virus/Anti Spyware • Desktop Firewall • Digital Signature • Email Security • Encryption Algorithm • Enterprise Firewall • Identity , Authentication , authorization and privacy • Identity management • Intrusion detection and prevention • IP Encapsulation security • IP security • Layer 2 Security • Proxy server • Public key infrastructure • Remote Security • Secure transport • VPN • XML security standards • Physical Security
Access	• Access Token • Animation • Compression • Kiosk • Mobile devices • Scripting • Smart Card • Directory Access • Web Access standard • Web browser • Work stations
Collaboration	• Email System

Technical Areas	Components
	• Enterprise Content Management • IP Telephony • Video Conferencing
Application Design & Development	• Application Development For Handheld Devices • Application development framework • Business Rules, Logic and Objects • Commercial, off-the-shelf applications(COTS) • Geographic information system • Modeling design and development • Programming language for Application Development • Reporting tools • Software configurations Management (SCM • Service Oriented Architecture • Smart Card Applications
Application Integration	• Message oriented Middleware • Object request brokers • Remote procedure calls
System Standards	• Application Servers • Backup Recovery • Business Intelligence • DB Connectivity and access technology • DBMS • Desktop O/S • Directory Services • Hardware Platforms • IT Operations Management • Mobile O/S • Portal servers • Server O/S • Storage Devices • Web Server
Specification for specific business areas	• Finance • Workflow and Web Services • e-Health • e-Learning • Legal • HR • E-News

The Standards table of nine technical areas of interoperability is given below followed by the standards catalogue table.

6.1 Interconnection

Interconnection covers interoperability components/infrastructure and technical specifications required to enable communication between different systems and the exchange of information over the networking environment. Interconnection is used when governmental organizations each have their own clients and must interconnect with other governmental organization to provide a comprehensive service. Based on our deep study of the projects in Nepal, the interconnection standard is vital for successful interoperability among the different governmental organizations.

This section describes the way in which the interconnection part of eGIF is organized and how to find the elements. Based on the country's specific current and future need, we have segmented the interconnection standards into the following standard areas: telecom level, enterprise level, and integrated system.

Telecom Level is further divided into three major sections for interconnection:

1. Access Transmission Network Standard
2. Fixed Line Next-Generation Network Standard (FL-NGN)
3. 2nd and 3rd Generation Mobile Network Standard

Enterprise Level is further divided into three major sections for interconnectivity:

1. Physical Infrastructure Layer Standard
2. Enterprise Level IP Network Layer Standard
3. Protocol Layer Standard

Integrated System is further divided into two areas:

1. Internet Service Providers Standard
2. Financial Services Connectivity Standards.

We also organize the document in to two formats for easy access to elements and readability: the first part provides the summary of all interconnection standards with table format and the second part provides the details of the standard with link for further access. Since Nepal is going under major construction of backbone network for interconnection, it is a must to have a set of standards for interconnection. Therefore, we have identified key challenges and recommendatory relevant standards specifically for areas requiring attention for interoperability in Nepal.

Table 6-2: Interconnection-Telecom

Interconnection- Telecom			
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Interconnection – Telecom Technical Standard Details**	**Kindly mention where / which standard is this adopted from. This column may be inserted for all these similar tables**
Access Transmission Network			
Coarse Wave Division Multiplexing (CWDM) should be the standard for transmitting multiple wavelength signals through the same fiber optic cable.	Mandatory	4.1.1.1.1 CWDM	e.g. ITU / W3C etc,
FTTB (Fiber To The Building), FTTH (Fiber To The Home), FTTD (Fiber To The Desk) should be the stand for RING topology with Failover/Auto-Recovery function	Recommendatory	4.1.1.1.2 FTTx	
Fixed Line Next Generation Network			
ADSL2 should be the standard to	Mandatory	4.1.1.2.2 ADSL2+	

Interconnection- Telecom			
address the bandwidth increase. ADSL2+ should be considered in near future			
VDSL2 can be the standard for HDTV, VoD, VC, high speed Internet access and advanced voice services including over a standard copper telephone cable.	Recommendatory	4.1.1.2.3 VDSL2	
Passive optical network (PON) should be the standard to enable a single optical fiber to serve multiple premises.	Mandatory	4.1.1.2.4 xPON	
WiMAX can be considered for wireless broadband voice, data and video transfer at large distances.	Recommendatory	4.1.1.2.5 WiMAX	
Next Generation Mobile Network Standards			
Mobile Broadband should be the standard followed for a range of data applications.	Mandatory	4.1.1.3.1 GSM/WCDMA-HSPA+	
CDMA2000 1X (IS-2000 - also known as 1x and 1xRTT) can be the core CDMA2000 wireless air interface standard.	Mandatory	4.1.1.3.2 CDMA 1x	
CDMA2000 1xEV-DO (Evolution-Data Optimized), often abbreviated as EV-DO should be the telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access.	Mandatory	4.1.1.3.3 CDMA 1x EV-DO	

6.1.1 Telecom Level Access Network Infrastructure Standards

6.1.1.1 Access Transmission Network

6.1.1.1.1 Access Layer – CWDM

Description:

Coarse Wave Division Multiplexing (CWDM) enables Service Providers to maximize existing fiber optic infrastructure by transmitting multiple wavelength signals through the same fiber optic cable. CWDM technology enables a dual fiber strand to support multiple network topologies and data rates to exponentially increase bandwidth capacity and provide the ability to add new customers without laying new fiber optic cable between sites. Coarse wavelength division multiplexing (CWDM) is a method of combining multiple signals on laser beams at various wavelengths for transmission along fiber optic cables, such that the number of channels is fewer than in dense wavelength division is multiplexing (DWDM) but more than in standard wavelength division multiplexing (WDM). CWDM systems have channels at wavelengths spaced 20 nanometers (nm) apart, compared with 0.4 nm spacing for DWDM. This allows the use of low-cost, uncooled lasers for CWDM. In a typical CWDM system, laser emissions occur on eight channels at eight defined wavelengths: 1610 nm, 1590 nm, 1570 nm, 1550 nm, 1530 nm, 1510 nm, 1490 nm, and 1470 nm. But up to 18 different channels are allowed, with wavelengths ranging down to 1270 nm.

Standards Details:

- The wavelengths used with CWDM implementations are defined by the International Telecommunications Union; reference ITU G.694.2, listing eighteen wavelengths from 1270nm to 1610nm with 20nm wavelength spacing. The ITU G.694.2 recommendation provides a grid of wavelengths (20-nm channel spacing) for target distance of up to 50 km on single-mode fibers.
- Due to different number of channels, CWDM and DWDM may have an issues with interconnect metro (CWDM) and national backbone (DWDM) network of 10Gbps or higher bandwidth.
- It is Recommendatory to use the common channels between CWDM and DWDM for 10Gbps or higher connectivity.

Resource Locator:

- CWDM

  http://www.itu.int/itudoc/itu-t/aap/sg15aap/history/g.694.2/index.html

6.1.1.1.2 FTTx (FTTB, FTTH, FTTD)

Description:

FTTB (Fiber to the Building), FTTH (Fiber to the Home), FTTD (Fiber to the Desk) is a new generation network structure in RING topology with Failover/Auto-Recovery function. If there is a failover in some node/segment in this Ring, this network platform will auto switchover to another direction. Besides, with Ethernet technique to build FTTB network, the cost of connecting the applicant `s equipment to the FTTB network will significantly decrease.

The advantages of Fiber media to replace copper twisted-pair wiring are: higher connection quality prevents cross-talk simpler network topology, less connection Failure. Lack of CPE with fiber interface in the country may be a challenge.

Standards Details:

- ITU-T's Study Group 15 has fast tracked a standard that significantly reduces costs for operators rolling out fiber to the home (FTTH). The new Recommendation G.657 "Characteristics of a Bending Loss Insensitive Single Mode Optical Fibers and Cables for the Access Network" gives fiber optic cable similarly flexible characteristics to copper meaning that it can be much more easily deployed in the street, in the building and in the home.
- FTTH/FTTB is the latest technology to reach last mile connectivity. It is Recommendatory to introduce CPE that has fiber interface for end users.

6.1.1.2 Fixed Line Next-Generation Network (FL-NGN)

6.1.1.2.1 Multi Service Access Gateway Standards

The figure below shows the relation between the application demand and the access network capacity based on the required standards.

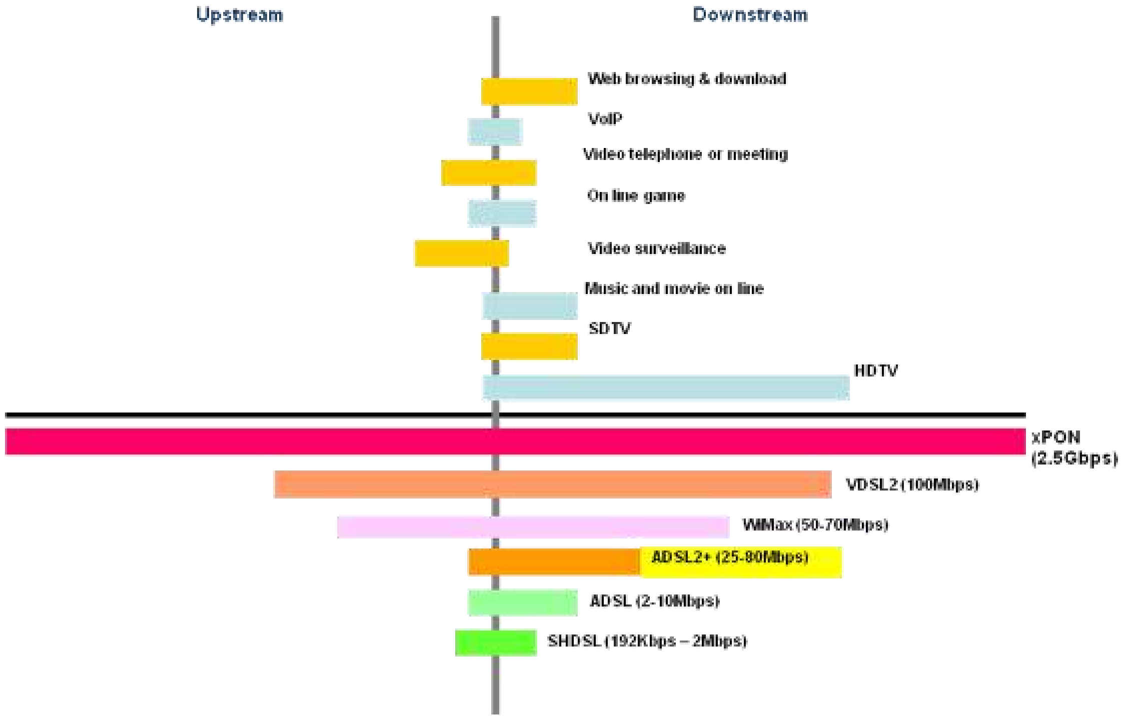


Figure 6-2: *Relation between Application Demand and Access Network Capacity*

6.1.1.2.2 ADSL 2+

Description:

ADSL2 addresses the growing demand for bandwidth to support services such as video. The new ADSL2 and ADSL2+ gear will interoperate with existing ADSL equipment, allowing carriers to roll out new high-speed services while gradually upgrading their legacy infrastructure.

Standard Details:

The ITU accepted the ADSL2 standard in July 2002 and the ADSL2+ standard in January 2003. The ADSL2 standard (ITU G.992.3) adds new features and functions targeted at improving ADSL performance and interoperability. In addition, the standard adds support for new applications, services, and deployment scenarios. Among the changes are improvements in data rate and reach performance, rate adaptation, improved diagnostics, and power enhancements. The conventional ADSL standard (ITU G.992.1) provides downstream data rates of up to 8 Mbps and upstream data rates of up to 0.8 Mbps, and ADSL2 provides higher downstream rates of up to 12 Mbps and upstream data rates of up to 1 Mbps. The ADSL2+ standard (ITU G.992.5) doubles the bandwidth used for downstream data transmission, effectively doubling the maximum downstream data rates, and achieving downstream data rates of up to 24 Mbps and upstream data rates of up to 1.5 Mbps. The exact data rates vary depending on the distance from the DSL access multiplexer (DSLAM), DSLAM type, line card and chipset, and firmware, noise profile, quality of copper, etc. The reach-extended ADSL2 standard (G.992.3) increases performance on loop lengths greater than 16,000 feet from the Central Office. The standard for G.992.3 (ADSL2) and G.992.5 (ADSL2+) was consented at the October 2003. The standard for G.992.3 (ADSL2) and G.992.5 (ADSL2+) contains PSD Masks for new ADSL2 service over POTS that increases the upstream data rates by doubling the number of tones to 64. As a result, the standard provides higher upload speeds for users by doubling the upstream data rate under certain loop and noise conditions.

Resource Locator:

- ADSL (ITU G.992.2)

http://www.itu.int/rec/T-REC-G.992.2/en

- ADSL2+ (ITU G.992.5)

  http://www.itu.int/rec/T-REC-G.992.5/en

6.1.1.2.3 VDSL2

Description:

The ITU-T Recommendation for very-high-bit-rate digital subscriber line 2 (VDSL2) will allow operators worldwide to compete with cable and satellite operators by offering services such as high definition TV (HDTV), video-on-demand, videoconferencing, high speed Internet access and advanced voice services including VoIP, over a standard copper telephone cable. VDSL2 will offer consumers up to 100 Mbps up and downstream, a massive ten-fold increase over the more common ADSL. Essentially it allows so-called 'fiber-extension' bringing fiber like bandwidth to premises not directly connected to the fiber-optic segment of a telecoms company's network. As well as addressing increasing consumer demands, VDSL2 offers telecom carriers a solution that promises to be interoperable with the ADSL kit that many operators already have in place. This interoperability will make the migration of customers to VDSL2 much simpler. Another important feature of VDSL2 is that it will work in both legacy ATM networks and next generation IP based networks.

Standard Details:

Meeting in Geneva, the ITU's standards group 15 (ITU-SG15) consented to Amendment 1 to the VDSL2 (ITU-G.993.2) standard. This amendment enhances the functionality of VDSL2 and gives it added flexibility to service both business and residential applications on both short and long loops. The additional functionality is achieved through newly-defined flexible band plans that allow the modem to be configured for either asymmetric or symmetric rate services. "With this new functionality, VDSL2 is now positioned as the highest-performance, most flexible universal DSL.

Resource Locator:

- VDSL2 (ITU-T G.993.1)

  http://www.itu.int/rec/T-REC-G.993.1/en

6.1.1.2.4 xPON

Description:

A description of the PON-based broadband access network technology that uses fiber optics running all the way from the Internet backbone to the office, home or premises. Sometimes other acronyms, FTTx, FTTP, or FTTB are used, but these are essentially interchangeable. FTTH is becoming the catch-all descriptor for all fiber to the home, premises, governmental offices, business offices and "x" technologies. The leading FTTH technology is PON or Passive Optical Network technology. This approach differs from most of the telecommunications networks in place today by featuring "passive" operation. Active networks like DSL, VDSL and cable have active components in the network backbone equipment, in the central office, in the neighbourhood network infrastructure, and in the customer premises equipment. PONs has only passive light transmission components in the neighbourhood infrastructure with active components only in the central office and the customer premises equipment.

BPON suffers from the very aggressive optical timing of ATM and the high complexity of the ATM transport layer. ATM-based FTTH solutions face the problems posed by the provisioning (requires ATM-based central office equipment), complexity (in timing requirements and protocol complexity) and subsequent cost of components. This cost is exacerbated by the relatively small market for traditional ATM equipment used in the backbone telecommunications network.

Standards details:

- These represent three flavours of PON technology. APON and BPON are the same specification which is commonly referred to as BPON. BPON is the oldest PON standard, defined in the mid-1990s and while there is an installed base of BPON, most of the new market deployment focus is now on EPON/GE-PON. GE-PON and EPON are different names for the same specification, which is defined by the IEEE 802.3ah Ethernet in the First Mile standard ratified in June 2004. This is the current standardized high-volume solution for gigabit PON technologies. GPON is now being standardized as the ITU-T G.984 recommendation and is receiving interest in North America and elsewhere, but with no final standard. GPON devices have just been announced, and there is no volume deployment as yet. One important distinction between the standards is operational speed. Another key distinction is the protocol support for transport of data packets between access network equipment.

Table 60-3: *PON-based broadband access network technology*

	TECHNOLOGY		
ATTRIBUTES	**BPON (APON)**	**GE-PON (EPON)**	**GPON**
Speed - Upstream/Downstream	155/622 Mbps	1.0/1.0 Gbps	1.25/2.5 Gbps
Native Protocol	ATM	Ethernet	GEM
Complexity	High	Low	High
Cost	High	Low	Undetermined
Standards Body	ITU-T	IEEE	ITU-T
Standard Complete	Yes, 1995	Yes, 2004	No
Volume Deployment	Yes, in 100,000s	Yes, in 1,000,000s	No
Primary Deployment Area	North America	Asia	Not applicable

- GE-PON or Ethernet in the First Mile has been ratified as the IEEE 802.3ah EFM standard and is already widely deployed in other parts of the world such as Asia. It uses Ethernet as its native protocol and simplifies timing and lowers costs by using symmetrical 1 Gbps data streams using standard 1Gbps Ethernet optical components. Like other Ethernet equipment found in the extended network, Ethernet-based FTTH equipment is much lower-cost relative to ATM-based equipment and the streamlined protocol support for an extended Ethernet protocol simplifies development. Therefore, it is Recommendatory going with GE-PON.

Resource Locator:

- EPON (IEEE 802.3av)

  http://www.ieee802.org/3/av/

- GPON (ITU-T G.984)

  http://www.pmc-sierra.com/ftth-pon/pon_standards.html

6.1.1.2.5 WiMAX

Description:

Worldwide Interoperability for Microwave Access- **W**iMAX is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access. WiMAX is a revolutionary technology for wireless broadband voice, data and video transfer at large distances. Based on the IEEE 802.16 standard, it received the name WiMAX by the WiMAX Forum in 2001, when it was found to provide communication, support and interoperability of the standard. The technology is suitable for building high-speed network, which is used to provide various services such as internet access, fixed telephone service, voice and data transfer, connection between offices, fax, urban and interurban virtual private networks, video information, multimedia applications, etc. The WiMAX services fulfill where the wired services such as LAN, cable modems, optics or DSL technology can't reach.

Standards details:

The IEEE 802.16 defines the wireless metropolitan area network (MAN) technology which is branded as WiMAX. The 802.16 includes two sets of standards, 802.16-2004 (802.16d) for fixed WiMAX and 802.16-2005(802.16e) for mobile WiMAX. The WiMAX wireless broadband access standard provides the missing link for the "last mile" connection in metropolitan area networks where DSL, Cable and other broadband access methods are not available or too expensive. WiMAX also offers an alternative to satellite Internet services for rural areas and allows mobility of the customer equipment.

The fixed WiMax standard IEEE 802.16-2004 (also known as 802.16d) is approved by the IEEE in June 2004, which provides fixed, point-to-multi point broadband wireless access service and its product profile utilizes the OFDM 256-FFT (Fast Fourier Transform) system profile. The fixed WiMAX 802.16-2004 standard supports both time division duplex (TDD) and frequency division duplex (FDD) services - the latter of which delivers full duplex transmission on the same signal if desired. In Dec. 2005, IEEE approved the mobile WiMax standard, the 802.16-2005 (also known as 802.16e). IEEE 802.16e, based on the early WiMax standard 802.16a, adds mobility features to WiMAX in the 2 to 11 GHz licensed bands. 802.16e allows for fixed wireless and mobile Non Line of Sight (NLOS) applications primarily by enhancing the OFDMA (Orthogonal Frequency Division Multiple Access).

IEEE 802.16 and WiMAX are designed as a complimentary technology to Wi-Fi and Bluetooth. The following table provides a quick comparison of 802.16 with to 802.11(WLAN) and 802.15.1 (Bluetooth):

Table 60-4: *WiMAX*

Parameters	IEEE802.16d (802.16-2004 Fixed WiMAX)	IEEE802.16e (802.16-2005 Mobile WiMAX)	802.11 (WLAN)	802.15.1 (Bluetooth)
Frequency Band:	2-66GHz	2 - 11GHz	2.4 – 5.8GHz	2.4GHz
Range	~31 miles	~31 miles	~100 meters	~10meters
Maximum Data rate:	~134 Mbps	~15 Mbps	~55 Mbps	~3Mbps
Number of users:	Thousands	Thousands	Dozens	Dozens

It is recommendatory to use WiMAX for area that are hard to reach with fixed line as well as business that demand higher bandwidth than CDMA 1x EV-DO connectivity.

6.1.1.3 Next-Generation Mobile Network Standards

6.1.1.3.1 GSM/WCDMA-HSPA+ Network

Description:

A simple explanation for Mobile Broadband is that it is like having your fixed home broadband experience delivered to your mobile device. Mobile Broadband rivals the performance of fixed broadband technologies and is suitable for a broad range of data applications – including accessing email with attachments, web browsing, multimedia streaming and file downloads – while stationary or on the go.

The last 18 months have seen a huge upswing in the adoption of mobile broadband globally, especially relating to PC connectivity through 3G USB "dongles", as well as high-end smart phones like the Apple iPhone™. There are several technologies competing to deliver commercial Mobile Broadband services. By far the most successful is HSPA, which has been commercially deployed by over 250 operators in more than 100 countries.

By 2010, when the number of wireless broadband connections is estimated to reach more than 600 million, HSPA will be the technology behind over 70 percent of Mobile Broadband connections. HSPA is a state-of-the art technology that provides mobile and wireless broadband services for the vast majority of the market, with unsurpassed performance and economies of scale.

The arrival of Mobile Broadband has prompted PC notebook manufacturers to embed cellular modems into their products, as they have done with Bluetooth®. Previous 2G and 2.5G mobile technologies were simply not fast or efficient enough to justify being embedded into notebooks. The GSMA designed the Mobile Broadband Enabled Service Mark to simplify customer communication by quickly and easily conveying to consumers that their devices are Mobile Broadband Enabled.

To date, over 1,600 HSPA devices have been launched globally. These devices initially included conventional mobile phones, PC Cards and Express Cards and USB 'dongles'. As device vendors have embraced the technology further we now feature a range of embedded notebooks and consumer electronics.

Mobile Broadband enabled devices are now proliferating the market, supporting a vast range of consumer and industry applications. These devices are being used to deliver solutions to people and industry in metropolitan and rural areas to a range of sectors including consumer electronics, clean technology, health care, transportation and utilities. The GSMA Embedded Mobile initiative is a GSMA market-development programme designed to accelerate the adoption of wireless connectivity across these sectors. In order for operators to deliver the Mobile Broadband connectivity that delivers feature rich applications to consumers and industry it is crucial that they can innovate in a defined and stable environment, confident in the security of spectrum allocations. The GSMA actively lobbies governments to fairly allocate spectrum to operators – including spectrum that has been freed up by the Digital Dividend.

Even though the GSM mobile core networks support 3G application, the majority mobile access networks are 2G based base station. This will limit the upgrade capability to HSPA+.

Standards details:

The first step required to upgrade WCDMA to HSPA is to improve the downlink by introducing HSDPA. The improved downlink provides up to 14 Mbit/s with significantly reduced latency. The channel reduces the cost per bit and enhances support for high-performance packet data applications. HSDPA is based on shared channel transmission and its key features are shared channel and multi-code transmission, higher-order modulation, short Transmission Time Interval (TTI), fast link adaptation and scheduling along with fast hybrid Automatic Repeat request (ARQ).

The second major step in the WCDMA upgrade process is to upgrade the uplink, which is introduced in 3GPP Release 6. Upgrading to HSUPA is often only a software update. Enhanced Uplink adds a new transport channel to WCDMA, called Enhanced Dedicated Channel (E-DCH). An enhanced uplink creates opportunities for a number of new applications including VoIP, uploading pictures and sending large e-mails. The enhanced uplink increases the data rate (up to 5.8 Mbit/s), and the capacity, and also reduces latency. The enhanced uplink features several improvements similar to those of HSDPA, such as multi code transmission, short Transmission Time Interval (TTI), fast scheduling and fast hybrid Automatic Repeat Request (ARQ).

Evolved HSPA (also known as: HSPA Evolution, HSPA+, I-HSPA or Internet HSPA) is an upcoming wireless broadband standard defined in 3GPP release 7 and 8 of the WCDMA specification. Evolved HSPA provides data rates up to 42 Mbit/s in the downlink and 11 Mbit/s in the uplink (per 5MHz carrier) with multiple input, multiple output (MIMO) technologies and higher order modulation.

It is Recommendatory to use 3G mobile access radio such as WCDMA as much as possible in order to elevate the limitation of upgrading to HSPA without significant upgrading cost.

Resource Locator:

- GSM/WCDMA-HSPA+ Network

  http://www.3gpp.org/

6.1.1.3.2 CDMA 1x Network

Description:

CDMA2000 1X (IS-2000), also known as 1x and 1xRTT, is the core CDMA2000 wireless air interface standard. The designation "1x", meaning 1 times Radio Transmission Technology, indicates the same RF bandwidth as IS-95: a duplex pair of 1.25 MHz radio channels. 1xRTT almost doubles the capacity of IS-95 by adding 64 more traffic channels to the forward link, orthogonal to (in quadrature with) the original set of 64. The 1X standard supports packet data speeds of up to 153 kbps with real world data transmission averaging 60–100 kbps in most commercial applications. IMT-2000 also made changes to the data link layer for the greater use of data services, including medium and link access control protocols and QoS. The IS-95 data link layer only provided "best effort delivery" for data and circuit switched channel for voice (i.e., a voice frame once every 20 ms).

As these 1x technologies are deployed, the public safety community will realize benefits along with commercial and business users. Applications such as tele-medicine and video conferencing could greatly impact how emergency medical personnel perform duties on the scene. Also, high-speed data communications could allow for real-time video feeds to/from police vehicles, promoting officer safety. And finally, since 1x technology is CDMA based, if the public safety community uses 1x technology they will benefit from the inherent security associated with CDMA (i.e., low probability of detection and interception). The possibilities and applications for using wireless high-speed data to ensure the safety of the public are virtually endless.

Standards details:

CDMA2000 1x is a standard that aims to bring high data rate capabilities to wireless communication products. It supports both voice and 153 Kbps of data using the same bandwidth configuration as legacy IS-95A CDMA networks (i.e., 1.25 megahertz (MHz) channel bandwidth). IS-95A is the standard that outlines the protocol for cellular subscriber user/device mobility and uses CDMA as the air access technology

6.1.1.3.3 CDMA 1x EV-DO Network

6.1.1.3.3.1 CDMA 1x EV-DO Revo Network

Description:

CDMA2000 1xEV-DO (Evolution-Data Optimized), often abbreviated as EV-DO or EV, is a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiple access (TDMA) to maximize both individual user's throughput and the overall system throughput. It is standardized by 3rd Generation Partnership Project 2 (3GPP2) as part of the CDMA2000 family of standards and has been adopted by many mobile phone service providers around the world – particularly those previously employing CDMA networks. It is also used on the Globalstar satellite phone network.

Mobile communications have been expanding from voice services to data services as it evolves from the first-generation analog mobile communication through the second-generation digital mobile communication and to the third-generation CDMA2000 mobile communication.

CDMA2000 1xEV-DO Rev0 technology is a high performance and cost effective Internet solution for consumers and business professionals. It offers high speed, high capacity wireless Internet technology, which is compatible with CDMA networks and optimized for packet data services. CDMA2000 1xEV-DO Rev0 offers a combination of high performance and economic benefits, unprecedented in systems capable of providing portable, mobile, and fixed services. 1xEV-DO Rev0 achieves this performance with minimized network and spectrum resources to provide a highly spectrally efficient technology. CDMA2000 1xEV-DO Rev0 systems support interoperating with IS series channels (IS-95 series and IS-2000), and accordingly supports the backward compatibility for functions of the conventional systems including vocoding, low-speed data services, fax services, short message services (SMS), medium-speed data services and handoff. In addition, CDMA2000 1xEV-DO Rev0 systems are capable of supporting both voice and data services, and can efficiently be applied to future CDMA2000 1xEV-DO rA/rB/rC services.

Rev0 is the first version of CDMA 1x EV-DO technology with speed of up to 2.4MB.

Standard Details:

1xEV is an enhancement of the current CDMA technology, developed by QUALCOMM (i.e., the IS-856 TIA/EIA standard). 1xEV is a high-performance, cost-effective solution that offers high-speed, high-capacity wireless Internet access with minimal impact to network and spectrum resources. IS-856 is the standard that defines the 1x Technology, specifically for the 1x-DO, the high data rate, data-only derivative of 1x Technology.

Since the cost of hardware and software between Rev0 and RevA very minimal, it is Recommendatory to upgrade Rev0 to RevA

Resource Locator:

- CDMA 1x EVDO rev 0

  http://cdg.org/news/press/2009/Aug17_09.asp

6.1.1.3.3.2 CDMA 1x EV-DO RevA Network

Description:

The phenomenal growth of Information Technology and the Internet, and the general population desire for timely information services, create a need for a high performance wireless Internet technology. Trends such as PC-on-a-Chip, wireless-capable Personal Digital Assistants, Smart Phones and Auto PCs point to the availability of a large number of new data-capable devices, enabling each of us to communicate wirelessly anytime, anywhere. CDMA2000 1xEV-DO rA is the ideal technology for providing such wireless Internet services, and is founded on a proven wireless technology and solid economic foundation.

CDMA2000 1xEV-DO rA systems are designed to be highly interoperable with CDMA systems. Leveraging from the same RF characteristics as IS-95/1X CDMA, dual-mode IS-95/1X and CDMA2000 1xEV-DO rA Access

Terminals can be offered in a compact and cost-effective manner. Within a given network, dual-mode IS-95/1X and CDMA2000 1xEV-DO rA devices allow users to access voice services via the IS-95/1X frequency carrier, while receiving data services through the CDMA2000 1xEV-DO rA frequency carrier. Wireless subscribers will benefit from the excellent IS-95/1X voice quality, as well as CDMA2000 1xEV-DO rA high performance data services and mobile flexibility. CDMA2000 1xEV-DO rA systems support interoperating with IS series channels (IS-95 series and IS-2000), and accordingly supports the backward compatibility for functions of the conventional systems including vocoding, low-speed data services, fax services, short message services (SMS), medium-speed data services and handoff. In addition, CDMA2000 1xEV-DO rA systems are capable of supporting both voice and data services, and can efficiently be applied to future CDMA2000 1xEV-DO rB/rC services.

As of today, CDMA 1x is providing both data and voice at cellular level with higher bandwidth than GSM mobile network. But, the technologies continue to evolve in providing voice, video and data (triple play) with single mobile access. CDMA 1x will face this challenges in near future.

Standards details:

Make sure the current CDMA 1x core and access network is able to evolve to IMS or LTE without incurring additional cost or with minimal hardware/software upgrade in order to provide 4G services which is around the corner.

Resource Locator:

- CDMA 1x Rev A

  http://cdg.org/news/press/2009/Aug17_09.asp

Table 6-5: Interconnection-Enterprise

Interconnection- Enterprise		
Standards Proposed	**Mandatory/ Recommendatory**	**References & Links to Interconnection –Enterprise Technical Standards Details**
Physical Layer Infrastructure		
A 19-inch rack should be used for mounting multiple equipment modules.	Mandatory	4.1.2.1.1 Cabinet
Cat 6 or better should be used for physical infrastructure within a 100m length.	Mandatory	4.1.2.2.1 Cat6 or Better
Information outlet with Cat 6 or better should be used to terminate cables to end users.	Mandatory	4.1.2.2.2 Information outlet Keystones
A Copper patch panel with Cat 6 or better should be used for the termination of Copper cable connections	Mandatory	4.1.2.2.3 Copper Patch Panel
A Copper patch cord with Cat 6 or better cable should be used to connect circuits on a patch panel to switches or from outlets to end devices.	Mandatory	4.1.2.2.4 Copper Patch Cord
Fibre optic should be used for carrying data above 100m length.	Mandatory	4.1.2.3.1 Fiber optic cable
A fibre pigtail should be used to extend fibre optic cables or to terminate fibre core cables on fibre patch panel.	Mandatory	4.1.2.3.2 Fiber pigtail
A fiber patch panel should be used for distributing and rearranging fiber cable connections and circuits..	Mandatory	4.1.2.3.3 Fiber Patch Panel
A fiber patch cord should be used to attach one device to another for signal routing.	Mandatory	4.1.2.3.4 Fiber Patch Cord
A Data Centre should house computer systems and associated components, such as telecommunications and storage systems.	Mandatory	4.1.2.4.1 Main Data Centre
Disaster recovery process, policies and procedures should be planned for recovery or continuation of technology infrastructure.	Mandatory	4.1.2.4.2 Disaster recovery-Failover
Load Balancing can be considered to distribute workload evenly across two or more links in order to get optimal resource utilization, maximize throughput, minimize response time and avoid overload.	Recommendatory	4.1.2.4.2 Disaster Recovery-Load Balancing
Infrastructure of data center should include systems that are important for the safety of data center such as fire suppression, access control etc. that should be available in a data centre.	Mandatory	4.1.2.4.3 Infrastructure of Datacenter
Enterprise Level IP Network		
All IT equipments should be IPv6 Compatible.	Recommendatory	4.1.2.5 Enterprise Level IP Network
Application Layer Protocols		

Interconnection- Enterprise		
Border Gateway Protocol should be used as the core routing protocol of the internet.	Mandatory	4.1.2.6.1 BGP
DNS should be used for resolution of names that locate computers assigned with IP addresses.	Mandatory	4.1.2.6.2 DNS
DHCP should be used by devices (DHCP clients) to obtain configuration information for operation in a network dynamically.	Mandatory	4.1.2.6.3 DHCP
File Transfer Protocol (FTP) should be used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet.	Mandatory	4.1.2.6.4 FTP
FTPS should be used for exchanging and manipulating files over internet securely.	Mandatory	4.1.2.6.5 FTPS
GPRS Tunneling Protocol (GTP) can be considered to carry General Packet Radio Service (GPRS) within GSM and UMTS networks.	Recommendatory	4.1.2.6.6 GTP
Hypertext Transfer Protocol (HTTP) should be used to distribute and collaborate, hypermedia information systems.	Mandatory	4.1.2.6.7 HTTP
HTTPS should be used to distribute and collaborate hypermedia information systems securely.	Mandatory	4.1.2.6.8 HTTPS
IMAP should be used for accessing mailboxes.	Mandatory	4.1.2.6.9 IMAP
Internet Relay Chat (IRC) can be considered for the use of real-time Internet text messaging or synchronous conferencing.	Recommendatory	4.1.2.6.10 IRC
Light Weight Directory Access Protocol should be used for querying and modifying directory services running over TCP/IP.	Mandatory	4.1.2.6.11 LDAP
Megaco (H.248) can be considered for controlling Media Gateways on IP networks and the public switched telephone network (PSTN).	Recommendatory	4.1.2.6.12 Megaco
Media Gateway Control Protocol can be considered for controlling media controllers on IP and telephone Networks similarly as Megaco.	Recommendatory	4.1.2.6.13MGCP
MIME (Multipurpose Internet Mail Extensions) should be used for formatting non-ASCII messages so that they can be sent over the Internet.	Mandatory	4.1.2.6.14 MIME
The multiprotocol BGP can be considered to enable multicast routing policy within and between BGP autonomous systems because it adds features to BGP.	Recommendatory	4.1.2.6.15 MP-BGP
Simple Network Management Protocol (SNMP) should be used to monitor network systems and network-attached devices for conditions that warrant administrative attention.	Mandatory	4.1.2.6.16 Network Management-SNMP
The Network News Transfer Protocol (NNTP) can be used for transporting Usenet news articles between	Recommendatory	4.1.2.6.17 NNTP

Interconnection- Enterprise		
servers.		
The Network Time Protocol (NTP) should be used for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.	Mandatory	4.1.2.6.18 NTP
POP (Post Office Protocol) should be used to retrieve e-mail from a mail server.	Mandatory	4.1.2.6.19 POP
The Routing Information Protocol (RIP) should be used to route packets in local and wide area networks.	Mandatory	4.1.2.6.20 RIP
RPC can be used to execute procedures in another address.	Recommendatory	4.1.2.6.21 RPC
Real-time Transport Protocol (RTP) can be used to deliver audio and video over the Internet.	Recommendatory	4.1.2.6.22 RTP
Real Time Streaming Protocol can be used, for controlling streaming data over an Internet Protocol network.	Recommendatory	4.1.2.6.23 RTSP
SCP can be used to allow clients to have multiple conversations over a single TCP connection.	Recommendatory	4.1.2.6.24 SCP
The Session Description Protocol (SDP) can be used for describing streaming media initialization parameters in an ASCII string.	Recommendatory	4.1.2.6.25 SDP
The Session Initiation Protocol (SIP) can be considered for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP).	Recommendatory	4.1.2.6.26 SIP
Simple Mail Transfer Protocol (SMTP) should be used for transmitting electronic mails (e-mail) across Internet protocol networks.	Mandatory	4.1.2.6.27 SMTP
Simple Object Access Protocol, XML-based messaging protocol should be used for encoding standards for web services messages.	Mandatory	4.1.2.6.28 SOAP
Secure Shell should be used for exchanging data between two networked devices securely.	Mandatory	4.1.2.6.29 SSH
Telnet (teletype network) should be used on the Internet or local area networks to provide a bidirectional interactive communications facility.	Mandatory	4.1.2.6.30 Telnet
Trivial File Transfer Protocol can be used to transfer small amounts of data between hosts on a network.	Recommendatory	4.1.2.6.31 TFTP
Extensible Messaging and Presence Protocol (XMPP) can be considered to be used in extensible instant messaging (IM) and in the near future for message oriented middleware.	Recommendatory	4.1.2.6.32 XMPP
Transport Layer Protocols		
DCCP should be used to enforce reliable connection setup, teardown, congestion control, and feature negotiation.		4.1.2.7.1 DCCP

Interconnection- Enterprise		
ECN should be used for an end-to-end notification of network congestion without dropping packets	Mandatory	4.1.2.7.2 ECN
RSVP can be considered for the use of reserving resources across a network for an integrated services internet.	Recommendatory	4.1.2.7.3 RSVP
SCTP should be used for transporting packets in a network.	Recommendatory	4.1.2.7.4 SCTP
TCP should be used for communication between server and a single client.	Mandatory	4.1.2.7.5 TCP
UDP should be used for broadcasting or multicasting of data.	Mandatory	4.1.2.7.6 UDP
XTP should be used for high-speed networks for error control, flow control, and rate control.	Recommendatory	4.1.2.7.7 XTP
Internet Layer Protocols		
ICMP should be used by networked computers' operating systems to send error messages.	Mandatory	4.1.2.8.1 ICMP
IGMP should be used for managing the IP multicast groups by IP hosts and adjacent multicast routers to establish multicast group memberships.	Mandatory	4.1.2.8.2 IGMP
IP should be used for delivering packets.	Mandatory	4.1.2.8.3 IP
IS-IS should be used by network devices (routers) to determine the best way to forward data grams through a packet-switched network.	Mandatory	4.1.2.8.4 IS-IS
MPLS-OAM should be used to monitor network operation in order to detect network faults and measure its performance	Mandatory	4.1.2.8.5 MPLS-OAM
MPLS-TE should be used to replicate and expand MPLS-enabled network upon the traffic engineering capabilities of Layer 2 ATM and Frame relay networks.	Mandatory	4.1.2.8.6 MPLS-TE
MSDP should be used to connect multiple PIM Sparse-Mode (PIM-SM) domains together or other protocols.	Recommendatory	4.1.2.8.7 MSDP
PIM should provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet.	Recommendatory	4.1.2.8.8 PIM
QoS should be used to provide different priority to different users or data flows or guarantee a certain level of performance to a data flow in accordance with requests from the application program.	Mandatory	4.1.2.8.9 QoS
RSVP-TE should be used to support the reservation of resources across an IP network. It runs on both IPv4 and IPv6.	Mandatory	4.1.2.8.10 RSVP-TE
SSM should be used to deliver multicast packets from a specific source address requested by the receiver.	Mandatory	4.1.2.8.11 SSM
Virtual Router Redundancy Protocol should be used to	Mandatory	4.1.2.8.12 VRRP

Interconnection- Enterprise		
increase the availability of the default gateway servicing host on the same subnet.		
Link layer Protocols		
Address Resolution Protocol should be used to map an IP address to a MAC address.	Mandatory	4.1.2.9.1 ARP
FDDI should be the standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles).	Recommendatory	4.1.2.9.2 FDDI
L2TP should be used to support virtual private networks (VPNs).	Mandatory	4.1.2.9.3 L2TP
MPLS should be the mechanism used to direct and carry data from one network node to the next.	Mandatory	4.1.2.9.4 MPLS
NDP should be used for discovery of other nodes on the link, information about the paths to other active neighbor nodes.	Recommendatory	4.1.2.9.5 NDP
OSPF should be used to route packets in an IP network dynamically.	Mandatory	4.1.2.9.6 OSPF
PPP should be used to establish a direct connection between two networking nodes and provide Authentication.	Mandatory	4.1.2.9.7 PPP
The Inverse Address Resolution Protocol (InARP/RARP) should be used for mapping MAC address to an IP address.	Mandatory	4.1.2.9.8 RARP
RSTP should be used to provide faster spanning tree convergence after a topology change and respond to changes within a second.	Mandatory	4.1.2.9.9 RSTP
STP should be used to ensure a loop-free topology for any bridged LAN.	Mandatory	4.1.2.9.10 STP
VLAN trunk should be used for allowing multiple bridged networks to transparently share the same physical link.	Mandatory	4.1.2.9.11 VLAN Trunk

6.1.2 Enterprise Level Network Infrastructure Standards

6.1.2.1 Physical Layer Infrastructure Standards

6.1.2.1.1 Cabinet (19-inch Rack)

Description:

A 19-inch rack is a standardized frame or enclosure for mounting multiple equipment modules. Each module has a front panel that is 19 inches (480 mm) wide, including edges or ears that protrude on each side which allow the module to be fastened to the rack frame with screws.

Standard Details:

The "Dimensions of mechanical structures of the 482,6 mm (19 in) standards are defined in IEC 60297. To the original IEC 60297-3:1988 publication was added Amendment 1:1995. The additional requirements were published in IEC 60297-4:1995 with Amendment 1:1999. The extended requirements were published in the IEC 60297-5-1XX series (2001). Responding to market requirements and for more clarity it became necessary to merge and technically enhance these standard "parts" into 3 "new" standards for subracks and associated plug-in units. This "merged" standard series now defined as IEC 60297-3-101, IEC 60297-3-102 and IEC 60297-3-103 explains its relationship to the previous "fragmented" IEC 60297-X standards, see table below.

The nomenclature of these new standards has been revised. The relationship to IEC 60297-1 (Part 1: Panels and Racks) has been maintained. The relationship to IEC 60297-2 (Part 2: Cabinets and pitches of rack structures) has been maintained. The relationship to IEC 61587-1 (Part 1: Climatic, mechanical tests and safety aspects for cabinets, racks, subracks and chassis) and IEC TS 61587-3 (Part 3: Electromagnetic shielding performance tests for cabinets, racks and subracks) has been added. IEC 60297-3-103 defines only the interface dimensions for an alignment pin and a keying device which is additional to those defined in IEC 60297-3-101.

New	Old
"merged" standard series Subracks and associated plug-in units	"fragmented" standard series Subracks and associated plug-in units
Subracks and plug-in units IEC 60297-3-101	IEC 60297-3 IEC 60297-4 IEC 60297-5-102 IEC 60297-5-103 IEC 60297-5-107
Subracks and plug-in units: Injector/extractor handle IEC 60297-3-102	IEC 60297-5-101 IEC 60297-4
Subracks and plug-in units: Keying and alignment pin IEC 60297-3-103	IEC 60297-5-104 IEC 60297-5-105

Resource Locator:

- Cabinet (19 inch Rack) IEC 60297-3 -100

  http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=english&wwwprog=pro-det.p&progdb=db1&He=IEC&Pu=60297&Pa=3&Se=100&Am=&Fr=&TR=&Ed=1

6.1.2.2 Physical Layer - Copper

6.1.2.2.1 Cat6 Cable or better

Description:

Cat 6 is the sixth generation of twisted pair Ethernet cabling, backward compatible with the Cat5e, 5 & 3.Supports 1 Gbps and expected to support 10 Gbps but with limitations of length.

- Transmission Performance Specifications for 4 Pair 100 Ohm
- Attenuation-to-crosstalk margin is positive to 200 MHz
- 4 pairs pure copper wire with polyethylene outer sheet

Copper cables in the market could be not qualitative. 4 pair cables might not be of copper.

Standard Details:

The latest edition of the Commercial Building Telecommunications Cabling Standard is ANSI/TIA/EIA-568-B. The Telecommunications Industry Association (TIA) TR-42 Technical Committee has broken the standard into a series of documents known as B.1, B.2 and B.3. The '568-B.1 document contains the information needed for designing, installing, and field testing a generic structured cabling system. The '568-B.2 and '568-B.3 documents contain manufacturing and component reliability test specifications for cable, patch cords and connecting hardware. The '568-B.3 document was published in April 2000 and is applicable to optical fiber components. The '568-B.2 document specifies the electrical and mechanical requirements of unshielded (UTP) and screened (F/UTP) balanced twisted-pair components.

Due to high speed/bandwidth capability; Cat6 or better is the minimum Recommendatory cable for all data network.

The quality of a copper cable could be checked by testing equipment such as Fluke. Copper cables which have a 4.8 db return loss or higher are said to be qualitative cables.

Resource Locator:

- Cat 6 Cable (TIA/EIA-568-B)

  http://www.tiaonline.org/standards

6.1.2.2.2 Information Outlet Keystones

Description:

In a data wiring system in a building, a connection device designed for a fixed location (usually on a wall) in which data wire terminates; the outlet contains a female jack to receive a male plug that is inserted into it.

Standard Details:

For the past ten years, the ANSI/TIA/EIA-568 standard has been in use by many end users, consultants, and manufacturers for the purpose of assuring that products from a variety of manufacturers will all work together in meeting appropriate system applications. Since the original publication of ANSI/TIA/EIA-568 in July of 1991, the office environment has undergone a period of rapid change marked by the growth of increasingly powerful PC's, access to more sophisticated applications and the need to interconnect different systems. These changes have placed increased demands on the transmission capacity of premise cabling. This growing trend has led to the development of enhanced transmission characteristics in cabling systems. A new published Standards document ANSI/TIA/EIA-568-B.1 replaces the current Standards document ANSI/TIA/EIA-568-A dated October 6, 1995.

ISO/IEC-11801 is an international cabling standard (also referred to as Generic Customer Premises Cabling). The standard was published in 1995. It is based on the ANSI/TIA/EIA-568 cabling standard. Note that the initial document is now considered obsolete. It was updated by ISO/IEC IS11801 AM2-1999, and later with ISO/IEC 11801 2nd Edition - 2000. These updates are outlined at the Cabletesting.com Web site given here.

Resource Locator:

- Information Outlet (TIA/EIA-568 –A or B)

  www.tiaonline.org/standards

- Information Outlet (ISO/IEC 11801)

  www.iso.org/iso/iso_catalogue

6.1.2.2.3 Copper Patch panel

Description:

A patch panel is a panel designed for the management of cable connections. On the front side of a patch panel there are jacks designed to receive short patch cables, while on the back of the panel there are either jacks or punch down blocks that receive the connections of longer and more permanent cables. The assembly of hardware is arranged so that a number of circuits appear on jacks for monitoring, interconnecting, and testing in a convenient and flexible manner. This offers the convenience of allowing quick change the circuit of select signals without the use of expensive dedicated switching equipment. Patch panels are typically rack mountable.

Patch Panels required are not usually matched while they get installed. Example Cat5e patch panels are installed while Cat6 patch panels are required.

Standard Details:

TSB 40(A) came after TSB 36 and is concerned with the connecting hardware. The following table details the maximum allowed attenuation (dB) across connecting hardware at a range of frequencies.

Table 6-6: *Maximum allowed attenuation (dB) across connecting hardware*

Frequency (MHz)	Cat 3	Cat 4	Cat 5
1.0	0.4	0.1	0.1
4.0	0.4	0.1	0.1
8.0	0.4	0.1	0.1
10.0	0.4	0.1	0.1
16.0	0.4	0.2	0.2
20.0		0.2	0.2
25			0.2
31.25			0.2
62.5			0.3
100			0.4

The following table shows the worst pair to pair NEXT (dB) across a range of frequencies for the hardware:

Table 6-7: *Worst pair to pair NEXT (dB) across a range of frequencies for the hardware*

Frequency (MHz)	Cat 3	Cat 4	Cat 5
1.0	58	>65	>65
4.0	46	58	>65
8.0	40	52	62
10.0	38	50	60
16.0	34	46	56
20.0		44	54
25			52
31.25			50

Frequency (MHz)	Cat 3	Cat 4	Cat 5
62.5			44
100			40

Make sure the patch panels chosen or installed meet the requirements and the Gig Speed patch panels are used for high bandwidth and speed.

Resource Locator:

- Copper Patch panel (TSB-40-A)

  www.tiaonline.org/standards

6.1.2.2.4 Copper Patch cords

Description:

A Copper patch cord is a piece of copper wire cable that connects circuits on a patch panel. The market here in Nepal is a challenge when considering buying copper cables. Copper patch cords and copper cables might not be pure copper.

Standard Details:

For the past ten years, the ANSI/TIA/EIA-568 standard has been in use by many end users, consultants, and manufacturers for the purpose of assuring that products from a variety of manufacturers will all work together in meeting appropriate system applications.

Since the original publication of ANSI/TIA/EIA-568 in July of 1991, the office environment has undergone a period of rapid change marked by the growth of increasingly powerful PC's, access to more sophisticated applications and the need to interconnect different systems. These changes have placed increased demands on the transmission capacity of premise cabling. This growing trend has led to the development of enhanced transmission characteristics in cabling systems.

A new published Standards document ANSI/TIA/EIA-568-B.1 replaces the current Standards document ANSI/TIA/EIA-568-A dated October 6, 1995.

It is Recommendatory to check and test copper cables with testing devices such as fluke to ensure its quality and copper wires.

Resource Locator:

- Copper Patch Cords (TIA/EIA-568-B)

  www.tiaonline.org/standards

6.1.2.3 Physical Layer – Optical Fiber

6.1.2.3.1 Optical Fiber Cables

Description:

Fibre optic cable is a cabling structure carrying light pulses which is used in the trunk telephone network for high capacity transmission of voice, data or video images. It is a flexible and secure meth od used for high speed Private Circuits; from 4 core cable to 384 core cables.

Standard Details:

EIA/TIA 568: standard for premises cabling is used by most manufacturers and users of premises cabling systems in the US. Internationally, IEC/ISO 11801 is very similar for fiber optics, although there are differences in various countries. TIA-568 has been under continual revision since its inception. The current version is "568 B.3" covering fiber optics. It includes some major changes from earlier versions for fiber optics. TIA 568 "C" was published sometime in 2008, but fiber optic cabling changes are not substantial. These include:

1. Adds 50/125 micron fiber (OM2 or OM3) as an alternative fiber type and specifies performance.

2. Allows alternate connectors to the SC, esp. small form factor connectors.

3. Adds performance standards for all connectors.

4. Includes bend radius specifications for cables.

5. Specifies requirements for connecting hardware.

Fiber Optic Cable Performance Standards

568 B3 adds 50/125 fiber as an acceptable type and specifies the performance of cabled fiber as follows:

Table 6-8: *Fiber Optic Cable Performance Standards*

Fiber Type	Wavelength (nm)	Max Attenuation Coefficient (dB/km)	Bandwidth (MHz-km with overfilled launch)
50/125 (OM2, OM3)	850	3.5	500 (OM2), 2000 (OM3)
	1300	1.5	500
62.5/125 (OM1)	850	3.5	160
	1300	1.5	500
Single mode (OS1, OS2) (Premises)	1310	1.0	NA
	1550	1.0	NA
Single mode (OS1, OS2) (Outside Plant)	1310	0.5	NA
	1550	0.5	NA

Resource Locator:

- Optical Fiber Cables (TIA/EIA-568-B.3)

  www.tiaonline.org/standards

6.1.2.3.2 Pigtail

Description:

A fiber pigtail is a single-fiber cable, usually short length that has an optical connector on one end and a length of exposed fiber at the other end.

Standard Details:

Fiber optic pigtails the typical use is to link the fiber optic cable with fiber optic equipment, the fiber optic pigtail with connector side is used to link the equipment, while the other side of the pigtail is melted together with the fiber cable, by melting together the fiber glasses, it can reach a minimum insertion loss. Common types of fiber optic pigtails are usually with 0.9mm fiber cable diameter, and usually installed inside ODF unit. Most commonly used types are SC fiber optic pigtail, ST fiber optic pigtail, FC fiber optic pigtail, LC fiber optic pigtail, MT-RJ fiber optic pigtail, SC/APC fiber optic pigtail, FC/APC fiber optic pigtail and E2000 fiber optic pigtail.

Resource Locator:

- Fiber Pigtail (TIA/EIA-604-10-A)

  www.tiaonline.org/standards

- Fiber Pigtail (IEC 61754-20)

  http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=61754&Pa=20&Se=11&Am=&Fr=&TR=&Ed=1

6.1.2.3.3 Fiber Patch panel

Description:

A fiber patch panel is a distribution area to rearrange fiber optic cable connections and circuits. A simple patch panel is a metal frame. One side of the panel is usually fixed. This means that the fiber optic cables are not intended to be disconnected. On the other side are plugs to connect other fiber optic cables.

Standard:

This standard discusses optical fiber cabling components and specifies components transmission, requirements for optical fiber cabling systems. The purpose of this standard is to provide the minimum requirements for telecommunications cabling within a commercial building or campus environment.

Make sure the connectors on your patch cables and pigtails match the fiber patch panel connectors.

Resource Locator:

- Fiber Patch Panel (TIA/EIA-568-B.3)

  www.tiaonline.org/standards

6.1.2.3.4 Fiber Patch cords

Description:

A fiber patch cord is a fiber optic cable used to attach one device to another for signal routing.

Standard Details:

Fiber optic patch cord sometimes is also called fiber optic jumper or fiber optic patch cables. Generally there are two types of fiber optic patch cords: single mode fiber optic patch cords and multimode fiber optic patch cords. Fiber optic patch cord are used for linking the equipment and components in the fiber optic network, they are with various kinds of fiber optic connector types. The fiber optic patch cord types are classified by the fiber optic connector types.

Resource Locator:

- Fiber Patch Cords (TIA/EIA-568-B.3)

  www.tiaonline.org/standards

6.1.2.4 Data Center

6.1.2.4.1 Main Data Center

A Data Centre is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (air conditioning, fire suppression, access control, climate & ventilation control, cable tray and central UPS etc.) and security devices.

6.1.2.4.2 Disaster Recovery/ Load Balance Data Center

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human induced disaster whereas;

Load Balancing is a technique to distribute workload evenly across two or more links in order to get optimal resource utilization, maximize throughput, minimize response time and avoid overload. It is usually provided by a dedicated program or hardware device (such as a multilayer switch or a DNS Server) and often used to implement failover— the continuation of a service after the failure of one or more of its components.

Resource Locator:

- Disaster recovery guidelines (ISO/IEC 24762)

  www.iso.org/iso/catalogue_detail.htm?csnumber=41532

6.1.2.4.3 Infrastructure of Data Center

Description:

Infrastructure of Data Centre deals with the components that are mandatory in a data centre. This infrastructure is required both at the main data centre as well as at the disaster recovery/load balancing data centre.

Data Centre is not usually fully equipped with the infrastructure, hence, vulnerable to a natural or man-made catastrophe.

Standard Details:

TIA-942 is a standard developed by the Telecommunications Industry Association (TIA) to define guidelines for planning and building data centers, particularly with regard to cabling systems and network design. The standard deals with both copper and fiber optic media.

TIA-942 addresses specification about Site Space and Layout, Cabling Infrastructure, Tiered reliability and Environmental considerations.

The TIA-942 specification references private and public domain data center requirements for applications and procedures such as:

- Network architecture

- Electrical design
- File storage, backup and archiving
- System redundancy
- Network access control and security
- Database management
- Web hosting
- Application hosting
- Content distribution
- Environmental control
- Protection against physical hazards (fire, flood, windstorm)
- Power management

The principal advantages of designing data centers in accordance with TIA-942 include standard nomenclature, failsafe operation, robust protection against natural or human made disasters, and long-term reliability, expandability and scalability.

Each of the components of the data center and its supporting systems must be planned, designed, and implemented to work together to ensure reliable access of data center resources while supporting future requirements. Neglecting any aspect of the design can render the data center Vulnerable to cost failures, early obsolescence, and intolerable availability. There is no substitute for careful planning and following the guidelines set forth in the TIA-942 Telecommunications Infrastructure Standards for Data Centers.

It is Recommendatory that each enterprise have its own Data centre and one national Level Data centre.

Data centre should be fully equipped with the essential infrastructure mentioned above to resist any natural or man-made calamities.

Resource Locator:

- Data center infrastructure (TIA-942)

  www.tiaonline.org/standards

6.1.2.5 Enterprise Level IP Network

Description:

Enterprise level IP network consist of Access/Data Link Layer such as managed switched, unmanaged switch and Core network layer such as Router, Multi- Layer Switches.

A Managed switch allows you to control the individual ports of your switch. It has the ability to turn the port on or off and control its link speed and duplex settings.

An Unmanaged switch works right out of the box; it doesn't need to be configured and doesn't have the ability to turn the port on or off and control its link speed and duplex settings.

A router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information (Packets).

A multilayer switch (MLS) is a computer networking device that switches on data link layer like an ordinary network switch and provides extra functions on higher layers.

Standards details:

- All IT equipments should be IPv6 Compatible.
- It is Recommendatory to have a managed switch so as to control and have security from anybody walking in to the Enterprise's LAN.

6.1.2.6 Application Layer Protocols

6.1.2.6.1 Border Gateway Protocol (BGP)

Description:

Border Gateway Protocol is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach ability among autonomous systems (AS). It is described as a path vector protocol. It runs over TCP.

Standard Details:

The early Internet had a set of centralized routers functioning like a "core" autonomous system. These routers used the Gateway-to-Gateway Protocol for communication between them within the AS, and the aptly-named Exterior Gateway Protocol (EGP) to talk to routers outside the core.

When the Internet grew the importance of communication between them grows as well. EGP was functional but had several weaknesses that became more problematic as the Internet grew in size. It was necessary to define a new exterior routing protocol that would provide enhanced capabilities for use on the growing Internet.

In June 1989, the first version of this new routing protocol was formalized, with the publishing of RFC 1105, A Border Gateway Protocol (BGP). This initial version of the BGP standard defined most of the concepts behind the protocol, as well as key fundamentals such as messaging, message formats and how devices operate in general terms. It established BGP as the Internet's exterior routing protocol of the future.

Resource Locator:

- BGPv4 (RFC 4271)

  http://www.rfc-editor.org/rfc/rfc4271.txt

6.1.2.6.2 Domain Name System (DNS)

Description:

DNS is name resolution software that lets users locate computers (assigned with IP addresses) on the Internet by domain name.

Standard Details:

The Domain Name System was originally invented to support the growth of email communications on the ARPANET, and now supports the Internet on a global scale. Alphabetic host names were introduced on the

ARPANET shortly after its creation, and greatly increased usability since alphabetic names are much easier to remember than semantically meaningless numeric addresses. Host names were also useful for development of network-aware computer programs, since they could reference a constant host name without concern about changes to the physical address due to network alterations. Starting with a formal proposal for centralization in Host Names On-line, RFC 606, in December, 1973, proceeding through agreement in Host Names On-Line, RFC 608, and further discussions in Comments on On-Line Host Name Service, RFC 623, it was settled by March, 1974 with On Line Hostnames Service, RFC 625, that the Stanford Research Institute Network Information Center (NIC) would serve as the official source of the master hosts file.

Resource Locator:

- DNS (RFC 1034)

  http://www.rfc-editor.org/rfc/rfc1034.txt

6.1.2.6.3 Dynamic Host Configuration Protocol (DHCP)

Description:

DHCP is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention.

Standard Details:

BOOTP used static table of mappings between hardware addresses and IP addresses which simply wasn't upto task. In many organizations, trying to keep track of constant IP address changes became a daunting task in and of it. It also offered no way to reuse addresses; once an address had been assigned, a device could keep it forever, even if it were no longer needed. Therefore, new host configuration protocol was needed to serve modern networks, which would move away from static, permanent IP address assignment. The IETF supplied this in the form of the Dynamic Host Configuration Protocol (DHCP), first formalized in RFC 1541, October 1993. (Actually, it was really originally specified in RFC 1531 in that same month, but due to minor errors in 1531 the standard was quickly revised and 1541 published.)

Resource Locator:

- DHCP IPv4 (RFC 2131)

  http://www.rfc-editor.org/rfc/rfc2131.txt

- DHCP IPv6 (RFC 3315)

  http://www.rfc-editor.org/rfc/rfc3315.txt

6.1.2.6.4 File Transfer Protocol (FTP)

Description:

File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet. FTP is built on client-server architecture and utilizes separate control and data connections between the client and server applications.

Standard Details:

FTP evolved from the conceptual division of methods of network use by developers such as: direct use and indirect use. The indirect use meant getting resources from a remote host and using them on the local system and transferring them back; this is where FTP fits in. The first FTP standard was RFC 114, published in April 1971, before TCP and IP even existed. This standard defined the basic commands of the protocol and the formal means by which devises communicate using it.

Resource Locator:

- FTP (RFC 0959)

  http://www.rfc-editor.org/rfc/rfc0959.txt

6.1.2.6.5 Secure File Transfer Protocol (FTPS)

Description:

Secure File Transfer Protocol an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

Standard Details:

This standard describes a mechanism that can be used by FTP clients and servers to implement security and authentication using the TLS protocol "The TLS Protocol Version 1.0.", and the extensions to the FTP protocol, "FTP Security Extensions". It describes the subset of the extensions that are required and the parameters to be used, discusses some of the policy issues that clients and servers will need to take, considers some of the implications of those policies, and discusses some expected behaviors of implementations to allow interoperation.

This specification is in accordance with RFC 959, "File Transfer Protocol". It relies on RFC 2246, "The TLS Protocol Version 1.0.", and RFC 2228, "FTP Security Extensions".

Resource Locator:

- FTPS (RFC 4217)

  http://www.rfc-editor.org/rfc/rfc4217.txt

6.1.2.6.6 GPRS Tunnelling Protocol (GTP)

Description:

GPRS Tunnelling Protocol (GTP) is an IP-based communications protocols used to carry General Packet Radio Service (GPRS) within GSM and UMTS networks.

It can be decomposed into separate protocols, GTP-C, GTP-U and GTP'. GTP-C is used within the GPRS core network for signaling between Gateway GPRS Support Nodes (GGSN) and Serving GPRS Support Nodes (SGSN). GTP-U is used for carrying user data within the GPRS Core Network and between the Radio Access Network and the core network. The user data transported can be packets in any of IPv4, IPv6, or PPP formats. Where GTP' (*GTP prime*) uses the same message structure as GTP-C and GTP-U, but has an independent function. It can be used for carrying charging data from the Charging Data Function (CDF) of the GSM or UMTS network to the Charging Gateway Function (CGF).It can be used with UDP or TCP. GTP version one is used only on UDP.

Standard Details:

GTP was originally standardized within ETSI (GSM standard 09.60). With the creation of the UMTS standards this was moved over to the 3GPP which, as of 2005 maintains it as 3GPP standard 29.060. GTP' uses the same message format, but its special uses are covered in standard 32.295 along with the standardized formats for the charging data it transfers. Later versions of TS 29.060 deprecate GTPv1/v0 interworking such that there is no fallback in the event that the GSN does not support the higher version.GTPv2 (for evolved packet services) went into draft in early 2008 and was released in December of that year. GTPv2 offers fallback to GTPv1 via the earlier "Version Not Supported" mechanism but explicitly offers no support for fallback to GTPv0.

Resource Locator:

- GTP

  www.3gpp.org/ftp/Specs/html-info/29060.htm

6.1.2.6.7 Hyper Text Transfer Protocol (HTTP)

Description:

Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It uses for retrieving inter-linked resources, called hypertext documents.

Standard Details:

HTTP was initially a very simple protocol used to request pages from a server. The browser would connect to the server and send a command and the server would respond with the contents of the requested file, there were no request headers. This protocol was first documented as HTTP/0.9. Browsers and servers extended the HTTP protocol from 0.9 with new features such as request headers and additional request methods. The resulting HTTP/1.0 protocol was only officially documented in early 1996 with the release of RFC1945.

Resource Locator:

- HTTP (RFC 2616)

  http://www.rfc-editor.org/rfc/rfc2616.txt

6.1.2.6.8 Secure Hypertext Transfer Protocol (HTTPS)

Description:

HTTPS is a secure hypertext transfer protocol.

Standard Details:

This document describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port; this document documents practice using TLS. A companion document describes a method for using HTTP/TLS over the same port as normal http [RFC 2817].

Resource Locator:

- HTTPS (RFC 2818)

  http://www.ietf.org/rfc/rfc2818.txt

6.1.2.6.9 Internet Message Access Protocol (IMAP)

Description:

IMAP (Internet Message Access Protocol) is a protocol for retrieving e-mail messages. The latest version, IMAP4, is similar to POP3 but supports some additional features. For example, with IMAP4, you can search through your e-mail messages for keywords while the messages are still on mail server. You can then choose which messages to download to your machine.

Standard Details:

The IMAP protocol (Internet Message Access Protocol) was first conceived in 1986, at Stanford University. IMAP2 was defined in 1987, and the first UNIX server was implemented at this time.

In July of 1988, the first IMAP RFC, RFC 1064 was published, and work began on the C-client. This was a series of library routines, written at Stanford by Mark Crispin. This code was originally intended as the low level foundation for a Macintosh client. Based on this was the first real IMAP client, MM-D (for "MM on Xerox D machines" - MM was a popular DEC-20 mail program) was written in Interlisp for Xerox Lisp machines.

At that time, there was no name for the embryonic Mac client, but since it was the first one to be written in C instead of Lisp, it was given a development name of "C client". This name subsequently became "c-client" because that is the name of the subdirectory on UNIX where the source files were stored.

In 1989, Mark Crispin was hired by the University of Washington, where he continued work on the c-client. The c-client was subsequently incorporated into the University of Washington's PINE mail client, which uses functionality provided by c-client for RFC-822 parsing, MIME parsing and decoding and SMTP.

By 1992, the University of Washington had deployed an IMAP server, and release PINE version 2.0, with IMAP support. Carnegie Mellon University began work on the Andrew II/Cyrus project, a competing offering With the release of the RFC's for IMAP4 (1730-1733), IMAP4 was approved as a proposed Internet standard, and the pace of development accelerated. By 1995 Carnegie Mellon had released its first IMAP4 server, and an IMAP4 server and rewritten c-client had been released by the University of Washington. With the release of the IMAP4rev1 specification (RFC 2060) in 1996, and the declaration of support for IMAP by Sun and Netscape, the way was paved for IMAP to become ubiquitous.

Resource Locator:

- IMAP (RFC 1203)

  http://www.rfc-editor.org/rfc/rfc1203.txt

6.1.2.6.10 Internet Relay Chat (IRC)

Description:

Internet Relay Chat (IRC) is a form of real-time Internet text messaging or synchronous conferencing. It is mainly designed for group communication in discussion forums but also allows one-to-one communication via private message as well as chat and data transfers via Direct Client-to-Client.

Standard Details:

IRC was created by Jarkko Oikarinen in August 1988 to replace a program called MUT (MultiUser Talk) on a BBS called OuluBox in Finland. Oikarinen found inspiration in a chat system known as Bitnet Relay, which operated on the BITNET.IRC was used to report on the 1991 Soviet coup d'état attempt throughout a media blackout. It was previously used in a similar fashion during the Gulf War.

Resource Locator:

- IRC (RFC 2813)

  http://rfc-editor.org/rfc/2813.txt

6.1.2.6.11 Light Weight Directory Access Protocol (LDAP)

Description:

Light Weight Directory Access Protocol is an application protocol for querying and modifying directory services running over TCP/IP. It uses Domain name system (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries).

Standard Details:

LDAP was inspired by the X.500 directory access protocol, or DAP, which is an earlier effort that aimed to provide industry standard protocol for accessing global directory services. The LDAP protocol itself was defined within the confines of the Internet Engineering Task Force (IETF) and the University of Michigan researchers, with some support from the U.S. National Science Foundation, built a freely available reference implementation.

Resource Locator:

- LDAP (RFC 4510)

  http://www.rfc-editor.org/rfc/rfc4510.txt

6.1.2.6.12Megaco

Description:

Megaco (H.248) is implementation architecture for controlling Media Gateways on IP networks and the public switched telephone network (PSTN). It defines the protocol for Media Gateway Controllers to control Media Gateways for the support of multimedia streams across computer networks. It is typically used to provide Voice over Internet Protocol (VoIP) services (voice and fax) between IP networks and the PSTN, or entirely within IP networks.

Standard Details:

The protocol was the result of collaboration of the MEGACO working group of the Internet Engineering Task Force (IETF) and International Telecommunication Union (ITU-T) Study Group 16. The IETF originally published the standard as RFC 3015, which was later replaced by RFC 3525. The term *Megaco* is the IETF designation. The ITU later took ownership of the protocol and IETF's version has been reclassified as historic. The ITU has published three versions of H.248.1, the most recent in September 2005.

Resource Locator:

- Megaco

  www.itu.int/itudoc/itu-t/aap/sg16aap/.../h248.1/index.html

6.1.2.6.13Media Gateway Control Protocol (MGCP)

Description:

Media Gateway Control Protocol is a similar protocol to Megaco. It is an implementation for controlling media controllers on IP and telephone Networks. It is the successor of session Gateway control Protocol. It is a signalling and call control protocol used within Voice over IP systems that typically interoperate with the public switched telephone network (PSTN). As such it implements a PSTN-over-IP model with the power of the network residing in a call control center. The protocol represents a decomposition of other VoIP models, such as H.323, in which the media gateways have higher levels of signalling intelligence.

MGCP uses the Session Description Protocol (SDP) for specifying and negotiating the media streams to be transmitted in a call session and the Real-time Transport Protocol (RTP) for framing of the media streams.

Standard Details:

Media Gateway Control Protocol architecture exists in the similarly named Megaco protocol, a collaboration of the Internet Engineering Task Force (RFC 3525) and International Telecommunication Union (Recommendation H.248.1). Both protocols follow the guidelines of the API Media Gateway Control Protocol Architecture and Requirements in RFC 2805.

Resource Locator:

- MGCP

  www.itu.int/itudoc/itu-t/aap/sg16aap/.../**h248.1**/index.html

6.1.2.6.14Multipurpose Internet Mail Extensions (MIME)

Description:

MIME (Multipurpose Internet Mail Extensions) is a specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII. In addition to e-mail applications, Web browsers also support various MIME types. This enables the browser to display or output files that are not in HTML format.

Standard Details:

MIME is one of the Internet protocol standards defined by the IETF (RFC 2633). It is associated primarily with electronic mail, MIME has evolved to become an important element supporting multimedia applications or other extension formats to a mail on the Net.

Resource Locator:

- MIME (RFC 2633)

  http://www.rfc-editor.org/rfc/rfc2633.txt

6.1.2.6.15Multiprotocol Border Gateway Protocol (MP-BGP)

Description:

The multiprotocol BGP feature adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. In other words, it is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) to build data distribution trees.

Standard Details:

This document defines extensions to BGP-4 to enable it to carry routing information for multiple network layer protocols. It is backward compatible with a router that supports the extensions can interoperate with a router that doesn't support extensions.

Resource Locator:

- MP-BGP(RFC 4760)

  http://www.rfc-editor.org/rfc/rfc4760.txt

6.1.2.6.16 Network Management Protocols- Simple Network management Protocol (SNMP)

Description:

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Standard Details:

The history of the SNMP Protocol goes back to the predecessor of the SNMP Framework, the Simple Gateway Monitoring Protocol (SGMP), which was defined in RFC 1028 in 1987. The SGMP standard specified the basic design model used in SNMP, by describing the SGMP protocol in terms of only retrievals of, or alterations to, variables stored on an Internet gateway (router). The standard also outlines the small number of protocol operations that are still the basis for SNMP's operation today.

The first version of the SNMP Framework, SNMPv1, included the first formal definition of the SNMP Protocol, in RFC 1067 (later revised by RFCs 1098 and 1157). This standard refines the protocol operations given in the SGMP document. It makes the operation of the SNMP Protocol fit into the overall SNMP Framework, working with formally-defined MIB objects.

Resource Locator:

- SNMP (RFC 3411)

  http://www.rfc-editor.org/rfc/rfc3411.txt

6.1.2.6.17 Network News Transfer Protocol (NNTP)

Description:

The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (*Netnews*) between news servers and for reading and posting articles by end user client applications.

Standard Details:

NNTP was first developed to allow news reader applications to display content. The specification for NNTP was completed in March of 1986. Its first development began for a personal project which studied client/server architecture and programming internet applications. And a protocol was proposed that would allow users to read newsgroups remotely via TCP/IP.

Resource Locator:

- NNTP (RFC 3977)

  http://www.rfc-editor.org/rfc/rfc3977.txt

6.1.2.6.18 Network Time Protocol (NTP)

Description:

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP on port 123 as its transport layer. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

People change the time on their workstations according to their preferences and time settings they are used to, therefore clashes the time in the network with their respective workstations. With this factor it becomes difficult to correlate information between devices accurately, if not impossible. Security wise makes it difficult to trace an incident if time logs for network routers, servers or devices is not synchronized and gives an attacker a room to do as he/she pleases.

Standard Details:

The first NTP implementation started around 1980 with an accuracy of only several hundred milliseconds. That very first implementation was documented in Internet Engineering Note [IEN-173]. The first complete specification of the protocol and accompanying algorithms for NTP version 1 appeared 1988 in [RFC 1059]. That version already had symmetric operation mode as well as client-server mode. Combining the good ideas of DTSS with those of NTP produced a new specification for NTP version 3, namely [RFC 1305], in 1992. This version introduced formal correctness principles.

Since Time is inherently important to the function of routers and networks. It provides the only frame of reference between all devices on the network. This makes synchronized time extremely important. Make sure all work stations on the network have the same time settings and set it once centrally.

Resource Locator:

- NTP (RFC 1305)

  http://www.rfc-editor.org/rfc/rfc1305.txt

6.1.2.6.19Post Office Protocol (POP)

Description:

POP (Post Office Protocol) is a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol). There are two versions of POP. The first, called POP2, became a standard in the mid-80 and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Standard Details:

The Post Office Protocol (POP) was designed for quick, simple and efficient mail access; it is used by millions of people to access billions of e-mail messages every day. The advantage of being able to retrieve e-mail from a server directly to a client computer, rather than accessing the mailbox on the server was recognized. In 1984, RFC 918 was published, defining the Post Office Protocol (POP). The idea behind POP was to provide a simple way for a client computer to retrieve e-mail from a mailbox on an SMTP server so it could use locally.

Resource Locator:

- POP (RFC 1939)

  http://www.rfc-editor.org/rfc/rfc1939.txt

6.1.2.6.20 Routing Information Protocol (RIP)

Description:

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. RIP is a distance-vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15.

Standard Details:

RIP was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, however, they are considered technically obsolete by more advanced techniques.

Resource Locator:

- RIPv2- RFC 2453

  http://www.rfc-editor.org/rfc/rfc2453.txt

6.1.2.6.21Remote Procedure Call (RPC)

Description:

Remote procedure call (RPC) is a technology that allows computer program to cause a subroutine or procedure to execute in another address space (another computer of a shared network) without an explicitly written coding that details the remote interaction.

Standard Details:

The idea of RPC (Remote Procedure Call) goes back at least as far as 1976, when it was described in RFC 707. One of the first business uses of RPC was by Xerox under the name "Courier" in 1981. The first popular implementation of RPC on UNIX was Sun's RPC (now called ONC RPC), used as the basis for Sun's NFS. ONC RPC is still widely used today on several platforms.

Resource Locator:

- RPC v2

http://rfc-editor.org/rfc/rfc5531.txt

6.1.2.6.22 Real-time Transport Protocol (RTP)

Description:

Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet. It is usually used in conjunction with the RTP Control Protocol (RTCP).

Standard Details:

The standard was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889, and superseded by RFC 3550 in 2003; which defines a standardized packet format for delivering audio and video over the Internet.

Resource Locator:

- RTP(RFC 3550)

  http://www.rfc-editor.org/rfc/rfc3550.txt

6.1.2.6.23 Real Time Streaming Protocol (RTSP)

Description:

Real Time Streaming Protocol, a standard for controlling streaming data over an Internet Protocol networks. RTSP uses RTP (Real-Time Transport Protocol) to format packets of multimedia content. It is designed to efficiently broadcast audio-visual data to large groups.

Standard Details:

This RFC discusses benefits and issues that arise when allowing Real-time Transport Protocol (RTCP) packets to be transmitted with reduced size. The size can be reduced if the rules on how to create compound packets outlined in RFC 3550 are removed or changed. Based on that analysis, this memo defines certain changes to the rules to allow feedback messages to be sent as Reduced-Size RTCP packets under certain conditions when using the RTP/AVPF (Real-time Transport Protocol / Audio-Visual Profile with Feedback) profile (RFC 4585). This document updates RFC 3550, RFC 3711, and RFC 4585.

Resource Locator:

- RTSP(RFC 5506)

  http://rfc-editor.org/rfc/5506.txt

6.1.2.6.24 Session control protocol (SCP)

Description:

SCP is a simple protocol which lets a server and client has multiple conversations over a single TCP connection. The protocol is designed to be simple to implement, and is modeled after TCP.

Standard Details:

SCP's main service is dialogue control. This service allows either end of the connection to establish a virtual session over a single transport connection. SCP also allows a sender to indicate message boundaries, and allows a reciever to reject an incoming session. SCP allows data to be sent with the session establishment; the recepient does not confirm successful connection establishment, but may reject unsuccessful attempts. This simplifies the design of the protocol, and removes the latency required for a confirmed operation.

Resource Locator:

- SCP

  www.w3.org/Protocols/HTTP-NG/http-ng-scp.html

6.1.2.6.25 Session Description Protocol (SDP)

Description:

The Session Description Protocol (SDP) is a format for describing streaming media initialization parameters in an ASCII string. It is intended for describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP does not deliver media itself but is used for negotiation between end points of media type, format, and all associated properties. The set of properties and parameters are often called a session profile. SDP is designed to be extensible to support new media types and formats.

Standard Details:

SDP started off as a component of the Session Announcement Protocol (SAP), but found other uses in conjunction with Real-time Transport Protocol (RTP), Real-time Streaming Protocol (RTSP), Session Initiation Protocol (SIP) and even as a standalone format for describing multicast sessions.

Resource Locator:

- SDP(RFC 4566)

  http://rfc-editor.org/rfc/4566.txt

6.1.2.6.26 Session Initiation Protocol (SIP)

Description:

The Session Initiation Protocol (SIP) is a signalling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams.

Standard Details:

SIP was conceived first to improve the setup and handling of telephone calls but was quickly adapted to real-time communications. The original drafts of what was to become the SIP standard started back in February 1996. The first Internet Engineering Task Force (IETF) draft was titled "draft-ietf-mmusic-sip-00," included only one request type, which was a call setup request. Revisions of this draft led to the publication of "draft-ietf-mmusic-sip-01" in December 1996. This draft would still be unrecognizable to most people as the precursor to SIP. Eleven versions and 3 years later, the draft took shape as the SIP with which people are now familiar. The IETF published this draft, which was called "draft-ietf-mmusic-sip-12," in January 1999. It contained the six requests that SIP has today. From "draft-ietf-mmusic-sip-12" to SIP's publication as RFC 2543 in March 1999 was a small step.

Resource Locator:

- SIP (RFC 3261)

  http://www.rfc-editor.org/rfc/rfc3261.txt

6.1.2.6.27 Simple Mail Transfer Protocol (SMTP)

Description:

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks. While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use SMTP for sending messages to a mail server for relaying.

Standard Details:

Technologists sought to find a way to communicate email messages between systems. This led to the publishing of Mail Transfer Protocol (MTP), which was first defined in RFC 772 in September 1980, then updated in RFC 780 in May 1981. MTP describes a set of commands and procedures by which two devices can connect using TCP to exchange e-mail messages. Where simpler form of this protocol evolved the name Simple Mail Transport Protocol took over.

Resource Locator:

- SMTP (RFC 5321)

  http://www.rfc-editor.org/rfc/rfc5321.txt

6.1.2.6.28 Simple Object Access Protocol (SOAP)

Description:

Simple Object Access Protocol is a lightweight, XML-based messaging protocol that is the encoding standard for web services messages.

Standard Details:

SOAP Version 1.2 Part 0: Primer (Second Edition) is a non-normative document intended to provide an easily understandable tutorial on the features of SOAP Version 1.2. In particular, it describes the features through various usage scenarios, and is intended to complement the normative text contained in Part 1 and Part 2 of the SOAP 1.2 specifications. This second edition includes additional material on the SOAP Message Transmission Optimization Mechanism (MTOM), the XML-binary Optimized Packaging (XOP) and the Resource Representation SOAP Header Block (RRSHB) specifications.

This protocol is Recommendatory to be used for the recently launched government portal of Nepal for e-services.

Resource Locator:

- SOAP

  www.w3.org/TR/soap12-part0/

6.1.2.6.29 Secure Shell (SSH)

Description:

Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Standard Details:

Secure Shell was originally created to provide secure terminal (shell) access to Unix servers over TCP/IP networks. Still today, secure replacement of Telnet-based terminal connections between servers is one of the most widespread uses of the technology. One of the key user groups for secure terminal access are system administrators who have adopted Secure Shell as the de-facto standard for administrating remote servers and other network devices.

Resource Locator:

- SSHv2

  http://www.rfc-editor.org/rfc/rfc4251.txt

6.1.2.6.30 Teletype Network (Telnet)

Description:

Telnet (teletype network) is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility.

Standard Details:

The purpose of the TELNET Protocol is to provide a fairly general, bi-directional, eight-bit byte oriented communications facility. Its primary goal is to allow a standard method of interfacing terminal devices and terminal-oriented processes to each other. It is envisioned that the protocol may also be used for terminal-terminal communication ("linking") and process-process communication (distributed computation).

Resource Locator:

- Telnet (RFC 854)

  http://www.rfc-editor.org/rfc/rfc854.txt

6.1.2.6.31Trivial File Transfer Protocol (TFTP)

Description:

Trivial File Transfer Protocol is a file transfer protocol, used to transfer small amounts of data between hosts on a network; uses UDP as its transport protocol.

Standard Details:

The need of TFTP came about from the issue of size. For example the starting up of devices (bootstrapping) meant ability to transfer files quickly and easily. The instructions to perform bootstrapping must fit into a ROM chip which made the size of the software an important issue. Hence, the solution to this need was to create a “light” version of FTP that would emphasize small program size and simplicity over functionality. This new protocol, called the Trivial File Transfer Protocol (TFTP), was initially developed in the late 1970s, and first standardized in 1980. The modern version, called TFTP version 2, was documented in RFC 783 in 1981, which was revised and published as RFC 1350, The TFTP Protocol (Revision 2), in 1992. This is the current version of the standard.

Resource Locator:

- TFTP (RFC 1350)

  http://www.rfc-editor.org/rfc/rfc1350.txt

6.1.2.6.32 Extensible Messaging and Presence (XMPP)

Description:

Extensible Messaging and Presence Protocol (XMPP) is an open, XML-based protocol originally aimed at near-real-time, extensible instant messaging (IM) and presence information but currently expanded into the broader realm of message oriented middleware. It allows anyone who has a domain name and a suitable Internet connection can run their own XMPP server and talk to users on other servers. The standard server implementations and many clients are also free and open source software.

Standard Details:

Jeremie Miller began the Jabber project in 1998. Its first major public release occurred in May 2000. The project's main software was jabbered, a XMPP server. Its main product was the XMPP protocol. The Internet Engineering Task Force (IETF) formed an XMPP Working Group in 2002 to formalize the core protocols as an IETF instant messaging and presence technology. The XMPP WG produced four specifications which were approved by the IESG as Proposed Standards in 2004. RFC 3920 and RFC 3921 are now undergoing revisions in preparation for advancing them to Draft Standard within the Internet Standards Process. The XMPP Standards Foundation is active in developing open XMPP extensions.

Resource Locator:

- XMPP (RFC 3920)

  http://rfc-editor.org/rfc/rfc3920.txt

6.1.2.7 Transport Layer Protocols

6.1.2.7.1 Datagram Congestion Control Protocol (DCCP)

Description:

Datagram Congestion Control Protocol (DCCP) is a message-oriented protocol that implements reliable connection setup, teardown, congestion control, and feature negotiation. It provides a way to gain access to congestion control mechanisms without having to implement them at the Application Layer and also allows flow-based semantics like in TCP, but does not provide reliable in-order delivery. Sequenced delivery within multiple streams as in SCTP is not available in DCCP.

Standard Details:

DCCP was published as RFC 4340, a proposed standard, by the IETF in March, 2006. RFC 4336 provides an introduction. Linux had an implementation of DCCP first released in Linux kernel version 2.6.14 released October 28, 2005. DCCP is useful for applications with timing constraints on the delivery of data that may become useless to the receiver if reliable in-order delivery combined with congestion avoidance is used.

Resource Locator:

- DCCP

  http://www.rfc-editor.org/rfc/rfc4340.txt

  http://www.rfc-editor.org/rfc/rfc5595.txt

  http://www.rfc-editor.org/rfc/rfc5596.txt

6.1.2.7.2 Explicit Congestion Notification (ECN)

Description:

Explicit Congestion Notification (ECN) is an extension to the Internet Protocol, allows end-to-end notification of network congestion without dropping packets contrary to the traditional TCP/IP networks signal congestion. It is only used when a mutual agreement to use it is established. When ECN is successfully negotiated, an ECN-aware router may set a bit in the IP header instead of dropping a packet in order to signal the beginning of congestion. The receiver of the packet echoes the congestion indication to the sender, which must react as though a packet drop were detected.

Standard Details:

A proposal to add Explicit Congestion Notification (ECN) to IP was suggested on September 1998, wherein congestion control is decoupled from packet loss. By doing this, packet losses will not invoke congestion control, such that transmission errors do not lead to a reduced throughput and is defined in RFC 3168 (2001).

Resource Locator:

- ECN (RFC 3168)

  http://www.rfc-editor.org/rfc/rfc3168.txt

6.1.2.7.3 Resource Reservation Protocol (RSVP)

Description:

The Resource Reservation Protocol is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. "RSVP does not transport application data but is rather an Internet control protocol. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness.

It can be used by intermediate or end users to request or deliver specific levels of quality of service (QoS) for application data streams or flows. It defines how applications place reservations and how they can relinquish the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path.

RSVP is not itself a routing protocol and was designed to interoperate with current and future routing protocols.

Standard Details:

RFC 2205: The version 1 functional specification was described in RFC 2205 (Sept. 1997) by IETF. Version 1 describes the interface to admission (traffic) control that is based "only" on resource availability. Later RFC2750 extended the admission control support. RFC 2210 defines the use of RSVP with controlled-load RFC

2211 and guaranteed RFC 2212 QoS control services. More details in Integrated Services. Also defines the usage and data format of the data objects (that carry resource reservation information) defined by RSVP in RFC 2205.

Resource Locator:

- RSVP (RFC 2205)

  http://www.rfc-editor.org/rfc/rfc2205.txt

6.1.2.7.4 Stream Control Transmission Protocol (SCTP)

Description:

The Stream Control Transmission Protocol serves similar roles as the TCP and UDP protocols. Indeed, it provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with congestion control.

Standard Details:

The protocol was defined by the IETF Signaling Transport (SIGTRAN) working group in 2000, and is maintained by the IETF Transport Area (TSVWG) working group. RFC 4960 defines the protocol. RFC 3286 provides an introduction. In the absence of native SCTP support in operating systems it is possible to tunnel SCTP over UDP, as well as mapping TCP API calls to SCTP ones.

Resource Locator:

- SCTP (RFC 4960)

  http://www.rfc-editor.org/rfc/rfc4960.txt

6.1.2.7.5 Transmission Control Protocol (TCP)

Description:

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

Standard Details:

The Transmission Control Protocol/Internet Protocol (TCP/IP) originated in the 1970's. It was initially developed by the Department of Defence (DOD) in an attempt to connect a number of different networks today, however, it is more commonly used as a standard communication protocol used in a number of networks the most common of which is the Internet.

Resource Locator:

- TCP (RFC 0793)

  http://www.rfc-editor.org/rfc/rfc0793.txt

6.1.2.7.6 User Datagram Protocol (UDP)

Description:

The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet.

Standard Details:

In the history of TCP/IP there was only one protocol that handled the functions now performed by both IP and TCP. This protocol, itself called TCP, provided network-layer connectivity like IP, and also established connections, provided reliability and took care of the typical transport-layer "quality" requirements.

It didn't take long to notice that mixing these functions together was a mistake. While most conventional applications needed the classic transport-layer reliability functions, some did not. These features introduced overhead, which would have to be endured even by the applications where reliability features were not needed at all which could have been a problem even with the small amount of lost performance. Hence, the solution was to separate the original protocol into IP and TCP. Basic internetworking was to be done by IP, and the reliability features by TCP. This paved the way for the creation of an alternative transport-layer protocol for applications that didn't want or need the features provided by TCP. This, of course, is the User Datagram Protocol (UDP).

Resource Locator:

- UDP (RFC 0768)

  http://www.rfc-editor.org/rfc/rfc0768.txt

6.1.2.7.7 Xpress Transport Protocol (XTP)

Description:

Xpress Transport Protocol (XTP) is a transport layer protocol for high-speed networks. It provides protocol options for error control, flow control, and rate control. It controls packet exchange patterns to produce different models, e.g. reliable datagrams, transactions, unreliable streams, and reliable multicast connections.

Standard Details:

It was promoted by the XTP Forum developed to replace TCP. XTP was developed to address issues about long latency in satellite communication. It works by the receiver detecting missing data packets and transmitting a list of those missing packets to the sender, who then is able to quickly resend missing packets as needed. As stated, XTP also provides rate control in which the maximum bandwidth can be specified as well as what size burst data can be accepted and offers a reliable multicast protocol, and the flexibility to match any specific application needs.

Resource Locator:

- XTP

  http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=558148

6.1.2.8 Internet Layer Protocols

6.1.2.8.1 Internet Control Message Protocol (ICMP)

Description:

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached. ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6.

Standard Details:

Best-designed systems still encounter problems. Incorrect packets are occasionally sent, hardware devices have problems, routes are found to be invalid, and so forth. IP devices also often need to share specific information to guide them in their operation, and to perform tests and diagnostics. However, IP itself includes no provision to allow devices to exchange low-level control messages. Instead, these features are provided in the form of a "companion" protocol to IP called the Internet Control Message Protocol (ICMP).

Resource Locator:

- ICMP (RFC 0792)

  http://www.rfc-editor.org/rfc/rfc0792.txt

6.1.2.8.2 Internet Group Management Protocol (IGMP)

Description:

The Internet Group Management Protocol is a protocol used for managing the IP multicast groups. It is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, operating above the network layer. It is analogous to ICMP for unicast connections. It can also be used for online streaming video, gaming and allows more efficient use of resources when supporting these types of applications. IGMP is only needed for IPv4 networks, as multicast is handled differently in IPv6 networks.

Standard Details:

There are three versions of IGMP, as defined by RFC documents of the Internet Engineering Task Force (IETF). IGMP v1 is defined by RFC 1112, IGMP v2 is defined by RFC 2236 and IGMP v3 is defined by RFC 3376.IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of IP addresses only.

Resource Locator:

- IGMP (RFC 3376)

  http://rfc-editor.org/rfc/rfc3376.txt

- IGMP (RFC 4604)

  http://rfc-editor.org/rfc/rfc4604.txt

6.1.2.8.3 Internet Protocol (IP)

Description:

The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internetwork. It is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagram's (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is being deployed actively worldwide.

Standard Details:

IPv6 ,sometimes also called the Next Generation Internet Protocol or IPng was Recommendatory by the IPng Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994 in RFC 1752 and the core set of IPv6 protocols were made an IETF Draft Standard on August 10, 1998. IPv6 is a new version of IP which is designed to be an evolutionary step from IPv4. It is a natural increment to IPv4.

It is Recommendatory to use IPv6 to communicate packet across network and should be backward compatible to IPv4.

Resource Locator:

- IPv4(RFC 791)

  http://www.rfc-editor.org/rfc/rfc791.txt

- IPv6(RFC 2460)

  http://www.rfc-editor.org/rfc/rfc2460.txt

6.1.2.8.4 Intermediate System-Intermediate System (IS-IS)

Description:

Is-Is is a protocol used by network devices (routers) to determine the best way to forward data grams through a packet-switched network. It runs over data link layer. IS-IS is an Interior Gateway Protocol (IGP) meaning that it is intended for use within an administrative domain or network.

Standard Details:

The IS-IS protocol was developed by Digital Equipment Corporation as part of DECent Phase V and was standardized by the ISO in 1992 as ISO 10589 for communication between network devices termed Intermediate Systems. IS-IS was developed at roughly the same time that the IETF was developing a similar protocol called OSPF. IS-IS was later extended to support routing of datagram using IP Protocol, the basic routed protocol of the global (public) Internet. This version of the IS-IS routing protocol was then called Integrated IS-IS (RFC 1195).

Resource Locator:

- IS-IS (RFC 1142)

  http://www.rfc-editor.org/rfc/rfc1142.txt

6.1.2.8.5 Multi Protocol Label Switching – OAM (MPLS-OAM)

Description:

OAM is a set of functions designed to monitor network operation in order to detect network faults and measure its performance. It simplifies the network operation, check the network performance and reduce the network operation cost. As Ethernet evolves from enterprise-level LANs to carrier-class networks and services, it requires automated end-to-end management and monitoring by service providers. Its functionality allows network operators to measure quality of service attributes such as Availability, Frame Delay, Frame Delay Variation and Frame Loss. Effective end-to-end service control also enables carriers to avoid expensive truck rolls to locate and contain faults thereby facilitating reduction of maintenance costs. Intrinsic OAM functionality is therefore essential in any carrier class technology and is a 'must have' capability in intelligent Ethernet network termination units.

Standard Details:

This Recommendation provides mechanisms for user-plane OAM functionality in Ethernet networks according to the requirements and principles given in Recommendation Y.1730. This Recommendation is designed specifically to support point-to-point connections and multipoint connectivity. The OAM mechanisms defined in this Recommendation offer capabilities to operate and maintain the network

Resource Locator:

- MPLS-OAM (ITU-T Y.1731)

  www.itu.int/itudoc/itu-t/aap/sg13aap/recaap/y1731/

6.1.2.8.6 Multi Protocol Label Switching –Traffic Engineering (MPLS-TE)

Description:

MPLS TE allows the MPLS-enabled network to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks. MPLS uses the reach ability information provided by Layer 3 routing protocols and operates like a Layer 2 ATM network. With MPLS, TE capabilities are integrated into Layer 3, which can be implemented for efficient bandwidth utilization between routers in the SP network.

Standard Details:

The RFC document presents a set of requirements for Traffic Engineering over Multiprotocol Label Switching (MPLS). It identifies the functional capabilities required to implement policies that facilitate efficient and reliable network operations in an MPLS domain. These capabilities can be used to optimize the utilization of network resources and to enhance traffic oriented performance characteristics.

Resource Locator:

- MPLS-TE(RFC 2702)

  http://www.rfc-editor.org/rfc/rfc2702.txt

6.1.2.8.7 Multicast source Discovery Protocol (MSDP)

Description:

The Multicast Source Discovery Protocol (MSDP) describes a mechanism to connect multiple PIM Sparse-Mode (PIM-SM) domains together. MSDP may be used with protocols other than PIM-SM. The purpose of this topology is to allow domains to discover multicast sources from other domains. If the multicast sources are of interest to a domain which has receivers, the normal source-tree building mechanism in PIM-SM will be used to deliver multicast data over an inter-domain distribution tree.

Standard Details:

The purpose of this topology is to allow domains to discover multicast sources from other domains. If the multicast sources are of interest to a domain which has receivers, the normal source-tree building mechanism in PIM-SM will be used to deliver multicast data over an inter-domain distribution tree.

Resource Locator:

- MSDP (RFC 3618)

  http://www.rfc-editor.org/rfc/rfc3618.txt

6.1.2.8.8 Protocol Independent Multicast (PIM)

Description:

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as the Border Gateway Protocol (BGP).

Standard Details:

PIM-DM is a multicast routing protocol that uses the underlying unicast routing information base to flood multicast datagrams to all multicast routers. Prune messages are used to prevent future messages from propagating to routers without group membership information.

Resource Locator:

- PIM-SM (RFC 2362)

  http://www.rfc-editor.org/rfc/rfc2362.txt

- PIM-DM (RFC 3973)

  http://www.rfc-editor.org/rfc/rfc3973.txt

6.1.2.8.9 Quality of Service (QoS)

Description:

Quality of Service refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Standard Details:

IEEE 802.1p is a 3 bit field within an Ethernet frame header when using tagged frames on an 802.1 network. It specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

It is Recommendatory that voice packets should be priority than data packets, thus configure the QoS as per the prioritization of packets that take a higher bandwidth first and go to the least in a descending order.

Resource Locator:

- QoS(IEEE 802.1p)

  http://www.ieee802.org/1/pages/802.1P.html

6.1.2.8.10 Resource Reservation Protocol – Traffic Engineering (RSVP-TE)

Description:

Resource Reservation Protocol - Traffic Engineering is an extension of the RSVP protocol for traffic engineering. It supports the reservation of resources across an IP network. It runs on both IPv4 and IPv6. RSVP-TE generally allows the establishment of MPLS label switched paths (LSPs), taking into consideration network constraint parameters such as available bandwidth and explicit hops.

Standard Details:

This document (RFC 5151) describes procedures and protocol extensions for the use of Resource Reservation Protocol-Traffic Engineering (RSVP-TE) signaling in Multiprotocol Label Switching-Traffic Engineering (MPLS-TE) packet networks and Generalized MPLS (GMPLS) packet and non-packet networks to support the establishment and maintenance of Label Switched Paths that cross domain boundaries.

Resource Locator:

- RSVP-TE (RFC5151)

  http://www.rfc-editor.org/rfc/rfc5151.txt

6.1.2.8.11 Source- Specific Multicast (SSM)

Description:

Source-specific multicast (SSM) is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security.

Standard Details:

Source specific multicast (SSM) has been introduced to overcome the issues in any source multicast (ASM) such as security, deployment complexity and address allocation. However, the scalability issue of SSM still poses a problem. To solve this state scalability problem, a scheme called aggregated multicast is proposed. The key idea is that multiple groups are forced to share a single delivery tree. In this paper, the basic idea of SSM and ASSM is give and a comparison between both is done. Based on what we have done, we conclude that aggregated multicast is an effective way to solve the scalability issue of SSM. However, it may suffer from routers under utilization problem. To achieve higher routers utilization, this paper proposes a new approach. The new approach was also discussed.

Resource Locator:

- SSM(RFC 4607)

  http://www.rfc-editor.org/rfc/rfc4607.txt

6.1.2.8.12 Virtual Router Redundancy Protocol (VRRP)

Description:

Virtual Router Redundancy Protocol is designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time.

Enterprises using a proprietary failover routing redundancy protocols may be a challenge for interoperability either between other enterprises or different equipments within their own Network.

Standard:

VRRP is based on Cisco's proprietary HSRP concepts. IETF (RFC 3768) designed this protocol to bring resiliency and redundancy to Layer 3 routers and switches that are run as statically configured default gateways. VRRP is actually a standardized version of Cisco's HSRP. Those protocols, while similar in concept, are not compatible.

It is Recommendatory to use an open standard failover routing protocol such as VRRP mentioned in this document for a seamless interconnection between different vendor equipments.

Resource Locator:

- VRRP (RFC 3768)

  http://www.rfc-editor.org/rfc/rfc3768.txt

6.1.2.9 Link Layer Protocols

6.1.2.9.1 Address Resolution Protocol (ARP)

Description:

Address Resolution Protocol is an internet Protocol used to map an IP address to a MAC address. ARP is a Link Layer protocol because it only operates on the local area network or point-to-point link that a host is connected to. The basic operation of ARP involves encoding the IP address of the intended recipient in a broadcast message. It is sent on a local network to allow the intended recipient of an IP datagram to respond to the source with its data link layer address.

Standard Details:

There are two basic methods that resolution could have been used to accomplish the correlation of addresses: direct mapping or dynamic resolution. However, Ethernet addresses are 48 bits long while IP addresses are only 32 bits, which immediately rules out direct mapping. Furthermore, the designers of IP wanted the flexibility that results from using the dynamic resolution model. To this end, they developed the TCP/IP Address Resolution Protocol (ARP). This protocol is described in one of the earliest of the Internet RFCs still in common use: RFC 826, An Ethernet Address Resolution Protocol, published in 1982.

Resource Locator:

- ARP (RFC 5494)

  http://rfc-editor.org/rfc/rfc5494.txt

6.1.2.9.2 Fiber Distributed Data interface (FDDI)

Description:

Fiber distributed data interface (FDDI) provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). A FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles). FDDI has a larger maximum-frame size than standard 100 Mbit/s Ethernet, allowing better throughput.

Standard Details:

X3T9.5 (American National Standards Institute standard for FDDI) conforms to the Open Systems Interconnection (OSI) model of functional layering of LANs using other protocols. FDDI-II, a version of FDDI, adds the capability to add circuit-switched service to the network so that it can also handle voice and video signals. Work has started to connect FDDI networks to the developing Synchronous Optical Network (SONET).

Resource Locator:

- FDDI

  www.t13.org/Documents/UploadedDocuments/meetings/d97003.doc

6.1.2.9.3 Layer 2 Tunnelling Protocol (L2TP)

Description:

Layer 2 Tunnelling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Standard Details:

Published in 1999 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for PPP: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3, was published as proposed standard RFC 3931 in 2005. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (e.g., Frame Relay, Ethernet, ATM, etc).

Resource Locator:

- L2TP (RFC 3931)

  http://www.rfc-editor.org/rfc/rfc3931.txt

6.1.2.9.4 Multiprotocol Label Switching (MPLS)

Description:

Multiprotocol Label Switching (MPLS) is a mechanism which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols. It is a highly scalable, protocol agnostic, data-carrying mechanism where it assigns labels and packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol.

Standard Details:

MPLS was originally proposed by a group of engineers from Ipsilon Networks, but their "IP Switching" technology, which was defined only to work over ATM, did not achieve market dominance. Cisco Systems, Inc., introduced a related proposal, not restricted to ATM transmission, called "Tag Switching". It was a Cisco proprietary proposal, and was renamed "Label Switching". It was handed over to the IETF for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors' work.

Resource Locator:

- MPLS (RFC 3031)

  http://www.rfc-editor.org/rfc/rfc3031.txt

6.1.2.9.5 Neighbor Discovery Protocol (NDP)

Description:

The Neighbor Discovery Protocol (NDP) is responsible for discovery of other nodes on the link, determining the link layer addresses of other nodes, finding available routers, and maintaining reach ability information about the paths to other active neighbor nodes.NDP performs functions for IPv6 similar to the way Address Resolution Protocol (ARP) and ICMP Router Discovery and Router Redirect protocols do for IPv4.

Standard Details:

This standard is an evolution of the vulnerable Internet Protocol. It maintains the same basic operational principles of IPv4, but makes some important modifications, particularly in the area of addressing. In fact, some of the more significant changes in IPv6 are actually not in the IP protocol itself, but in the protocols that support IP. One of the most interesting of these was the creation of an entirely new support protocol for IPv6. It combines several tasks previously performed by other protocols in IPv4, adds some new functions, and makes numerous improvements to the whole package. This new standard is called the IPv6 Neighbor Discovery (ND) protocol.

Resource Locator:

- NDP (RFC 4861)

  http://rfc-editor.org/rfc/rfc4861.txt

6.1.2.9.6 Open Shortest Path First (OSPF)

Description:

Open Shortest Path First (OSPF) is a dynamic routing protocol for use in Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol and falls into the group of interior gateway protocols, operating within a single autonomous system (AS).

Standard Details:

The IETF recognized that RIP by itself simply would not meet the needs of all autonomous systems on the Internet, hence formed working group to develop a new routing protocol in 1988 based on the link-state algorithm. This new protocol was called Open Shortest Path First, or OSPF, and its name conveys two of its most important characteristics. The first word refers to the fact that the protocol, like all TCP/IP standards, was developed using the open and public RFC process, so it is not proprietary and no license is required to use it. The SPF portion of the name refers to the type of algorithm it uses, which is designed to allow routers to dynamically determine the shortest path between any two networks.

The first version of OSPF was described in RFC 1131, published in October 1989. This was quickly replaced by OSPF Version 2 in July 1991, described in RFC 1247. Since then there have been several revisions to the OSPF Version 2 standard, in RFCs 1583, 2178, and 2328, with the last of these the current standard. OSPF Version 2 and OSPF Version 3 are the versions in use today.

Resource Locator:

- OSPF v3 (RFC 5340)

  http://www.rfc-editor.org/rfc/rfc5340.txt

- OSPFv2 (RFC 5709)

  http://www.rfc-editor.org/rfc/rfc5709.txt

6.1.2.9.7 Point-to- point Protocol (PPP)

Description:

It is commonly used to establish a direct connection between two networking nodes. It can provide connection authentication, transmission encryption privacy, and compression. It is used over many types of physical networks including serial cable, phone line, trunk line etc.

Standard Details:

PPP was originally emerged as an encapsulation protocol for transporting IP traffic between two peers. It is a data link layer protocol (layer 2 in the OSI model) in the TCP-IP protocol suite over synchronous modem links, as a replacement for the non-standard layer 2 protocol SLIP. However, other protocols other than IP can also be carried over PPP, including DECnet and Novell's Internetwork Packet Exchange (IPX).

Resource Locator:

- PPP (RFC 1661)

  http://www.rfc-editor.org/rfc/rfc1661.txt

6.1.2.9.8 Reverse Address Resolution Protocol (RARP)

Description:

The Inverse Address Resolution Protocol (InARP/RARP), is a protocol used for mapping MAC address to an IP address. The packet formats are the same as ARP; only the operation code and the certain field values differ.

Standard Details:

It is primarily used in Frame Relay and ATM networks, where Layer 2 addresses of virtual circuits are sometimes obtained from Layer 2 signalling, and the corresponding Layer 3 addresses must be available before these virtual circuits can be used. RARP was obsolete by BOOTP which itself has been superseded by the Dynamic Host Configuration Protocol (DHCP).

Resource Locator:

- RARP (RFC 2390)

  http://rfc-editor.org/rfc/rfc2390.txt

6.1.2.9.9 Rapid Spanning-tree Protocol (RSTP)

Description:

Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. It is typically able to respond to changes within a second.

Standard Details:

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard. The 802.1D terminology remains primarily the same. Most parameters have been left unchanged so users familiar with 802.1D can rapidly configure the new protocol comfortably. In most cases, RSTP performs better than proprietary extensions of Cisco without any additional configuration. 802.1w can also revert back to 802.1D in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

Resource Locator:

- RSTP (IEEE 802.1w)

  http://www.ieee802.org/1/pages/802.1w.html

6.1.2.9.10 Spanning Tree protocol (STP)

Description:

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN.

Standard Details:

802.1D is the IEEE MAC Bridges standard which includes Bridging, Spanning Tree and others. It is standardized by the IEEE 802.1 working group. It includes details specific to linking many of the other 802 projects including the widely deployed 802.3 (ethernet), 802.11 (WiFi) and 802.16 (WiMax) standards.

Resource Locator:

- STP (IEEE 802.1D)

  http://www.ieee802.org/1/pages/802.1D-2003.html

6.1.2.9.11 VLAN Trunk

Description:

VLAN Tagging or Trunk is a networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks.

Standard Details:

Large networks use up a lot of bandwidth and are slow. It is desirable to break up these huge LANs into smaller, more manageable networks. To address this problem, the 802.1Q standard was developed as a part of IEEE 802. This standard enables large LANs to be broken into much smaller "fragments." These fragments can broadcast and multicast at a much lower bandwidth. Fragmenting the LAN using this protocol also provides a much more secure environment between the segments of the internal network.

Resource Locator:

- Vlan Trunk (IEEE 802.1 Q)

  http://www.ieee802.org/1/pages/802.1Q.html

Table 6-9: Integrated systems (Telecom+Enterprise)

Integrated systems (Telecom + Enterprise)		
Standards Proposed	Mandatory/ Recommendatory	Reference & Links to Interconnection – Telecom and Enterprise Technical Standards Details
Internet Service Provider Standards		
ETC's web hosting should be used to make websites accessible through browsers.	Mandatory	4.1.3.1.1 Web hosting
.et domain should be used to convert domain names to IP addresses.	Mandatory	4.1.3.1.2 Domain Registration & Services
Electronic commerce can be considered as the main interface for buying and selling of products in the near future.	Recommendatory	4.1.3.1.3 E-Commerce Services
Financial Interconnectivity System Standards		
Wireless communication should be employed as a convenient and high efficient communication/interconnectivity method.	Mandatory	4.1.3.2.1 ATM Standards
EMV standard should be used for interoperation of IC cards ("Chip cards") and IC capable POS terminals and ATMs, for authenticating credit and debit card payments.	Recommendatory	4.1.3.2.2 IC Card System Standards

6.1.3 Integrated System Standards

6.1.3.1 Internet Service Providers Standards

6.1.3.1.1 Website Hosting

Description:

A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their own website accessible via the World Wide Web. Web hosts are companies that provide space on a server they own or lease for use by their clients as well as providing Internet connectivity, typically in a data center. Web hosts can also provide data center space and connectivity to the Internet for servers they do not own to be located in their data center, called co-location.

Today, the web hosting services from ETC is very limited and lacks the capability of growing from hundreds to millions of subscribers.

Standard Details:

A summary of the standards that service provider will:

- Be highly reliable with at least 99.5% service uptime.
- Only offer plans that they have the resources to support.
- Use controlled overselling that can be supported.
- Charge reasonable bandwidth over usage fees.
- ONLY allow legal files (hosts that host illegal files and sites can get shut down and are very unreliable).

- Promptly inform customers about any changes to the T&C and/or their plan.
- Provide accurate and up-to-date hosting product information.
- Provide helpful solutions to sales and support requests.
- Honor the money-back guarantee period specified (if any).
- Provide clear and proper billing.
- Provide Secure Sockets Layer (SSL) encryption during payment transactions.
- Resolve customer disputes promptly and professionally.
- Pro-actively monitor services to ensure maximum server performance and uptime.
- Safeguard customer privacy by not sharing, renting or selling client information.

Any hosting service provider that can follow the above standards will be highly reliable. Since the ISP standard differs from country to country, Nepal needs to create one based on the country's broadcasting policy and regulation.

We recommend using one of the countries listed on the leading practice as model and developing a web hosting service standard and policy to create scalable and reliable hosting services.

6.1.3.1.2 Domain Registration & Services

Description:

A domain name registry is a database of all domain names registered in a top-level domain. A registry operator, also called a Network Information Center (NIC), is the part of the Domain Name System (DNS) of the Internet that keeps the database of domain names, and generates the zone files which convert domain names to IP addresses. Each NIC is an organisation that manages the registration of Domain names within the top-level domains for which it is responsible, controls the policies of domain name allocation, and technically operates its top-level domain. It is potentially distinct from a domain name registrar. Domain names are managed under a hierarchy headed by the Internet Assigned Numbers Authority (IANA), which manages the top of the DNS tree by administrating the data in the root nameservers. IANA also operates the .int registry for intergovernmental organisations, the .arpa zone for protocol administration purposes, and other critical zones such as root-servers.net. IANA delegates all other domain name authority to other domain name registries such as VeriSign. Country code top-level domains (ccTLD) are delegated by IANA to national registries such as DENIC in Germany, or Nominet in the United Kingdom.

As of today, most of the local citizens have an external domain. The .et domain and sub domain has not been utilized as it should be.

Standard Details:

Generally, domain name registries operate a first-come-first-served system of allocation but may reject the allocation of specific domains on the basis of political, religious, historical, legal or cultural reasons. For example, in the United States, between 1996 and 1998, InterNIC automatically rejected domain name applications based on a list of perceived obscenities. Registries may also control matters of interest to their local communities: for example, the German, Japanese and Polish registries have introduced internationalized domain names to allow use of local non-ASCII characters.

Domain name registries may also impose a system of second-level domains on users. DENIC, the registry for Germany (.de), does not impose second level domains. AFNIC, the registry for France (.fr), has some second level domains, but not all registrants have to use them, and Nominet UK, the registry for the United Kingdom (.uk), requires all names to have a second level domain (e.g. .co.uk or .org.uk)

Registrants of second-level domains sometimes act as a registry by offering sub-registrations to their registration. For example, registrations to .fami.ly are offered by the registrant of fami.ly and not by GPTC, the registry for Libya (.ly).

It is Recommendatory to create a strong policy that will allow the country to utilize the .et domain and sub domain for all citizens.

6.1.3.1.3 e-Commerce Services

Description:

Electronic commerce, commonly known as (electronic marketing) e-commerce or eCommerce, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. The use of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at some point in the transaction's lifecycle, although it can encompass a wider range of technologies such as e-mail as well.

Due to lack of connectivity in the country, almost no business or governmental organization uses e-commerce for online business.

Standard Details:

e-Business interoperability consortium OASIS defined the standard of a royalty-free data method for international electronic commerce has been released by one of its technical groups. The new OASIS schemas encompass the Universal Business Language (UBL). UBL is a standard for XML (define) document formats that encode business messages, such as purchase orders and invoices. UBL treats business-to-business (B2B) communication across all industry sectors and domains for all types of organizations, including small- and medium-sized enterprises.

In addition to the ebXML Core Components, UBL built on the commercial XML Common Business Library, or xCBL, schemas from Commerce One and SAP; early XSL (define) stylesheet implementations; and the UBL Liaisons Subcommittee.

Since the country is going through under major infrastructure construction, it is Recommendatory that the use of e-commerce to began developing and commercialized.

Resource Locator:

- xCBL

  http://www.xcbl.org/

- UBL

  http://oasis-open.org/committees/ubl/lsc/

6.1.3.2 Financial Interconnectivity System Standards

6.1.3.2.1 ATM Standards

Description:

As competition in today's financial field heats up, major financial institute have started to center on their service, providing value-added services and convenient means to satisfy customer requirements, of which the financial self-service has become one of the most important channels of financial institute services. Today major banks have enlarged the implementation of convenient ATM. In this case, banks and ATM operators have to face such communication problems: How to realize the ATM network conveniently and promptly? How to reduce the communication cost? How to ensure the communication security?

Recently wireless communication has been employed in many fields as a convenient and high efficient communication/interconnectivity method.

Today all financial institutes in Nepal uses independent and proprietary based teller machine/system which is not cost effective and interoperable to other firm's teller machine.

Standard Details:

ATM networks have changed very little since the ATM technology was first introduced. Similarly, the business models of vendors in the ATM market, and the relationships between hardware and software, vendors and banks, have remained fairly static. But recent changes in technology, and the introduction of open standards into the ATM device and network architecture, have the potential to realise a new dawn in ATM channel functionality and efficiency.

It is Recommendatory that to minimize the CAPEX and OPEX as well as to create interoperability among all financial institutes, it is Recommendatory to use central teller machines and use open standard platform so all financial institute can interface to the central teller machine such as ATM. As it was mention in the description, it also advised to use secured wireless access for all financial transaction over the wired connection. Some of the Recommendatory technologies are:

- Mobile network access technology: This technology provides access to 2.5G mobile communication network (CDMA), internet access, and the access bandwidth according with that of the bearing network, to support a new network and realize high-speed mobile access.
- VPN: VPN technology, basing on IPSec standard, is employed to realize the safe interconnection of dispersed networks and the construction of seamless industrial virtual private network.
- Connection management technology: This technology utilizes the manageable connection to help connect or disconnect at either network ends and realize on-demand connection, automatic disconnection, and manual activation.
- Disconnection detection, automatic recovery: This technology can improve the reliability of mobile data communication and solve the drop-line problem to provide a reliable communication link for the upper level application.
- Flow management technology: Aiming at the small bandwidth of mobile data communication, flow management method ensures the bandwidth requirement of key applications and high utilization efficiency of limited bandwidth by differentiating the priorities of services to adjust the data flow dynamically.
- Embedded technology: With 32-bit embedded CPU; the system hardware platform provides powerful process function. The system software platform uses embedded OS to realize safe, mature, steady and reliable service.

- Modularization implementation Technology: With modularization and standardization technologies, the system hardware and software platforms can upgrade and support new technology applications easily.

Resource Locator:

- Interactive Financial Exchange Forum

  http://www.ifxforum.org/standards/

6.1.3.2.2 IC (Integrated Circuit) Card System Standards

Description:

EMV is a standard for interoperation of IC cards ("Chip cards") and IC capable POS terminals and ATMs, for authenticating credit and debit card payments. The name EMV comes from the initial letters of Europay, MasterCard and VISA, the three companies which originally cooperated to develop the standard. Europay International SA was absorbed into Mastercard in 2002. JCB (formerly Japan Credit Bureau) joined the organization in December 2004, and American Express joined in February 2009. IC card systems based on EMV are being phased in across the world, under names such as "IC Credit" and "Chip and PIN".

Standard Details:

The EMV standard defines the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions. Portions of the standard are heavily based on the IC Chip card interface defined in ISO/IEC 7816.

The first version of EMV standard was published in 1995. Now the standard is defined and managed by the public corporation EMVCo LLC.The current members of EMVCo are JCB International, American Express, MasterCard Worldwide, and Visa, Inc. Each of these organizations owns one quarter of EMVCo and has representatives in the EMVCo organization and EMVCo working groups.

Since version 4.0, the official EMV standard documents, that define all the components in an EMV payment system, are published as four "books":

- Book 1 - Application Independent ICC to Terminal Interface Requirement and Application Selection
- Book 2 - Security and Key Management
- Book 3 - Application Specification
- Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements

Resource Locator:

- The organization responsible for developing and maintaining the standard

  http://www.emvco.com/

6.2 Data Integration

Data Integration provides for aggregation of data from disparate sources and facilitates inter organisational communication. Use of standards for representation of data and suitable converters such as Optical Character Recognizing (OCR) engines enable aggregation. It covers components and technical specifications required to support the recognition of data (txt, images, maps and multimedia.), codes, recognition methods, interpretation formats, converters and filters.

Table 6-10: Data Integration

Data Integration		
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Data Integration Technical Standards Details**
Character and encoding for information interchange		
• American Standard Code for Information Interchange (ASCII) should be used as the minimum set of characters for data interchange. • Unicode should be used for language(Amharic) support • UCS Transformation Format (UTF-8) should be used for encoding Unicode ISO 8859-1	Mandatory	4.2.1 Character and Encoding for Information interchange
Data description		
• Resource Description Framework (RDF) model should be used to define models for describing interrelationships among resources in terms of named properties and values. • Extensible Markup Language Version 1.1 and above should be used for Structured data description • Extensible Name and Address Language Version 2 (xNAL) can be used for defining name and address • Extensible Customer Information Language xCIL can be used to capture specifying formats for citizen information elements such as name, address etc. • Extensible Customer relationship Language xCRL can be used to define relationship between an Organisation and another	Mandatory	4.2.2 Data Description 4.2.2.1 RDF 4.2.2.2 XML 4.2.2.3 XNAL 4.2.2.4 XCIL 4.2.2.5 XCRL
Data exchange & Transformation		
• XML Metadata Interchange (XMI) Format should be encouraged as an open information interchange model. • ISO 8601 should be followed for data elements and interchange formats • Extensible cascaded style sheet Language transformations (xSLT) should be used for transforming XML documents into other XML document.	Mandatory	4.2.3 Data Exchange & Transformation 4.2.3.1 XMI 4.2.3.2 Data Elements 4.2.3.3 xSLT
Data exchange Formats		
• Standards Used for Data exchange formats include: - Ministries should adopt ANSI X12 and UN/EDIFACT	Mandatory	4.2.4 Data Exchange Formats 4.2.4.1 Electronic data

Data Integration		
electronic data interchange (EDI) standards for international compatibility. XML/EDI can be considered for future use for using XML for Electronic data interchange through XML - PDF can be used for accessing non-editable documents - MS office document type such as Doc, XLS, and PPT can be used for inter-departmental information interchange between users of Microsoft office product. In the future, Open document format for office application can be considered. - Tagged Image File Format (TIFF/IT) can be used for facsimile and scanned documents(especially useful for archiving and digitization) - Graphic Interchange Format (GIF) and Joint Photographic Experts Group (JPEG) for raster based color documents, drawings, graphic image, photographs etc. - RTF can be used for editable word processing documents format for text and graphics interchange - Initial Graphics Exchange Specification (IGES) and DXF should be used for computer aided design documents - Moving Picture Experts Group (MPEG) should be used for moving images and audio - PST and CSV should be used as a standard for interdepartmental information interchange. (usually through Email exchange) - Computer Graphics Metafile (CGM) and Scalable Vector Graphics (SVG) for editable vector based graphics, 2D content, raster images and font text. - HTM should be used for publishing/presentation on the web through popular browser - AVI and MP3/MP4 format can be used for audio streaming files.		interchange 4.2.4.2 Portable document format 4.2.4.3 Office application document type 4.2.4.4 Tag Image File Format 4.2.4.5 Graphics Interchange for 4.2.4.6 Joint Photographic Experts Group 4.2.4.7 Rich text Format 4.2.4.8 Initial Graphics Exchange specification 4.2.4.9 Moving Picture and Experts Group Standard 4.2.4.10 Email Document type Standards 4.2.4.11 Computer Graphics Metafile (CGM) and WebCGM 4.2.4.12 Hyper text markup language 4.2.4.13 Audio Formats Standards
Ontology-based information exchange		
• For formal descriptions of the meaning of terminology used in web document for the automatic processing of such documents. OWL can be used with RDF for adding sematics	Recommendatory	4.2.5 Ontology-based information exchange 4.2.5 .1 OWL
Data modelling language		
- For data modeling, business modeling, object modeling and component modeling standardized general-purpose modeling language UML Should be used to specify, visualize, modify, construct and document the artifacts.	Mandatory	4.2.6 Data modelling language 4.2.6.1 UML
Data integration meta language		
• Standards Used for Data integration meta language formats include:	Mandatory	4.2.7 Data integration meta language

Data Integration		
- XML signatures - XML encryption - XML signature and encryption - XML key management where a PKI environment is used - XML security assertion mark-up - XML access control		4.2.7.1 XML-Signature Syntax and Processing 4.2.7.2 XML-DSS 4.2.7.3 XML-Encryption 4.2.7.4 Syntax and Processing Decryption Transform 4.2.7.5 XML Signature 4.2.7.6 XML-Key Management Specification 4.2.7.7 SAML 4.2.7.8 XACML
Minimum interoperable character set		
- Minimum Interoperable Character Set is required to define the minimum character sets to be used for the content to be interchanged in between related parties, e.g. agencies and departments as well as third parties such as suppliers.	Mandatory	4.2.8 Minimum interoperable character set 4.2.8.1 UTF-8
Digitization		
• This is the way to convert hard-copy or non-digital records into digital format.	Mandatory	4.2.9 Digitization
Data Definition for Smart Cards		
• The following standards are Recommendatory for data definition aspects for smart card applications: - ISO/IEC 7816-6 - ISO/IEC 7812-1 Additionally the following standards can be considered for review for future versions: - EN 1546-3 - EN 1546-4	Recommendatory	4.2.10 Smart Cards

6.2.1 *Character and encoding for information interchange*

Description:

Character and encoding for information interchange standards help to define the minimum character sets to be used for the content to be interchanged in between related parties, e.g. agencies and ministries etc and to allow computers to consistently represent and manipulate text expressed in most of the world's writing systems.

Standard Details:

6.2.1.1 ASCII

American Standard Code for Information Interchange (ASCII) should be used as the minimum set of characters for data interchange.

Unicode

Unicode provides a unique number for every character, irrespective of the platform, the program and the language. Unicode consists of a repertoire of more than 100,000 characters, a set of code charts for visual reference, an encoding methodology and set of standard character encodings. Unicode is required by modern standards such as XML, Java, ECMA Script (JavaScript), LDAP, CORBA 3.0, WML, etc., and is the official way to implement ISO/IEC 10646. It is supported in many operating systems, all modern browsers, and many other products. The emergences of the Unicode Standard, and the availability of tools supporting it, are among the most significant recent global software technology trends.

Incorporating Unicode into client-server or multi-tiered applications and websites offers significant cost savings over the use of legacy character sets. Unicode enables a single software product or a single website to be targeted across multiple platforms, languages and countries without re-engineering. It allows data to be transported through many different. The latest version of the Unicode Standard is Version 5.2.0. This is a consolidated version of the standard, incorporating all changes into the full text.

6.2.1.2 UCS Transformation Format (UTF-8)

UTF should be used for encoding Unicode ISO 8859-1. ISO/IEC 10646-1 defines a multi-octet character set called the Universal Character Set (UCS) which encompasses most of the world's writing systems. Multi-octet characters, however, are not compatible with many current applications and protocols, and this has led to the development of a few so-called UCS transformation formats (UTF), each with different characteristics. UTF-8, the object of this memo, has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values.

This memo updates and replaces RFC 2044, in particular addressing the question of versions of the relevant standards.

Resource Locator:

- ASCII
  http://www.columbia.edu/kermit/ascii.html
- UTF

  http://www.ietf.org/rfc/rfc2279.txt
- Unicode

  http://www.unicode.org/

  http://www.unicode.org/versions/Unicode5.2.0/

6.2.2 Data Description

In order to facilitate information sharing and retrieval, it is necessary to have standard descriptions to avoid ambiguity in describing data resource. Data description language will be referred to when defining documents, business specific schemas etc. to ensure consistent understanding and terminology. Standard on Data Description is required to enable applications to exchange metadata and can be used in a variety of application scenarios e.g. to provide better search capabilities or in knowledge management. The standard defines the languages/frameworks which are used to represent that metadata.

6.2.2.1 RDF

Description:

Resource Description Framework (RDF) is a general method for conceptual description or modeling of information that is implemented in web resources, using a variety of syntax formats. RDF model should be used to define models for describing interrelationships among resources in terms of named properties and values.

Standard Details:

The Resource Description Framework (RDF) integrates a variety of applications from library catalogs and world-wide directories to syndication and aggregation of news, software, and content to personal collections of music, photos, and events using XML as interchange syntax. The RDF specifications provide a lightweight ontology system to support the exchange of knowledge on the Web.

It defines XML syntax for RDF called RDF/XML in terms of Namespaces in XML, the XML Information Set and XML Base. The formal grammar for the syntax is annotated with actions generating triples of the RDF graph as defined in RDF Concepts and Abstract Syntax. The triples are written using the N-Triples RDF graph serializing format which enables more precise recording of the mapping in a machine processable form. The mappings are recorded as tests cases, gathered and published in RDF Test Cases.

Resource Locator:

- RDF

  http://www.w3.org/RDF/

6.2.2.2Extensible Markup Language (XML)

Description:

According to W3C Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language [ISO 8879]. By construction, XML documents are conforming SGML documents.

XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure. It is a widely used system for defining data formats. It provides a very rich system to define complex documents and data structures. In other words, XML is a set of rules for encoding documents electronically. Extensible Markup Language Version 1.1 should be used for structured data description.

Standard Details:

XML 1.1, a deliverable of the XML Core Working Group as defined in the XML Blueberry Requirements. XML 1.1 was formerly known as XML Blueberry. The standards has to be read with other standards such as associated standards (Unicode [Unicode] and ISO/IEC 10646 [ISO/IEC 10646] for characters, Internet RFC 3066 [IETF RFC 3066] for language identification tags, ISO 639 [ISO 639] for language name codes, and ISO 3166 [ISO 3166] for country name codes).

Resource Locator:

- XML 1.1

  http://www.w3.org/TR/xml11/#sec-intro

6.2.2.3Extensible Name and Address Language(XNAL)

Description:

Extensible Name and Address Language (xNAL) is a universal format used to describe name and address data regardless of the origin of the country. It is based on XML for representing and managing name and address. The OASIS Customer Information Quality Committee (CIQ) was formed to consult with the industry and develop open standards for the interchange of customer data. The committee has developed three XML Standards for Customer Information/Profile Management:

- xNAL : extensible Name and Address Language
- xCIL : extensible Customer Information Language
- xCRL : extensible Customer Relationships Language

The challenge for xNAL is to provide the ability to handle the following:

- About 36+ customer name formats
- Addresses of 241+ Countries
- About 130+ Address Formats
- Represented in 5,000+ languages (dialects)
- Should be application independent, ie., capable of being used for a variety of
- applications ranging from simple user profiling to name and address parsing, matching,
- validation and postal services
- Should be Platform independent
- Should be open, and
- Should be vendor neutral.

Standard Details:

XNAL consists of two parts; **xNL**, eXtensible Name Language, to define the name components, and **xAL**, eXtensible Address Language, to define the address components. xNL is an XML specification for the interchange of address data both domestically and internationally. It is based on storing the parts of an address, or address elements, and then combining them together with intelligent editing to create output formats, or renditions, for particular mailpieces. It includes data about the addresses, such as whether they are complete or missing particular elements that affect address quality. xAL is also another XML specification for the interchange of name data of an individual / groups of people or business names both domestically and internationally.

xNAL v2.0 is Recommendatory which wile consist of extensible Name Language (xNL) Ver.2.0 and - extensible Address Language (xAL) Ver.2.0. In xNL A Name can be classified into two, namely Person Name and Organisation Name.

xAL the address specification is designed to describe the address elements, not be specific about the formatting and presentation of the address. However, formatting at the higher -composite- levels is preserved since these are either a single string value or an ordered list of multiple strings. This is only considered a side effect at this time; there is no detailed specification of how to handle and preserve white space in these strings. In the Netherlands for example, it is customary to use double spacing between postal code and town on a single line, but naturally this only works with fixed-width fonts. New lines are made explicit by only defining composite elements at line-level.

Resource Locator:

- xNAL

  http://www.oasis-open.org/committees/ciq/ciq.html#4

http://www.oasis-open.org/committees/ciq/download.html

6.2.2.4Extensible Customer Information Language(XCIL)

Description:

xCIL is an XML based specification used for the identification of a customer. Different data attributes such as telephone, e-mail address and credit card numbers etc. of the customer are stored in an XML format. Although name and address data is the key identifier of a customer, other data helps to uniquely identify a customer. Customer addresses frequently change and it is not trivial to link the customer across multiple addresses with just name information. In the example below, a customer can have two completely different addresses and it is nearly impossible to uniquely identify the customer with the name alone. Customer centric data such as telephone numbers, e-mail addresses, account numbers, credit card numbers etc. will be necessary to achieve this. This helps in achieving single customer view, customer relationship management strategies, understanding customer profile, etc.

Standard Details:

Following are the customer data elements that xCIL Standard supports:

1. Customer Name and address Details
2. Customer Identifier
3. Organisation Details (Branches, Stocks, etc)
4. Birth Details
5. Age Details
6. Gender
7. Marital Status
8. Language Details
9. Nationality Details
10. Occupation Details
11. Qualification Details
12. Passport Details
13. Religion Details
14. Ethnicity
15. Telephone Details

16. Facsimile Details

17. Cellular Phone Details

18. Pager Details

19. E-mail Details

20. URL

21. Financial Account Details

22. Identification card Details

23. Person Physical Characteristics

24. Tax number Details

25. Vehicle Information Details

26. Family Member Details

28. Income Details

29. Reference Contact Details

30. Hobbies

31. Habbits

32. Residency Details

33. Visa Details

xNAL is a subset of xCIL. xNL and xAL are referenced by xCIL

Resource Locator:

- XCIL

  http://www.oasis-open.org/committees/ciq/ciq.html#7

6.2.2.5Extensible Customer Relationship Language(XCRL)

Description:

Customer relationship management is the key to build effective customer relationships.

Customer relationships could be categorised into the following:

- Organisation to Organisation Relationship
- Organisation to Person Relationship, and
- Person to Person Relationship

A standard way to represent customer relationship helps to achieve interoperability between different systems, processes and platforms and in building effective single customer views. There are no standards for representing customer relationship and hence, this work attempts to define a standard in XML to capture and represent such relationships.

Standard Details:

The Standards covers the following relationship

- Contact Management
- Person to Person Relationship
- Person to Organisation Relationship
- Organisation to Organisation Relationship.

xNL, xAL and xCIL are referenced by xCRL.

Resource Locator:

- xCRL

  http://www.oasis-open.org/committees/ciq/download.shtml

6.2.3 *Data exchange & Transformation*

Data exchange & transformation standards are standards that will enable easy exchange/interchange of data between systems.

6.2.3.1 XML Metadata Interchange(XMI)

Description:

XMI is an OMG standard for exchanging metadata information through XML. It is a standard which defines how to serialize object instances. Although XML is a very good way to store information in a tree structured way, it is not object oriented. XMI extends XML to make it object oriented. The purpose of XMI is to enable easy interchange of metadata between UML-based modeling tools and MOF-based metadata repositories in distributed heterogeneous environments.

Standard Details:

XMI integrates four industry standards:

- XML - eXtensible Markup Language, a W3C standard.
- UML - Unified Modeling Language, an OMG modeling standard.
- MOF - Meta Object Facility, an OMG language for specifying metamodels.
- MOF Mapping to XMI.

The XMI, v2.1.1 specification was produced in response to an urgent issue. The changes based on this issue are marked with change bars. This specification represents a revision to the XML Metadata Interchange (XMI), v2.1 specification (formal/05-09-01). XMI is now ISO/IEC 19503:2005 Information technology standard.

Resource Locator:

- XMI

  http://www.omg.org/technology/documents/formal/xmi.htm http://www.omg.org/cgi-bin/doc?formal/2007-12-02

6.2.3.2Data Elements and Interchange Formats

Description:

The Data elements and interchange formats Information interchange and Representation of dates and times and was issued by the International Organization for Standardization (ISO). ISO 8601 is followed for data elements and interchange formats. The purpose of this Standard is to eliminate the risk of misinterpretation where numeric representation of dates and times are interchanged across national boundaries, and to avoid the confusion and other consequential errors or losses. The standard organizes the data so the largest temporal term (the year) appears first in the data string and progresses to the smallest term (the second). It also provides for a standardized method of communicating time-based information across time zones by attaching an offset to Coordinated Universal Time (UTC).

Standard Details:

The standard represents dates in the Gregorian calendar, times in the 24-hour timekeeping system, time intervals and recurring time intervals. This standard does not cover dates and times where words are used in the representation and dates and times where characters are not used in the representation. And it also does not assign any particular meaning or interpretation to any data element that uses representations. The salient basis of this standard are

- Date and time values are organized from the most to the least significant: year, month (or week), day, hour, minute, second, and fraction of second. The lexicographical order of the representation thus corresponds to chronological order, except for date representations involving negative years.

- Each date and time value has a fixed number of digits that must be padded with leading zeros.

- Representations can be done in one of two formats—a basic format with a minimal number of separators or an extended format with separators added to enhance human readability.[4] The separator used between date values (year, month, week, and day) is the hyphen, while the colon is used as the separator between time values (hours, minutes, and seconds). For example, the 6th day of the 1st month of the year 2009 may be written as "2009-01-06" in the extended format or simply as "20090106" in the basic format without ambiguity. The extended formats are preferred over the basic formats not only for human readability, but because some basic formats can appear to be ambiguous to those unfamiliar with the standard.

- For reduced accuracy, any number of values may be dropped from any of the date and time representations, but in the order from the least to the most significant. For example, "2004-05" is a valid ISO 8601 date, which indicates the 5th month of the year 2004. This date will never represent the 5th day of some unknown month in 2004.

- When higher precision is needed, the standard supports the addition of a decimal fraction to the smallest time value in the representation.

Resource Locator:

- ISO 8601

  http://www.iso.org/ISO8601:2004

6.2.3.3 Extensible cascaded style sheet Language transformations (XSLT)

Description:

XSL is a family of recommendations for defining XML document transformation and presentation. An XSLT style sheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses a formatting vocabulary, such as (X) HTML or XSL-FO.in short it's a language for transforming XML documents into other XML documents. XSLT is also designed to be used independently of XSL.

Standard Details:

XSLT is not intended as a completely general-purpose XML transformation language. Rather it is designed primarily for the kinds of transformations that are needed when XSLT is used as part of XSL.

This specification defines the syntax and semantics of the XSLT language. A transformation in the XSLT language is expressed as a well-formed XML document [XML] conforming to the Namespaces in XML Recommendation [XML Names], which may include both elements that are defined by XSLT and elements that are not defined by XSLT. XSLT-defined elements are distinguished by belonging to a specific XML namespace (see [2.1 XSLT Namespace]), which is referred to in this specification as the XSLT namespace. Thus this specification is a definition of the syntax and semantics of the XSLT namespace. A transformation expressed in XSLT is called a stylesheet. This is because, in the case when XSLT is transforming into the XSL formatting vocabulary, the transformation functions as a stylesheet.

An XSL style sheet is, like with CSS, a file that describes how to display an XML document of a given type. XSL shares the functionality and is compatible with CSS2 (although it uses a different syntax). Styling requires a source XML documents, containing the information that the style sheet will display and the style sheet itself which describes how to display a document of a given type.

A transformation expressed in XSLT describes rules for transforming a source tree into a result tree. The transformation is achieved by associating patterns with templates. A pattern is matched against elements in the source tree. A template is instantiated to create part of the result tree. The result tree is separate from the source tree. The structure of the result tree can be completely different from the structure of the source tree. In constructing the result tree, elements from the source tree can be filtered and reordered, and arbitrary structure can be added.

Resource Locator:

- xSLT

http://www.w3.org/TR/xslt

6.2.4 Data exchange Formats

Data exchange formats provides the communications common denominator between disparate systems.

6.2.4.1 Electronic Data Interchange

Description:

Electronic data interchange is the transmission of data between two entities by electronic means. It is more than mere E-mail; for instance, organizations might replace bills of lading and even cheques with appropriate EDI messages. It exhibits its pre-Internet roots, and the standards tend to focus on ASCII (American Standard Code for Information Interchange)-formatted single messages rather than the whole sequence of conditions and exchanges that make up an inter-organization business process.

Standard Details:

EDI is considered to be a technical representation of a business conversation between two entities, either internal or external. It is considered to describe the rigorously standardized format of electronic documents. The EDI standards were designed to be independent of communication and software technologies. EDI can be transmitted using any methodology agreed to by the sender and recipient. The major standards of EDI are ANSI ASC x12(US), UN/EDIFACT. However in the long run XML/EDI should be considered is to deliver unambiguous and durable business transactions via electronic means.

Resource Locator:

- XML/EDI

  http://www.eccnet.com/xmledi/guidelines-styled.xml ANSI ASC x12

- UN/EDIFACT

  http://www.unece.org/cefact/cf_plenary/plenary98/docs/98cf4.pdf

6.2.4.2Portable Document Format

Description:

A Portable Document Format (pdf) file is a self-contained cross-platform document. Although it contains the complete formatting of the original document, including fonts and images, PDF files are highly compressed, allowing complex information to be downloaded efficiently. It used to access non-editable files. PDF captures all of the elements of a printed document as an electronic image and preserves the exact layout, font attributes, and formatting of the document from the base document. Though this is a proprietary standard as opposed to an open standard, PDF is adopted by many organisation all over the world including eGIF standard because

- PDF is a predominant format for document publishing and extensively used on the Internet.
- It is supported by freely available Acrobat Reader and browser plug-ins.
- Access controls and permissions can be defined in PDF documents, which allow authorised persons to view, edit, or even print documents.
- It is platform independent

Standard Details:

PDF is used for representing two-dimensional documents in a manner independent of the application software, hardware, and operating system. Each PDF file encapsulates a complete description of a fixed-layout 2D document that includes the text, fonts, images, and 2D vector graphics which compose the documents.

Proper subsets of PDF have been, or are being, standardized under ISO for several constituencies:

- PDF/X for the printing and graphic arts as ISO 15930 (working in ISO TC130)
- PDF/A for archiving in corporate/government/library/etc environments as ISO 19005 (work done in ISO TC171)
- PDF/E for exchange of engineering drawings (work done in ISO TC171)
- PDF/UA for universally accessible PDF files

Resource Locator:

- PDF/UA

  http://pdf.editme.com/pdfua

- PDF/E

  http://pdf.editme.com/PDFE

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42274

- PDF/A

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38920

  http://pdf.editme.com/PDFA

- PDF/X

  http://pdf.editme.com/PDFX

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=42876

6.2.4.3Office application document type

Office applications such as Word, Excel and Power point in Nepal's baseline has been predominantly Microsoft office suite of products, this is proprietary and an exemption to the principle of Open standards. The reasons for accepting proprietary standards are:

- It is very predominant in Nepal's baseline
- It is one of the major office applications accepted in few countries eGIF.

Standard Details:

The exchange of word, Excel, and Powerpoint between the users of Microsoft products should use .doc, xls and ppt format. However the following condition should be fulfilled

- Incompatible version should not exists
- Backward compatible should be allowed
- It should supported by open source alternatives.

The MS office 2003 and above is Recommendatory for document exchange between Microsoft office. However In future Open Document Format for Office Applications formats can be considered.

The Open Document Format (ODF) is an open standard based on XML- for office applications to be used for documents containing text, spreadsheets, charts, and graphical elements. OASIS stewards the OpenDocument and provide expertise and resources. The file format makes transformations to other formats simple by leveraging and reusing existing standards wherever possible. It also has the potential to create new types of applications to be developed apart from the traditional office productivity applications.

CSV should also be made *de facto* standard for delimited files for use in interdepartmental information interchange. CSV has wide support from popular and widely used spreadsheet applications such as Microsoft Excel, Lotus 123, and OpenOffice Calc.

Resource Locator:

- MS office Suite

  www.Microsoft.com

- Open format for office application

  http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office

6.2.4.4Tag Image File Format (TIFF)

Description:

TIFF is a file format for storing images, including photographs and line art. The TIFF format is widely supported by image-manipulation applications, by publishing and page layout applications, by scanning, faxing, word processing, optical character recognition and other applications. TIFF is supported by most of the common browsers through freely-available plug-ins and the majority of image processing, graphics design, photo processing and scanner accessory software. Though TIFF has been acquired by Adobe it is not necessary to buy a license from Adobe to implement software reading and writing the TIFF format. The TIFF library LUB TIFF is a free and open source, and is properly supported.

Standard Details:

TIFF is a flexible, adaptable file format for handling images and data within a single file, by including the header tags (size, definition, image-data arrangement, applied image compression) defining the image's geometry. It also can include a vector-based Clipping path (outlines, cropping, image frames). The ability to store image data in a lossless format makes a TIFF file a useful image archive, because, unlike standard JPEG files, a TIFF file using lossless compression (or none) may be edited and re-saved without losing image quality. ISO 12639:1998tandard is Recommendatory for Graphic technology -- Prepress digital data exchange -- Tag image file format for image technology (TIFF/IT) standard.

Resource Locator:

- TIFF

  http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

  http://www.remotesensing.org/libtiff/

  http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=2181

6.2.4.5Graphics Interchange for (GIF)

Description:

The Graphics Interchange Format(sm) defines a protocol intended for the on-line transmission and interchange of raster graphic data in a way that is independent of the hardware used in their creation or display. The format supports up to 8 bits per pixel allowing a single image to reference a palette of up to 256 distinct colors chosen from the 24-bit RGB color space. It also supports animations and allows a separate palette of 256 colors for each frame. The color limitation makes the GIF format unsuitable for reproducing color photographs and other images with continuous color, but it is well-suited for simpler images such as graphics or logos with solid areas of color. GIFs are typically used for sharp-edged line art (such as logos), to store low-color sprite data for games and small animations and low-resolution film.

Standard Details:

GIF files start with a fixed-length header ("GIF87a" or "GIF89a") giving the version, followed by a fixed-length Logical Screen Descriptor giving the size and other characteristics of the canvas. The screen descriptor may also specify the presence and size of a Global Color Table, which follows next if present. However Gif 89a is recommend to be used.

Thereafter, the file is divided into segments, each introduced by a 1-byte sentinel:

- An image (introduced by 0x2C, a comma ',')
- An extension block (introduced by 0x21, an exclamation point '!')
- The trailer (a single byte of value 0x3B, a semi-colon ';'), which should be the last byte of the file.
- An image starts with a fixed-length Image Descriptor, which may specify the presence and size of a Local Color Table (which follows next if present). The image data follow: one byte giving the bit width of the unencoded symbols (which must be at least 2 bits wide, even for bi-color images), followed by a linked list of sub-blocks containing the LZW-encoded data.

Extension blocks (blocks that "extend" the 87a definition via a mechanism already defined in the 87a spec) consist of the sentinel, an additional byte specifying the type of extension, and a linked list of sub-blocks with the extension data. Extension blocks that modify an image (like the Graphic Control Extension that specifies the optional animation delay time and optional transparent background color) must immediately precede the segment with the image they refer to.

The linked lists used by the image data and the extension blocks consist of series of sub-blocks, each sub-block beginning with a byte giving the number of subsequent data bytes in the sub-block (1 to 255), the series terminated by the empty sub-block (a 0 byte).

This structure allows the file to be parsed even if not all parts are understood. A GIF marked 87a may contain extension blocks; the intent is that a decoder can read and display the file without the features covered in extensions it doesn't understand.

Resource Locator:

- GIF89a

  http://www.w3.org/Graphics/GIF/spec-gif89a.txt

6.2.4.6Joint Photographic Experts Group (JPEG)

Description:

JPEG is a commonly used method for compression of photographic images. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality. JPEG typically achieves 10:1 compression with little perceptible loss in image quality.

The JPEG standard specifies the codec, which defines how an image is compressed into a stream of bytes and decompressed back into an image, but not the file format used to contain that stream. The Exif and JFIF standards define the commonly used formats for interchange of JPEG-compressed images.

Standard Details:

JPEG standards are officially called ISO/IEC IS 10918-1 | ITU-T Recommendation T.81, as the document was published by both ISO through its national standards bodies, and CCITT, now it is called ITU-T. IS 10918. It has following parts:

1. ISO/IEC 10918-1:1994 T.81 (09/92) - The basic JPEG standard, which defines many options and alternatives for the coding of still images of photographic quality
2. ISO/IEC 10918-2:1995 T.83 (11/94) - which sets rules and checks for making sure software conforms to Part 1
3. ISO/IEC 10918-3:1997 T.84 (07/96) – which sets up to add a set of extensions to improve the standard, including the SPIFF file format
4. ISO/IEC 10918-4:1999 T.86 (06/98) – which defines methods for registering some of the parameters used to extend JPEG.
5. ISO/IEC CD 10918-5 – Which describes the standardised file format JPEG File Interchange Format (JFIF) as the de-facto file format for images encoded by the JPEG standard.

Resource Locator:

- JPEG

  http://www.jpeg.org/jpeg/index.html

6.2.4.7Rich text Format (RTF)

Description:

The Rich Text Format (RTF) specification provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems. Though it is developed by Microsoft Most word processors are able to read and write.

Standard Details:

RTF embraces the American National Standards Institute (ANSI),PC-8, Macintosh, or IBM PC character set to control the representation and formatting of a document, both on the screen and in print. RTF documents offering cross-platform interoperability.(i.e. documents created under different operating systems, with different software applications can be transferred between those operating systems and applications). RTF 1.9.1 is the latest specification that is Recommendatory to be followed. However there are some limitations that needs to be understood although most word processing software reads RTF format when documents from proprietary formats get converted into RTF some features may be lost

Resource Locator:

- RTF 19.1 specification

  http://www.microsoft.com/downloads/details.aspx?FamilyId=DD422B8D-FF06-4207-B476-6B5396A18A2B&displaylang=en

6.2.4.8 Initial Graphics Exchange Specification (IGES)

Description:

The Initial Graphics Exchange Specification (IGES) defines a neutral data format that allows the digital exchange of information among Computer-aided design (CAD) systems. Using IGES, a CAD user can exchange product data models in the form of circuit diagrams, wireframe, free form surface or solid modeling representations. Applications supported by IGES include traditional engineering drawings, models for analysis, and other manufacturing functions.

The FIPS for IGES shall be used when one or more of the following situations exist:

- The product definition application or program is under constant review, and changes may result frequently.
- It is anticipated that the life of the data files will be longer than the life of the presently utilized CAD/CAM system.
- The application is being designed centrally for a decentralized system that may employ computers of different makes and models and different CAD/CAM devices.
- The product definition application may run on equipment other than that on which it was developed.
- The product definition data is to be used and maintained by other than the original designer.
- The product definition data is or is likely to be used by organizations outside the Federal Government.
- It is desired to have the design understood by multiple people, groups, or organizations.

Standard Details:

The official title of IGES is Digital Representation for Communication of Product Definition Data, first published in January, 1980 by the U.S. National Bureau of Standards as NBSIR 80-1978. Many documents (like early versions of the Defense Standards MIL-PRF-28000[1] and MIL-STD-1840[2]) referred to it as ASME Y14.26M, the designation of the ANSI committee that approved IGES Version 1.0. However we recommend to also consider specification in Federal Information Processing Standards (FIPS PUB 177) issued by the National Institute of Standards and Technology.

Resource Locator:

- FIPS PUB 177

  http://www.itl.nist.gov/fipspubs/fip177-1.htm
- IGES 5.3 (ANSI-1996)

  http://www.uspro.org/documents/IGES5-3_forDownload.pdf

6.2.4.9Moving picture and Experts Group (MPEG) Standard

Description:

Moving Image and Audio/Visual contents are required to define the compressed format and file types for interchange of audio/visual content such as movies. MPEG is the popular and widely accepted family of standard for audio and video compression and transmission. There are several MPEG players available at no cost and conversion is provided by most mainstream packages.

Standard Details:

MPEG is the standard Recommendatory that is defined by ISO Standard 11172. The MPEG standards consist of different Parts. Each part covers a certain aspect of the whole specification. The standards also specify Profiles and Levels. Profiles are intended to define a set of tools that are available, and Levels define the range of appropriate values for the properties associated with them. Some of the approved MPEG standards were revised by later amendments and/or new editions. MPEG has standardised the following compression formats and ancillary standards, however MPEG-1 and MPEG 2 should be considered for adoption in this eGIF and other standards can be considered for adoption at a later stages as well. :

- MPEG-1 Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s - ISO/IEC 11172 1993
- MPEG-2 Generic coding of moving pictures and associated audio information - ISO/IEC 13818 1995
- MPEG-3 abandoned, incorporated into MPEG-2
- MPEG-4 Coding of audio-visual objects - ISO/IEC 14496 1999
- MPEG-7 Multimedia content description interface- ISO/IEC 15938 2002
- MPEG-21 Multimedia framework (MPEG-21) - ISO/IEC 21000 2001
- MPEG-A Multimedia application format (MPEG-A) - ISO/IEC 23000 2007
- MPEG-B MPEG systems technologies - ISO/IEC 23001 2006
- MPEG-C MPEG video technologies - ISO/IEC 23002 2006
- MPEG-D MPEG audio technologies - ISO/IEC 23003 2007
- MPEG-E Multimedia Middleware - ISO/IEC 23004 2007

Resource Locator:

- MPEG Standards

  http://www.chiariglione.org/mpeg/standards.htm

6.2.4.10 Email Document type standards

Description:

Currently in Nepal people uses external free web mails (like Hotmail, Yahoo) more than the official email. There is a lack of awareness and interest due to space constraint and lack of features in the official email suite. In this version of eGIF it has been Recommendatory to move towards an official email suite(client server based). Webmail interfaces allow users to access their mail with any standard web browser, from any computer, rather than relying on an e-mail client.

Standard formats for mailboxes include Maildir and mbox etc. In event of moving towards Email system (client server based) several prominent Email clients use their own proprietary format and require conversion software to transfer e-mail between them. The file type (extensions/format) standards should address the needs for the email system chosen.

Standard Details:

Email transport protocols are required to enable the sending of email messages between servers and from email clients to mail servers. These protocols are also required to enable the exchange of messages in languages with different character sets as well as emails with attachments. Recommended standards / specifications:· SMTP / MIME – Simple Mail Transport Protocol / Multipurpose Internet Mail Extensions. Simple Mail Transport Protocol (SMTP) is the protocol used to deliver or relay e-mail messages. Multipurpose Internet Mail Extensions (MIME) is a specification for enhancing the capabilities of standard Internet electronic mail. It offers a simple standardized way to represent and encode a wide variety of media types for transmission via Internet mail.

Resource Locator:

- SMTP Standards

  http://datatracker.ietf.org/doc/rfc5335/

  http://datatracker.ietf.org/doc/rfc5336/

- MIME Standards

  http://datatracker.ietf.org/doc/rfc2045/

  http://datatracker.ietf.org/doc/rfc2046/

  http://datatracker.ietf.org/doc/rfc2047/

  http://datatracker.ietf.org/doc/rfc2048/

  http://datatracker.ietf.org/doc/rfc2049/

6.2.4.11 Computer Graphics Metafile (CGM) and WebCGM

Description:

Computer Graphics Metafile (CGM) is a open standard file format for 2D vector graphics, raster graphics, and text. . CGM provides a platform independent means of graphics data interchange for computer representation of 2D graphical. The metafile contains the information that describes or specifies another file. The CGM format has numerous elements to provide functions and to represent entities, so that a wide range of graphical information and geometric primitives can be accommodated. CGM contains the instructions and data for reconstructing graphical components to render an image using an object-oriented approach.

WebCGM is a profile of CGM, which adds Web linking and is optimized for Web applications in technical illustration, electronic documentation, geophysical data visualization, and similar fields. First published (1.0) in 1999 and followed by a second (errata) release in 2001, WebCGM unifies potentially diverse approaches to CGM utilization in Web document applications. It therefore represents a significant interoperability agreement amongst major users and implementers of the ISO CGM standard.

Standard Details:

The CGM standard is defined by ISO/IEC 8632 however we recommend WebCGM2.0 standards are detailed by W3C.

Resource Locator:

- WebCGM 2.0

  http://www.w3.org/TR/2007/REC-webcgm20-20070130/

6.2.4.12 Hyper Text Markup Language (HTML, HTM)

Description:

HTM is the format of storage for all HTML files which is the dominant markup language for web pages. Formatting of hypertext documents for presentation on browsers via a range of delivery channels including Internet and Intranet should be HTML 4.0 and above. HTML is a simple markup language used to create hypertext documents that are platform independent. The markup conveys to the Web browser the way to display a Web page's words and images for the user. HTML markup can represent hypertext news, mail, and documentation, and hypermedia, menus of options, database query results and hypertext views of existing bodies of information.

Standard Details:

HTML4.0 and above should be adopted, HTML 4 supports more multimedia options, scripting languages, style sheets, better printing facilities, and documents that are more accessible to users with disabilities in \addition to the previous versions of HTML such as 3.2 etc. Detailed specification is given by w3c in the following URL. One important aspect to be considered while adopting these standards is to ensure that the government web content is tested for the compatibility of their content with different combinations of widely used browser configurations and widely used operating system configurations and seek with appropriate vendor the relevant documentation/ information on restrictions and deviations from the specifications. It is also good to state in the web page how the content can best be viewed. XHTML is a separate language that began as a reformulation of HTML 4.01 using XML 1.0. This can be considered in the future versions.

Resource Locator:

- HTML4.01

  http://www.w3.org/TR/html4/

6.2.4.13 Audio formats Standards (MP3/MP4)

Description:

MP3 is an audio-specific format that was designed by the Moving Picture Experts Group as part of its MPEG-1 standard. It is a patented digital audio encoding format using a form of lossy data compression. It is a common audio format for consumer audio storage, as well as a de facto standard of digital audio compression for the transfer and playback of music on digital audio players.

MP4 file format, , is a multimedia container format standard specified as a part of MPEG-4. It is most commonly used to store digital video and digital audio streams, especially those defined by MPEG, but can also be used to store other data such as subtitles and still images.

Standard Details:

ISO/IEC 11172-3, ISO/IEC 13818-3 is the standard for MP3. ISO/IEC 14496-14:2003 is the standard for Mp4. the details of the specification/standard are provide in the resource locator.

Resource Locator:

- ISO/IEC 13818-3

  http://www.pdf-search-engine.com/iso/iec-11172-3-pdf.html

- ISO/IEC 14496-14:2003

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=38538

6.2.5 Ontology-based information exchange

Ontology is a "formal, explicit specification of a shared conceptualisation". An ontology provides a shared vocabulary, which can be used to model a domain — that is, the type of objects and/or concepts that exist, and their properties and relations

6.2.5.1 Web Ontology Language (OWL)

Description:

The Web Ontology Language (OWL) is a knowledge representation languages for authoring ontologies. The languages are characterised by formal semantics and RDF/XML-based serializations for the Semantic Web. OWL is endorsed by the World Wide Web Consortium and has attracted academic, medical and commercial interest.

Standard Details:

The Web Ontology Language being designed by the W3C Web Ontology Working Group, contains a high-level abstract syntax for both OWL DL and OWL Lite, sublanguages of OWL. A model-theoretic semantics is given to provide a formal meaning for OWL ontologies written in this abstract syntax. A model-theoretic semantics in the form of an extension to the RDF semantics is also given to provide a formal meaning for OWL ontologies as RDF graphs (OWL Full). A mapping from the abstract syntax to RDF graphs is given and the two model theories are shown to have the same consequences on OWL ontologies that can be written in the abstract syntax.The details can be found in the resource locator.

Resource Locator:

- OWL

  http://www.w3.org/TR/owl-semantics/

  http://www.w3.org/TR/owl2-overview/

6.2.6 *Data modelling language*

Data modeling is the analysis of data objects that are used in a business or other context and the identification of the relationships among these data objects. Data modeling is a first step in doing object-oriented programming. As a result of data modeling, you can then define the classes that provide the templates for program objects.

6.2.6.1 Unified Modeling Language (UML)

Description:

UML is a visual language for specifying, constructing, and documenting the artifacts of systems. You can use UML with all processes, throughout the development lifecycle, and across different implementation technologies

Standard Details:

UML was approved by the OMG™ as a standard in 1997. Over the past few years there have been minor modifications made to the language. UML 2 is the first major revision to the language

Resource Locator:

- UML

  http://www.omg.org/technology/documents/formal/uml.htm

6.2.7 Data integration meta language

The meta-language standard provides an easy and available way to identify and share data. XML, as defined by W3C being lightweight, easy, and increasingly available is considered to be the data integration meta-language.

6.2.7.1 XML-Signature Syntax and Processing

Description:

XML Signature is a W3C recommendation that defines XML syntax for digital signatures. Functionally, it has much in common with PKCS#7 but is more extensible and geared towards signing XML documents. It is used by various Web technologies such as SOAP, SAML, and others.

Standard Details:

W3C provided the standard for this which can be found in the resource locator

Resource Locator:

- XMLSig

  http://www.w3.org/TR/xmldsig-core/

6.2.7.2 XML-DSS

Description:

This defines the XML syntax and semantics for the Digital Signature Service core protocols, and for some associated core elements. The core protocols support the server-based creation and verification of different types of signatures and timestamps. The core elements include an XML timestamp format, and an XML signature property to contain a representation of a client's identity

Standard Details:

The standard for this has been provided by OASIS Digital Signature Service Technical Committee, Details of which can be found in the resource locator.

Resource Locator:

- XML-DSS

  http://docs.oasis-open.org/dss/cd/oasis-dss-1%5B1%5D.0-core-spec-cd.pdf

6.2.7.3 XML encryption

Description:

XML Encryption is process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption element which contains or references the cipher data.

Standard Details:

Standard for XML Encryption has been laid down by W3C details of which can be found in the resource locator

Resource Locator:

- XML-Encryption

  http://www.w3.org/TR/xmlenc-core/

6.2.7.4XML signature and encryption

Description:

This describes the XML Signature "decryption transform" that enables XML Signature applications to distinguish between those XML Encryption structures that were encrypted before signing (and must not be decrypted) and those that were encrypted after signing (and must be decrypted) for the signature to validate.

Standard Details:

The standard has been provided by W3C and details can be found in the resource locator

Resource Locator:

- XML-Encryption

  http://www.w3.org/TR/xmlenc-decrypt

6.2.7.5XML key management where a PKI environment is used

Description:

This specifies protocols for distributing and registering public keys, suitable for use in conjunction with the W3C Recommendations for XML Signature [XML-SIG] and XML Encryption [XML-Enc]. The XML Key Management Specification (XKMS) comprises two parts — the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS)

Standard Details:

The standard has been provided by W3C and details can be found in the resource locator

Resource Locator:

- XML-Key Management Specification(XKMS)

http://www.w3.org/TR/xkms2/

6.2.7.6XML security assertion mark-up

Description:

This is an XML-based framework for communicating user authentication, entitlement, and attribute information. This allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.

Standard Details:

The standard has been provided by OASIS and details can be found in the resource locator

Resource Locator:

- Security Assertion Markup Language(SAML)

  http://www.oasis-open.org/committees/security/index.shtml

6.2.7.7 XML access control

Description:

This is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. In encoded data exchange, this is a simple, flexible way to express and enforce access control policies in a variety of environments, using a single language

Standard Details:

The standard has been provided by OASIS and details can be found in the resource locator

Resource Locator:

- eXtensible Access Control Markup Language(XACML)

  http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

6.2.8 Minimum interoperable character set

Standard on Minimum Interoperable Character Set is required to define the minimum character sets to be used for the content to be interchanged in between related parties, e.g. agencies and departments as well as third parties such as suppliers.

Description:

ISO/IEC 10646-1 defines a multi-octet character set called the Universal Character Set (UCS) which encompasses most of the world’s writing systems. Multi-octet characters, however, are not compatible with many current applications and protocols, and this has led to the development of a few so-called UCS transformation formats (UTF), each with different characteristics. UTF-8 has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values.

Standard Details:

UTF-8 is a proposed IETF standard defined in RFC 2279 “UTF-8, a transformation format of ISO 10646”.

Resource Locator:

- UTF-8

  http://datatracker.ietf.org/doc/rfc3629/

6.2.9 Digitization

Digitisation, also known as imaging or scanning, is the means of converting hard-copy, or non-digital,records into digital format. It may also involve taking digital photographs of the source records. Once converted to digital objects, they may be captured as a static picture (raster image) represented by pixels,processed by optical character recognition, technology which converts the pixels into digital representations which are searchable, editable and manipulable; or captured into both formats.

Description:

A large volume of technical standards associated with digitisation are available. Such standards include recommendations on

- File formats;
- Resolution;
- Colour resolution or bit depth;
- Compression;
- Colour Management.

These standards are rapidly evolving, especially in the area of technical capacity of equipment to accommodate such standards. The primary consideration in adopting technical specifications is to ensure the legibility of the digitised image. The following basic criteria should be adhered to when selecting technical standards:

- The highest technical specifications that can be realistically supported SHOULD be incorporated into the digitisation process
- Format should be open source (that is,non-proprietary), have published technical specifications available in the public domain, or be widely deployed within the relevant sector
- Format should not contain embedded objects, or link out to external objects beyond the specific version of the format
- Format should be supported by many software applications and operating systems
- Format should be able to be read by utilising a readily available viewing plug-in if the specific production software is not available to all users, Adequate technical support should exist to enable ongoing maintenance and assurance of migration capability when necessary

Standard Details:

Table 6-11: Digitization standard

Document Type	Resolution	Bit Depth	File Format	Compression
Text only, black and white	Minimum 300ppi	1 bit (bi-tonal)	TIFF PDF/A containing TIFF or JPEG 2000	Lossless compression
Documents with watermarks, grey shading,grey graphics	Minimum 600 ppi	8 bit greyscale	TIFF JPEG 2000 PDF/A containing TIFF or JPEG 2000	Lossless compression

Document Type	Resolution	Bit Depth	File Format	Compression
Documents with discrete colour used in text or diagrams	Minimum 600 ppi	Minimum: 8 bit colour	TIFF JPEG 2000 PDF/A containing TIFF or JPEG 2000	Lossless compression
Black and white photographs	Sufficient to provide > 3000 pixels across long dimensions	8 bit greyscale	TIFF JPEG 2000 PDF/A containing TIFF or JPEG 2000	Lossless compression
Colour photographs	Sufficient to provide > 3000 pixels across long dimensions	24 bit colour	TIFF JPEG 2000 PDF/A containing TIFF or JPEG 2000	Lossless compression
Black and white negatives	Sufficient to provide > 3000 pixels across long dimensions	8 bit greyscale or 24 bit colour	TIFF JPEG 2000 PDF/A containingTIFF or JPEG 2000	Lossless compression
Colour negatives and transparencies	Sufficient to provide > 3000 pixels across long dimensions	24 bit colour	TIFF JPEG 2000 PDF/A containing TIFF or JPEG 2000	Lossless compression
Microforms	When scanning microforms, the approach should be to emulate the methods detailed above consistent with the source document on the (typically greyscale) microform – that is, to produce a minimum resolution of 600 ppi (in relation to the original document). However, this may vary for textual records to focus more on creating digital images with reasonable or good legibility. JPEG 2000 and PDF/A are recommended formats.			

Table 6-12: Digitization Areas and Issues

Area	Issues
File formats	Categories of file formats are: **Raster**: also known as bit-mapped formats, where images take the form of a grid or matrix with each picture element (pixel) having a unique location and independent colour value. Examples are TIFF, JPG/JPEG, GIF, PNG; **Vector**: also known as object oriented, based on a set of mathematical instructions typically used by drawing programs to construct an image – not of relevance to digitisation which will use raster formats **Encoding**: or metafiles which may contain either vector or raster images. Such formats enable the contents to be consistently displayed and used across different computer programs and operating systems. Typically, they support internal metadata, support multi-page images and enable security management. Examples include Adobe PDF and TIFF.

Area	Issues
Resolution	A measure of the ability to capture detail in the original work, often quantified in pixels per inch (ppi). The optimum resolution depends on the nature of the documents being scanned. Photographs, for example, require much greater resolution than text-based documents. **ppi**: (pixels per inch) is a measurement of resolution for computer display. **dpi**: (dots per inch) is often used interchangeably with ppi, but actually refers specifically to measurement of the resolution for computer printers.
Color resolution or bit depth	A measure of the number of colors (or degree of brightness, in grey scale images) available to represent the colors (or shades of grey) in the original document. For example: 1 Bit, Black and White or line art: only black and white pixels; Greyscale: black and white in addition to a range of intermediate greys, requiring 8 bits to describe each pixel; 8 Bit Color: uses a palette of 256 colors; 24 Bit Color: a resolution that enables storage of 8 bits of information describing the red, green and blue components of every pixel, thus enabling a much greater palette of colors; and 36-48 Bit RBG Color: uses an extended color space, creating a much larger file, and requiring storage in formats that explicitly support this color depth (TIFF or PNG).
Compression	Algorithms designed to reduce the size of the image for storage or transmission. Multiple options exist but decisions should be made on the characteristics of the document to be imaged. The two major categories of compression are: **Lossy**: where information is removed from the stored information during the compression process; and **Lossless**: where no information is irretrievably lost and where the decompressed object will always appear exactly the same as the original. Examples include LZW or ZIP lossless compression with TIFF files. Newer forms of compression emerging are fractals and wavelets.
Color management	Means of attempting to ensure that the image looks the same across a range of different output devices. Monitors and printers typically use different color spectrum. The standard for color representation is the ICC color management system, which uses a standardized and known 'color space' based on the human eye and then compares all devices to the known standard.

6.2.10 Data Definition for Smart Cards

Description:

For smart card application there are data definition standards predominantly defined by ISO that are usually complied, though there is no universal standards these standards are followed by many countries.

Standard Details

ISO/IEC 7816-6:2004

This standard specifies the Data Elements (DEs) used for inter-industry interchange based on integrated circuit cards (ICCs) both with contacts and without contacts. It gives the identifier, name, description, format, coding and layout of each DE and defines the means of retrieval of DEs from the card.

ISO/IEC 7812-1:2006

This standard specifies a numbering system for the identification of issuers of cards that require an issuer identification number to operate in international, inter-industry and/or intra-industry interchange.

Resource Locator:

- ISO/IEC 7816-6:2004

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=38780

- ISO/IEC 7812-1 :2006

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=31443

6.3 Security

Security covers components and technical specifications needed to enable the secure exchange of information as well as the secure access to public sector information and services.

Table 6-13: Security

Security		
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Security Technical Standards Details**
Access management		
• The system should support operating systems, application servers, database management systems, identity management and directory services. standards • The system should have APIs for identification and authentication • The access management should encrypt user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one-way hash format.	Mandatory	4.3.1 Access Management
Anti Spam		
• Anti-spam product should be compatible with standards adopted for operating systems and electronic mail systems.	Mandatory	4.3.2 Anti- Spam
Anti Virus/Anti Spyware		
• They should be able to provide protection against various kinds of attacks from virus, worms, Trojan horse etc. • Anti-virus and anti-spyware products should be compatible with the standards adopted for operating systems.	Mandatory	4.3.3 Anti-Virus/Anti- Spyware
Desktop Firewall		
• Technologies must support standards approved in various categories such as operating systems and network protocols.	Mandatory	4.3.4 Desktop Firewall
Digital Signature		
• Secure Hash Algorithm should be used as a standard for digital signature. • Provides authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality.	Mandatory	4.3.5 Digital Signature
Email Security		
• S/MIMEv3 should be the standard used for a secure mail to transport for a source to a destination.	Mandatory	4.3.6 Email Security
Encryption Algorithm		
• Triple DES and DES standards should be used for encryption algorithm.	Recommendatory	4.3.7 Encryption Algorithm
Enterprise Firewall		
• The firewall should support various layers of	Mandatory	4.3.8 Enterprise Firewall

Security		
TCP/IP protocol stack. • The firewall should support approved standards of operating systems, network protocols, data transport, electronic mail systems and application technologies.		
SwIPe		
• SwIPe should be the standard used for IP security at the network layer for confidentiality, integrity and authentication of network traffic.	Mandatory	4.3.9 SwIPe
Cryptographic algorithm		
• MD5 algorithm should be used for cryptographic hash function.	Mandatory	4.3.10 MD5
User Level Security		
• AAA and TACACS should be the standards used for user level security.	Mandatory	4.3.11 User Level Security 4.3.11.1 AAA 4.3.11.2 TACACS
Identity , Authentication , authorization and privacy		
• Security Assertions Markup Language (SAML1.1) should be the framework for exchange of authentication and authorization information • X.509 should be the standard for identity certificates. • Platform for Privacy Preferences Project (P3Pv1.0) should the standards adopted for enabling web sites to express privacy practices in a standardized form that can be automatically retrieved and interpreted by user agents, such as browsers.	Mandatory	4.3.12 Identity, Authentication , Authorization and Privacy
Identity management		
• Identity Management should enable encryption of user-ids and passwords during transmission. In addition, passwords should be stored in an encrypted or one-way hash format. • It should have APIs for identification and authentication. Technologies should be vendor neutral and support operating systems, database management systems, application servers, access managers and directory services.	Mandatory	4.3.13 Identity Management
Intrusion detection and prevention		
• Technologies must support approved standards in various categories such as operating systems, and firewalls	Mandatory	4.3.14 Intrusion Detection and Prevention
IP Encapsulation security		
• ESP should be used for communicating secure data transmission, confidentiality, data origin authentication, connectionless integrity, an anti-replay, and traffic flow confidentiality	Mandatory	4.3.15 IP Encapsulation Security

Security		
IP security		
• The standard for securing internet protocol communications by authentication or encrypting should be IPSec.	Mandatory	4.3.16 IP Security
Layer 2 Security		
• L2TP should be used to support a secure communication in VPN on data link layer.	Mandatory	4.3.17 Layer 2 Security
Proxy server		
• Evaluates the request according to its filtering rules. • Proxy servers should be compatible with LDAPv3 and should be able to integrate with adopted standards for directory services	Mandatory	4.3.18 Proxy Server
Public key infrastructure		
• PKI should be used for communicating confidential information in banking sectors and other ministries.	Mandatory	4.3.19 Public Key Infrastructure
Remote Security		
• SSH should be used for secure remote login when accessing data from GIDC or other ministries/agencies .	Mandatory	4.3.20 Remote Security
Secure transport		
• TLS/SSL should be the standards used for a secure transport of data from a source to a destination.	Mandatory	4.3.21 Secure Transport 4.3.21.1 Secure Socket Layer 4.3.21.2 Transport Security
VPN		
• The VPN must use vendor neutral, standards-based, APIs for identification and authentication • The VPN should allow encrypting user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one-way hash format • The technology should be compatible with adopted standards for PKI, proxy servers, firewalls and operating systems.	Mandatory	4.3.22 Virtual Private Network
XML security standards		
• XML-DSIG should be used for representing and verifying web signatures. • WS – Security should be the standards for security of messages transmitted between web services components. • WS- I Basic Security Profile Version 1.0 can be used for Web Services-Interoperability	Mandatory	4.3.23 XML Security Standards
Physical Security		
• It includes different kinds of methods and equipments for securing an environment such as:	Mandatory	4.3.24 Physical Security 4.3.24.1 IP Base Surveilance

Security		
- IP-based surveillance cameras, access control (card or biometric) devices.		Cameras 4.3.24.2 Encoding Server 4.3.24.3 Media Server 4.3.24.4 CODEC 4.3.24.5 Display Screen
Security of Smart card		
• ISO/IEC 7816-8: 2004 Identification cards – Integrated circuit cards Security inter industry commands • ISO/IEC 7816-9: 2004 Identification cards – Integrated circuit cards Commands for card management • ISO/IEC 7816-11: 2004 Identification cards – Integrated circuit(s) cards Personal verification through biometric methods and Integrated circuit cards • ISO/IEC 7816-15: 2004 Identification cards – Integrated circuit cards Cryptographic information application • ISO/IEC 7816-15: 2004/Cor 1: 2004 PIN for POS • ISO 9564-1: 2002 Banking -- Personal Identification Number (PIN) management and securityBasic principles and requirements for online PIN handling in ATM and POS systems • ISO 9564-2: Banking -- Personal Identification Number management and security Approved algorithm(s) for PIN encipherment • ISO 9564-3: 2003 Banking -- Personal Identification Number management and security Requirements for offline PIN handling in ATM and POS systems • ISO 9564-4: 2004 Banking -- Personal Identification Number management and security Guidance for PIN handling in open networks		4.3.25 Security of Smart Card

6.3.1 Access Management

Description:

Access management is a concept that information from businesses needs to be protected from unauthorized disclosure. To protect information, companies define policies that govern who can access specific classes of business and/or personal information. Its goal is to allow sensitive information to be removed from the process without loss of access control. One of the problems could be that the access policy used by software guards is often coded directly into the business application. When access policy or audit requirements change, application software must be modified, tested and redeployed. Additionally, when access policy needs to be examined or applications audited for conformance a code review is required.

Standard Details:

Access Management solutions provide an alternative to the costly embedding of access policy. They allow application software guards to leverage services that enable access policy to be modified, tested and deployed dynamically without application code changes. This enables your developers to concentrate on providing business software. Access management solutions efficiently enable high performance access controls in distributed environments while allowing centralized management of access policy. An Access Management solution includes programming interfaces (APIs), policy management tools and auditing capabilities.

Resource Locator:

- Access management

  http://www.2ab.com/pdf/AccessManagement.pdf

6.3.2 Anti-Spam

Description:

Anti-spam is a software, hardware or process that is used to combat the proliferation of spam or to keep spam from entering a system.

Anti-spam techniques can be broken into four broad categories: those that require actions by individuals, those that can be automated by e-mail administrators, those that can be automated by e-mail senders and those employed by researchers and law enforcement officials.

The two key features of a spam are unsolicited or bulk and contents of mail might not determine this as a spam.

Standard Details:

Balancing false negatives (e.g.: missed spams) vs false positives (e.g.: rejecting good e-mail) is critical for a successful anti-spam system. Most techniques have both kinds of errors, to varying degrees. Anti-spam systems may use techniques that have a high false negative rate (miss a lot of spam), in order to reduce the number of false positives (rejecting good e-mail).

The popular method to detect a spam is based on the content of the e-mail i.e. either by detecting keywords or by statistical means. Such methods can be very accurate when they are correctly tuned to the types of legitimate email that an individual gets, but they can also make mistakes such as detecting keywords which are part of another word such as “cialis” in “specialist”.

6.3.3 Anti-Virus/Anti spyware

Description:

It is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

Spyware is a type of malware that is installed on computers and collects information about users without their knowledge. The presence of spyware is typically hidden from the user. Typically, spyware is secretly installed on the user's personal computer. Unlike viruses and worms, spyware does not usually self-replicate. Like many recent viruses, however, spyware—by design—exploits infected computers for commercial gain.

Antispyware helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software. To keep up with the latest forms of spyware, you must keep your antispyware updated.

Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you try to uninstall this software like any other program, you might find that the program reappears as soon as you restart your computer.

Standard Details:

There are several methods which antivirus software can use to identify malware.

Signature based detection is the most common method. To identify viruses and other malware, antivirus software compares the contents of a file to a dictionary of virus signatures. Because viruses can embed themselves in existing files, the entire file is searched, not just as a whole, but also in pieces.

Heuristic-based detection, like malicious activity detection, can be used to identify unknown viruses.

File emulation is another heuristic approach. File emulation involves executing a program in a virtual environment and logging what actions the program performs. Depending on the actions logged, the antivirus software can determine if the program is malicious or not and then carry out the appropriate disinfection actions.

Resource Locater:

- Antivirus Software

  http://en.wikipedia.org/wiki/Antivirus_software

6.3.4 Desktop Firewall

Description:

A firewall is a part of a computer system or network that is designed to block unauthorized access. A desktop firewall is part of a computer system which is used by end users on their personal computers. It is different from a conventional firewall in terms of scale as it only protects the computer it is installed on.

Standard Details:

This RFC specifies an Internet Best Current Practices for the Internet Community. This document has been written for the large number of firewalls in the Internet that inappropriately reset a TCP *connection* upon receiving certain packets. Hence, firewalls (hardware/software) have to be used for the assurance of a network's security.

Resource Locator:

- Firewall (RFC-3360)

  http://rfc-editor.org/rfc/rfc3360.txt

6.3.5 Digital Signature

Description:

A digital signature is a scheme for demonstrating the authenticity of a digital message or document. It gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. They are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.

Standard Details:

Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.

Digital Signatures are used for Authentication and Integrity. Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. Even though encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature will invalidate the signature.

The Secure Hash Algorithm (SHA for use with the Digital Signature Standard (DSS) is specified within the Secure Hash Standard (SHS) SHA is a cryptographic message digest algorithm similar to the MD4 family of hash functions The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash.

Resource Locator:

- RFC 4359 (SHA)

  http://www.rfc-editor.org/rfc/rfc4359.txt

  http://www.w3.org/PICS/DSig/SHA1_1_0.html

6.3.6 E-mail Security (S/MIME)

Description:

S/MIME provides a consistent way to send and receive data. Encryption provides data confidentiality. Compression can be used to reduce data size.

Standard Details:

S/MIME has been proposed by RSA as a standard to the Internet Engineering Task Force (IETF). PGP/MIME is an alternative to S/MIME. S/MIME was developed by RSA Data Security to thwart forgery and interception of electronic messages. S/MIME was created on the existing MIME protocol standard and it can be integrated easily into the existing email and messaging products. Another reason for the S/MIME protocol's wide acceptance is that S/MIME allows a Windows user to send a digitally signed and secure email with the Outlook email client to a Unix OS user, who can receive the email using the Netscape email client. The users do not have to install any additional program or software to utilize this facility.

Resource Locator:

- S/MIME (RFC 3851)

  http://rfc-editor.org/rfc/rfc3851.txt

6.3.7 Encryption Algorithm

Description:

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers.

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message. DES and 3DES are the standards used for encryption algorithm.

Standard Details:

DES is an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such. DES itself can be adapted and reused in a more secure scheme

3DES is a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key). It provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.

Resource Locator:

- DES RFC 4772

  http://www.rfc-editor.org/rfc/rfc4772.txt

  http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

- 3DES

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37972

6.3.8 Enterprise Firewall

Description:

Enterprise Firewall is a hardware/Software Firewall that protects assets and business transactions by ensuring fast, secure connections with the Internet and networks. It enables fast, controlled connectivity, providing strong protection against unwanted intrusion without slowing the flow of approved traffic.

Standard Details:

This RFC specifies an Internet Best Current Practices for the Internet Community. This document has been written for the large number of firewalls in the Internet that inappropriately reset a TCP connection upon receiving certain packets. Hence, firewalls (hardware/software) have to be used for the assurance of a network's security.

Resource Locator:

- Firewall (RFC-3360)

  http://rfc-editor.org/rfc/rfc3360.txt

6.3.9 Internet Protocol (IP) security network protocol – swIPe

Description:

swIPe is an Internet Protocol (IP) security network protocol that operates at the network layer of the OSI model. swIPe provides confidentiality, integrity, and authentication of network traffic, and can be used to provide both end-to-end and intermediate-hop security. It is concerned only with security mechanisms. It works by augmenting each packet with a cryptographically-strong authenticator and/or encrypting the data to be sent. swIPe works by encapsulating each IP datagram to be secured inside a swIPe packet.

Standard Details:

This document describes swIPe, a network-layer security protocol for the IP protocol suite. swIPe provides confidentiality, integrity, and authentication of network traffic, and can be used to provide both end-to-end and intermediate-hop security. swIPe is concerned only with security mechanisms; policy and key management are handled outside the protocol.

Resource Locator:

- SwIPe

  http://www.crypto.com/papers/swipe.id.txt

6.3.10 MD5

Description:

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. It has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

Standard Details:

MD5 is one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1994). When analytic work indicated that MD5's predecessor MD4 was likely to be insecure, MD5 was designed in 1991 to be a secure replacement. (Weaknesses were indeed later found in MD4 by Hans Dobbertin.)In 1993, Den Boer and Bosselaers gave an early, although limited, result of finding a "pseudo-collision" of the MD5 compression function; that is, two different initialization vectors which produce an identical digest.

Resource Locator:

- MD5 (RFC 1321)

  http://www.rfc-editor.org/rfc/rfc1321.txt

6.3.11 User Level Security

6.3.11.1 AAA

Description:

AAA is a Standard used for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. It is important for effective network management and security.

Standard Details:

RFC 4962 provides guidance to designers of Authentication, Authorization, and Accounting (AAA) key management protocols. It is useful to designers of systems and solutions that include AAA key management protocols. The guidelines in this document apply to documents requesting publication as IETF RFCs. these guidelines will also be useful to other organizations that specify AAA key management.

Resource Locator:

- AAA (RFC 4962)

  http://rfc-editor.org/rfc/rfc4962.txt

6.3.11.2 TACACS

Description:

TACACS is an authentication Protocol that provides remote access authentication and related services such as event logging. User Passwords are administered in a central database rather than individual routers, providing an easy scalable network security solution.

Standard Details:

It is a client/server protocol where a client (Network Access Servers) sends an authentication /authorization request, which is responded by the server (authentication server). The protocol is based on the UDP transport protocol. It was developed and described in the RFC 1492 by July 1993.

Resource Locator:

- TACACS (RFC 1492)

  http://rfc-editor.org/rfc/rfc1492.txt

6.3.12Identity Authentication, Authorization and privacy

Description:

Security Assertion Markup Language, X.509 and P3Pv1.0 are the standards that address identity, authentication, authorization and privacy. SAML defines XML based exchange mechanism and data structures for authentication and authorization information. X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and Privilege Management Infrastructure (PMI). The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices and to automate decision-making based on these practices when appropriate. The P3P1.0 specification defines the syntax and semantics of P3P privacy policies, and the mechanisms for associating policies with Web resources.

Standard Details:

SAML has become the definitive standard underlying many web Single Sign-On solutions in the enterprise identity management problem space. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. SAML is built upon a number of existing standards such as Extensible Markup Language (XML), XML Schema, XML Signature, XML Encryption, Hypertext Transfer Protocol (HTTP) and SOAP.

X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. X.509 certificates based on SHA-1 had been deemed to be secure up until very recent times

The structure of an X.509 v3 digital certificate is as follows:

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (Optional)
  - Subject Unique Identifier (Optional)
  - Extensions (Optional)
    - ...
- Certificate Signature Algorithm
- Certificate Signature

P3P version 1.0 is a protocol designed to inform Web users of the data-collection practices of Web sites. It provides a way for a Web site to encode its data-collection and data-use practices in a machine-readable XML format known as a *P3P policy*. The P3P specification defines:

- A standard schema for data a Web site may wish to collect, known as the "P3P base data schema"
- A standard set of uses, recipients, data categories, and other privacy disclosures
- An XML format for expressing a privacy policy
- A means of associating privacy policies with Web pages or sites, and cookies
- A mechanism for transporting P3P policies over HTTP

The goal of P3P version 1.0 is twofold. First, it allows Web sites to present their data-collection practices in a standardized, machine-readable, easy-to-locate manner. Second, it enables Web users to understand what data will be collected by sites they visit, how that data will be used, and what data/uses they may "opt-out" of or "opt-in" to.

Resource Locator:

- P3P v1.0

  http://www.w3.org/TR/P3P/
- SAML

  http://saml.xml.org/saml-specifications#samlv11
- X.509

  RFC 4158

  http://rfc-editor.org/rfc/rfc4158.txt

  RFC5280

  http://rfc-editor.org/rfc/rfc5280.txt

6.3.13 Identity Management

Identity management (IDM) covers issues such as how users are given an identity, the protection of that identity and the technologies supporting that protection such as network protocols, digital certificates, passwords and so on.

Identity management is multidisciplinary and covers many dimensions such as:

Technical. With identity management systems (identification, implementation, administration and termination of identities with access to information systems, buildings and data within an organization).

- Legal. Such as legislation for data protection.
- Police. For instance for dealing with identity theft.
- Social and humanity. Dealing with issues such as privacy.
- Security. With elements such as access control.
- Organizations.

Standard Details:

- It provides significantly greater opportunities to online businesses beyond the process of authenticating and granting access to authorized users via cards, tokens and web access control systems. It provides the focus to deal with system-wide data quality and integrity issues often encountered by fragmented databases and workflow processes.
- IdM embraces what the user actually gets in terms of products and services and how and when they acquire them. Therefore, applies to the products and services of an organization. It is also applicable to means by which these products and services are provisioned and assigned to users.
- It can deliver single-customer views that include the presence and location of the customer, single products and services as well as single IT infrastructure and network views to the respective parties.

Resource Locator:

- Identity Management

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51625

6.3.14Intrusion detection system/ Intrusion Prevention System (IDS/IPS)

Description:

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems (DDOS) mainly through a network, such as the Internet. In a passive system, the intrusion detection system (IDS) sensor detects a potential security breach, logs the information and signals an alert on the console and or owner. In a reactive system, also known as an intrusion prevention system (IPS), the IPS responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious.

Standard Details:

A preliminary concept of IDS began with James P. Anderson and reviews of audit trails. Fred Cohen noted in 1984 (see Intrusion Detection) that it is impossible to detect an intrusion in every case and that the resources needed to detect intrusions grows with the amount of usage. Dorothy E. Denning, assisted by Peter Neuman, published a model of IDS in 1986 that formed the basis for many systems today.

Resource Locator:

- IDS/IPS

  http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1517609

6.3.15IP Encapsulation Security

Description:

The Encapsulating Security Payload (ESP) is designed to provide a mix of security services in IPv4 and IPv6. It is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay, and traffic flow confidentiality.

Standard Details:

This RFC describes an updated version of the Encapsulating Security Payload (ESP) protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. This document obsoletes RFC 2406 (November 1998).

Resource Locator:

- ESP (RFC 4303)

  http://rfc-editor.org/rfc/rfc4303.txt

6.3.16IP SEC

Description:

Internet Protocol Security (IP-sec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

Standard Details:

This RFC Specifies the basis for "Security Architecture for IP", which is designed to provide security services for traffic at the IP layer. It describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the requirements for systems that implement IPsec, the fundamental elements of such systems, and how the elements fit together and fit into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment.

Resource Locator:

- IP SEC (RFC 4301)

  http://rfc-editor.org/rfc/rfc4301.txt

6.3.17Layer 2 Security (L2TP)

Description:

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Standard Details:

Published in 1999 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for PPP: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3, was published as proposed standard RFC 3931 in 2005. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (e.g., Frame Relay, Ethernet, ATM, etc).

Resource Locator:

- L2TP (RFC 3931)

  http://www.rfc-editor.org/rfc/rfc3931.txt

6.3.18Proxy Server

Description:

Proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server for services such as a file, connection, web page, or other resource, available from a different server. It then evaluates the request according to its filtering rules. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

Standard Details:

A proxy server has many potential purposes, such as:

- Keeping machines behind it anonymous (mainly for security).
- Speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
- Apply access policy to network services or content, e.g. to block undesired sites.
- Log / audit usage, i.e. to provide company employee Internet usage reporting.
- Bypass security/ parental controls.
- Scan transmitted content for malware before delivery.
- Scan outbound content, e.g., for data leak protection.
- Circumvent regional restrictions.

6.3.19Public key Infrastructure (PKI)

Description:

It is an arrangement that binds public keys with respective user identities by means of a certificate authority; where the set of hardware, software, people, policies, and procedures are created, managed, distributed, used, stored and revoke digital certificates. The user identity must be unique for each Certificate Authority. For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgettable in public key certificates issued by the CA.

Standard Details:

There are 3 approaches to getting this trust: Certificate Authorities (CAs), Web of Trust (WoT), and Simple public key infrastructure (SPKI).

1. Certificate Authorities: The primary role of the CA is to publish the key bound to a given user. This is done using the CA's own key, so that trust in the user key relies on one's trust in the validity of the CA's key. In the context of Nepal, as informed by the “Office of the Controller of Certificates(OCC)” in Nepal, only a government accredited CA is allowed to issue digital certificates.

2. Web of Trust: The Web of trust scheme uses self-signed certificates and third party attestations of those certificates.
3. SPKI: Another alternative, which however does not deal with public authentication of public key information, is the simple public key infrastructure (SPKI) that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, since the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an "authorization loop" in SPKI terminology, where authorization is integral to its design.

Pls. note though approach 2(Web of Trust) & 3 (SPKI) above are general standards followed worldwide, however as per the Office of the Controller of Certificates in Nepal, these as not permitted/ or not legally valid within Nepal.

Resource Locator:

- PKI

  http://www.oasis-pki.org/resources/techstandards/

6.3.20 Remote Security (SSH)

Description:

Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Standard Details:

Secure Shell was originally created to provide secure terminal (shell) access to Unix servers over TCP/IP networks. Still today, secure replacement of Telnet-based terminal connections between servers is one of the most widespread uses of the technology. One of the key user groups for secure terminal access are system administrators who have adopted Secure Shell as the de-facto standard for administrating remote servers and other network devices.

Resource Locator:

- SSHv2

  http://www.rfc-editor.org/rfc/rfc4251.txt

6.3.21Secure Transport

6.3.21.1 Secure Socket Layer (SSL)

Description:

SSL is a commonly used protocol for managing the security of a message transmission on the Internet. The SSL protocol runs above TCP/IP and bellow higher-level protocols such as TELNET, FTP or HTTP. It provides for encryption, server and client authentication and message authentication.

Standard Details:

SSL was developed by Netscape with its major goal is to provide privacy and reliability between two communicating applications, and prevents eavesdropping, tampering or message forgery. Netscape developed

The Secure Sockets Layer Protocol (SSL) in 1994, as a response to the growing concern over security on the Internet. SSL was originally developed for securing web browser and server communications. The specification was designed in such a way so you can enable other applications, such as TELNET and FTP, to use SSL.

Resource Locator:

- Secure Socket Layer

  http://wp.netscape.com/eng/ssl3/draft302.txt

6.3.21.2 Transport security

Description:

TLS is based on the Secure Socket Layer (SSL), a protocol originally created by Netscape. It provides privacy and data integrity between two communicating applications. It is used for encapsulation of various higher level protocols.

Standard Details:

Developed by Netscape, SSL version 3.0 was released in 1996, which later served as a basis to develop TLS version 1.0, an IETF standard protocol first defined in RFC 2246. Many leading financial institutions have endorsed SSL for commerce over the Internet. SSL operates in modular fashion: its authors designed it for extendibility, with support for forwards and backwards compatibility and negotiation between peers.

Resource Locator:

- Transport Layer Security (RFC 5246)

  http://rfc-editor.org/rfc/rfc5246.txt

6.3.22 Virtual Private network (VPN)

Description:

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. It can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.It works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

Standard Details:

VPN does not need to have explicit security features such as authentication or traffic encryption. VPNs can also be used to separate the traffic of different user communities over an underlying network with strong security features, or to provide access to a network via customized or private routing mechanisms.

Generally, a VPN has a network topology more complex than a point-to-point connection. VPNs are also used to mask the IP address of individual computers within the Internet in order, to surf the World Wide Web anonymously or to access location restricted services.

Resource Locator:

- RFC 4026 VPN

  http://www.rfc-editor.org/rfc/rfc4026.txt

- RFC 2764 IP based VPN

  http://www.rfc-editor.org/rfc/rfc2764.txt

6.3.23 XML Security standards

Description:

The aim of the XML Security Standards developed by W3C and OASIS is the definition of meta-data to protect XML documents and elements. XML Digital signatures web Services security and web services interoperability address XML security Standards.

Standard Details:

WS-Security (Web Services Security) is a communications protocol providing a means for applying security to Web services. It specifies on how integrity and confidentiality can be enforced on Web services messaging. It includes details on the use of SAML and Kerberos, and certificate formats such as X.509.WS-Security describes how to attach signatures and encryption headers to SOAP messages. In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages.

WS-Security incorporates security features in the header of a SOAP message, working in the application layer. Thus it ensures end-to-end security. WS-Security however addresses the wider problem of maintaining integrity and confidentiality of messages until after a message was sent from the originating node, providing so called end to end security.

XML-Signature provides a framework assuring integrity and reliability of XML data using digital signatures. It supports signing of whole documents as well as single elements or the content of elements which analogous to XML-encryption. Digital signatures become a persistent part of the document. So, the signatures are kept verifiable permanently.

WS-I is used for web services interoperability. The basic profile (WS-I v 1.0) is developed by a set of principles. These principles are No guarantee of interoperability, Application semantics, Testability, Strength of requirements, Restriction vs. relaxation, Multiple mechanisms, Future compatibility, Compatibility with deployed services, Focus on interoperability, Conformance targets and Lower-layer interoperability.

Resource Locator:

- *XML-Signature*

  www.w3.org/TR/xmldsig-core/

- WSS

  www.oasis-open.org/committees/wss/

- WS-I

  http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html

6.3.24 *Physical Security (IP Based Security/Surveillance)*

Enterprise level physical security is nothing but surveillance i.e. monitoring behavior or activities in a surreptitious manner. The IP based security/surveillance includes equipments such as cameras, encoding & media servers, display monitor etc.

Description:

6.3.24.1 IP Based Surveillance Cameras

IP cameras/ Network cameras are Closed-circuit television (CCTV) cameras that use Internet Protocol to transmit image data and control signals over a Fast Ethernet link. They are primarily used for surveillance. A number of IP cameras are normally deployed together with a network video recorder (NVR) to form a video surveillance system.

6.3.24.2 Encoding server

Video Surveillance Encoding Server (ES) is an all-in-one appliance that encodes, distributes, manages, and archives digital video feeds. Encoding server is capable of encoding up to 64 channels or more. It provides the flexibility to meet a diverse range of video surveillance requirements.

6.3.24.3 Media server

Video Surveillance Media Server (MS) is the core component in the VSM, enabling distribution, archiving, and management of video feeds. It offers the power and flexibility to meet a diverse range of video surveillance requirements and can coexist on an IP network with other IT applications.

6.3.24.4 CODEC

A CODEC is used to convert an analogue video signal to a digital video signal either using hardware or software. Codec's play an important role in digital video recorders; they are not only used to convert the analogue signal to a digital signal but to also produce the best quality video information at the smallest file size. This makes a big difference to the amount of video that can be recorded on a DVRs hard drive.

6.3.24.5 Display screen

A video surveillance system is disclosed in which modulated signals from a plurality of video cameras are multiplexed onto a single path capable of carrying up to 4 to more than 64 video channels. One or more such communication paths are provided to a signal splitter which provides the paths to one or more video screens and tuners. The tuners are operated under computer control so as to sequence the display of information from the different video cameras. Advantageously, structure is also provided for recording the video display on a VCR when a display includes matters of interest. The computer is also responsive to alarm inputs to display on one or more screens the signals from video cameras in the area adjacent the alarm.

Standard Details:

The first IP camera was released in 1996 by Axis Communications. It used an embedded Linux platform internal to the camera. Axis also released documentation for their low-level API called "VAPIX" which builds on the open standards of HTTP and RTSP. This open architecture was intended to encourage third-party software manufacturers to develop compatible management and recording software. In order to address issues of standardization of IP video surveillance, two industry groups were formed in 2008; the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA). There are many standards of CODEC, those used for video compression that you may come across are MPEG-2, MPEG-4, JPEG 2000, AVI and H.264, H.264 is the latest codec being introduced into the CCTV market, deriving from video conferencing equipment.

Resource Locator:

- IP based Surveillance

  http://www.onvif.org/

  http://www.onvif.org/Documents/Specifications/tabid/284/Default.aspx

- Codec

  www.itu.int/rec/T-REC-H.264

6.3.25 Security of Smart Card

Description:

The self-containment of Smart Card makes them resistant to attack as they do not need to depend upon potentially vulnerable external resources. Because of this, Smart Cards are often used in applications which require strong security protection and authentication.

Standard Details:

- **ISO/IEC 7816-8:2004**

  Specifies inter-industry commands for integrated circuit cards (either with contacts or without contacts) that may be used for cryptographic operations

  The choice and conditions of use of cryptographic mechanisms may affect card exportability.

- **ISO/IEC 7816-9:2004**

  It describes the inter-industry commands of integrated circuit cards for card and files management, e.g. file creation and deletion. These commands cover the entire life cycle of the card and therefore some commands may be used before the card has been issued to the cardholder or after the card has expired.

- **ISO/IEC 7816-11:2004**

  It specifies about the usage of inter-industry commands and data objects related to personal verification through biometric methods in integrated circuit cards. It also presents examples for enrollment and verification and addresses security issues. These commands used are defined in ISO/IEC 7816-4.

- **ISO/IEC 7816-15:2004**

  It describes a card application containing information on cryptographic functionality. Further, ISO/IEC 7816-15:2004 defines a common syntax (in ASN.1) and format for the cryptographic information and mechanisms to share this information whenever appropriate.

  ISO/IEC 7816-15:2004 supports the following capabilities:

  - storage of multiple instances of cryptographic information in a card;
  - use of the cryptographic information;
  - retrieval of the cryptographic information;
  - cross-referencing of the cryptographic information with DOs defined in ISO/IEC 7816 when appropriate;

    - different authentication mechanisms; and
    - Multiple cryptographic algorithms.

- **CEN-ISSS Secure Networks and Smart Cards**
    - CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices
    - CWA 14170 Security Requirements for Signature Creation Systems
    - CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+'
    - CWA 14167 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
        - Part 1: System Security Requirements
        - Part 2 Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)
    - CWA 14890 - Application Interface for smart cards used as Secure Signature Creation Devices
        - Part 1: Basic Requirements
        - Part 2: Additional Services

    These CWAs have now been submitted to CEN TC224 for development of a European Standard and possible transposition into an ISO standard

- **ISO 9564**

    It specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs. It also specifies PIN protection techniques applicable to financial transaction-card-originated transactions in an online environment and a standard means of interchanging PIN data.

    The provisions of this part of ISO 9564 are not intended to cover:

    - PIN management and security in the offline PIN environment, which is covered in ISO 9564-3;
    - PIN management and security in the electronic commerce environments, which is to be covered in a subsequent part of ISO 9564;
    - the protection of the PIN against loss or intentional misuse by the customer or authorized employees of the issuer;
    - privacy of non-PIN transaction data;
    - protection of transaction messages against alteration or substitution, e.g. an authorization response to a PIN verification;
    - protection against replay of the PIN or transaction;
    - Specific key management techniques.

- **ISO 9564-2:2005**

It specifies algorithms for the encipherment of Personal Identification Numbers (PINs). Based on the approval processes established in ISO 9564-1, these are the data encryption algorithm (DEA) and the RSA encryption algorithm.

- **ISO 9564-3:2003**

  This standard describes the minimum security measures required for offline PIN handling and a standard means of interchanging PIN data in an offline environment. It is applicable to financial transaction card-originated transactions requiring offline PIN verification and to those institutions responsible for implementing techniques for the management and protection of the PIN at Automated Teller Machines (ATMs) and acquirer sponsored Point-of-Sale (POS) terminals.

- **ISO/TR 9564-4:2004**

  provides guidelines for personal identification number PIN handling in open networks, presenting finance industry leading -practice security measures for PIN management and the handling of financial card originated transactions in environments where issuers and acquirers have no direct control over management, or where no relationship exists between the PIN entry device and the acquirer prior to the transaction.

*This list of smartcard security standards is not exhaustive and is dynamic in nature. Additional standards with a security implication for smartcards can be found in 'Security Standards for Smart cards, Issue 1.1, dated January 2004', namely CC, ETSI, FIPS and EMVCo.

Furthermore, NIST IT 6887 2003 Edition, GSC-ISS, Version 2.1 is an architectural model for interchangeable smartcard service provider modules.

Resource Locator:

- Security Standards for Smart cards, Issue 1.1, dated January 2004', namely CC, ETSI, FIPS and EMVCo

  http://www.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif/security_standards_for_smart_cards.aspx

- ISO/IEC 7816-8:2004

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=37989

- ISO/IEC 7816-9:2004

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=37990

- ISO/IEC 7816-11:2004

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31419

- ISO/IEC 7816-15:2004

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35168

- ISO 9564

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29374

- ISO 9564-2:2005

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=36289

- ISO 9564-3:2003

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35124

- ISO/TR 9564-4:2004

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36761

6.4 Access

Access relates to provision to be made to enable users to effectively access information and service electronically via a range of delivery channels (e.g. World Wide Web) and devices (e.g. personal computers, mobile phones, PDAs) for their needs via a range of delivery channels. This is realized by using components as per technical specifications standards to enable delivery of service, user interfaces and interaction models. This is also connected with security standards to ensure security of access, integrity of data and privacy requirements.

Table 6-14: Access

Access		
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Access Technical Standards Details**
Access Token		
• All hardware tokens must have an inherent unique identity that should be tamper proof and with access restricted only to applications offered by the token vendor or another trusted organization. No other access should be permitted • The authentication should require a two-factor authentication key wherein the hardware token requiring per-session local activation (with a password or biometric). • The token design should be FIPS compliant.	Mandatory	4.4.1 Access Token
Animation		
• SVG 1.1 (.svg), as per W3C specifications. • SVG tiny1.2 as per W3C specifications for mobile specification • GIF (.gif), as per GIF89a specification	Recommendatory	4.4.2 Animation 4.4.2.1 SVG 4.4.2.2 GIF
Compression		
The following standards should be used for Compacting the files. • GNU ZIP (.gz). • Tape Archive TAR Pack (.tar). • Compact TAR Pack (.tgz ou .tar.gz).	Mandatory	4.4.3Compression 4.4.3.1 GNU 4.4.3.2 Tape Archive
Kiosk		
• The kiosk machine should support the Content management and personalization technologies used for delivering services. • The Kiosk should support the application needs	Recommendatory	4.4.4 Kiosk

Access		
for a minimum period of 5 years. • Transponder on the server side should have the capability to effect the required transformation of content for delivering it through kiosks		
Other Delivery Channels		
• Information Access covers components and technical specifications required to enable users to access Public Sector information and services electronically via a range of delivery channels like Hypertext Web Content, Document, Spreadsheet, Presentation, Character Sets and Encoding		4.4.5.1 Hypertext Web Content 4.4.5.2 Document 4.4.5.3 Spreadsheet 4.4.5.4 Presentation 4.4.5.5 Character Sets and Encoding
Mobile Devices		
• Application schedule be compatible for delivering service with mobile devices such as PDA's Wi-Fi , Digital TV etc. • Transponder on the server side should have the capability to effect the required transformation of content for the target delivery device	Recommendatory	4.4.6 Mobile Devices
Scripting		
• ECMA 262 should be the standards for server side scripting • Java Script should be the standards for client side scripting	Mandatory	4.4.7 Scripting 4.4.8 Java Script
Smart Cards – Physical		
For Physical layout location/dimension/configurations the following standards are Recommendatory : • ISO/IEC 7810 Identification cards physical characteristics • ISO/IEC 7811-1 and 7811-3: Identification cards Recording technique • ISO/IEC 7816-1 and 7816-2: Identification cards-Integrated circuit(s) cards with contacts • ISO/IEC 14443-1: Identification cards – Contactless integrated circuit(s) cards – Proximity cards • ISO/IEC 15693-1: Identification cards – Contact less integrated circuit(s) cards – Vicinity cards • BS EN 1332-2 Identification card systems – Man-machine interface	Recommendatory	4.4.9 Smart Card-Physical
Smart Cards – Electrical (Integrated Circuits)		
For the electrical(integrated circuits) related aspects the following standards are Recommendatory • ISO/IEC 7816-10: Identification cards – Integrated circuit(s) cards with contacts • ISO/IEC 7816-12 Identification cards –	Recommendatory	4.4.10 Smart Cards – Electrical (Integrated Circuits)

Access		
Integrated circuit(s) cards with contacts • ISO/IEC 14443-2: Identification cards – Contactless integrated circuit(s) cards – Proximity cards • ISO/IEC 15693-2: Identification cards – Contactless integrated circuit(s) cards – Vicinity cards		
Smart Cards – Data Definition		
For the data definition related aspects the following standards are Recommendatory • ISO/IEC 7816-6: 2004 Identification cards - Integrated circuit(s) cards with contacts • ISO/IEC 7812-1:2006 Identification cards Identification of issuers • CEN-ISSS: CWA 13987-1: 2003 Smart Card Systems - Interoperable Citizen Services - User Related Information • EN 1545-1 - Identification card systems - Surface transport applications. • EN 1545-2 - Identification card systems - Surface transport applications.	Recommendatory	4.4.11 Smart Cards – Data Definition
Smart Cards - Applications including Multi-Applications		
For the applications including multi-applications the following standards are Recommendatory • ISO/IEC 7816-4: 2005 Identification cards-- Integrated circuit(s) cards with contacts • ISO/IEC 7816-5: 2004 Identification cards -- Integrated circuit(s) cards with contacts • ISO/IEC 7816-7: 1999 Identification cards -- Integrated circuit(s) cards with contacts • ISO/IEC 7813: 2006 Identification cards, Financial transaction cards • ISO/IEC 7812-2: 2007 Identification cards Identification of issuers • EN 1332-1: 1999 Identification card systems – Man machine interface • EN 1332-4: 1999 Identification card systems – Man machine interface • Integrated Transport Smartcard Organisation (ITSO) Specification TS 1000 (version 2.1) ITSO/1000-0 Concept and Content ITSO/1000-1 General Reference ITSO/1000-2 Customer Media Data and Customer Media Architecture ITSO/1000-3 Terminals ITSO/1000-4 HOPS ITSO/1000-5 Customer Media, Data Record Definitions ITSO/1000-6 Message Data	Recommendatory	4.4.12 Smart Cards - Applications including Multi-Applications

Access		
ITSO/1000-7 ITSO Security Subsystem ITSO/1000-8 ISAM Detailed Operation (available on request from ITSO) ITSO/1000-9 ITSO Communications ITSO/1000-10 Customer Media Definitions		
Smart Cards - Communication Protocols		
For specification relating to initialization and transmission of smart cards infrastructure the following standards are Recommendatory • ISO/IEC 7816-3: Integrated circuit(s) cards with contacts • ISO/IEC 14443-3/4: Identification cards – Contactless integrated circuit(s) cards – Proximity cards • ISO/IEC 15693-3: Identification cards – Contactless integrated circuit(s) cards – Vicinity cards • ISO 8583-1: 2003 Financial transaction card originated message – interchange message specification	Recommendatory	4.4.13 Smart Cards - Communication Protocols
Smart Cards - Security		
For specification relating to security the following standards are Recommendatory • ISO/IEC 7816-8: 2004 Identification cards – Integrated circuit cards • ISO/IEC 7816-9: 2004 Identification cards – Integrated circuit cards • ISO/IEC 7816-11: 2004 Identification cards – Integrated circuit(s) cards • ISO/IEC 7816-15: 2004 Identification cards – Integrated circuit cards • CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices • CWA 14170 Security Requirements for Signature Creation Systems • CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+' • CWA 14167 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures • ISO 9564-1: 2002 Banking -- Personal Identification Number (PIN) management and security • ISO 9564-2: Banking -- Personal Identification Number management and security • ISO 9564-3: 2003 Banking -- Personal Identification Number management and security • ISO 9564-4: 2004	Recommendatory	4.4.14 Smart Cards - Security

Access		
Banking -- Personal Identification Number management and security		
Smart Card - Terminal Infrastructure		
For specification relating to terminal infrastructure the following standards are Recommendatory • EN 1332-3: 1999 Identification card systems – Man machine interface • PC/SC Standards • Consortium standards PC/SC Workgroup Interoperability Specification for ICCs and Personal Computer Systems • Unified POS Retail Peripheral Architecture • GSC-IS V2.1 The US Government Smart Card Interoperability Specification	Recommendatory	4.4.15 Smart Card - Terminal Infrastructure
Directory Access		
• LDAP v3 – Lightweight Directory Access Protocol version 3 should be the standard to locate and access information stored in directories	Mandatory	4.4.16 Directory Access
Web Access standard		
• WCAG should be the standard for making information accessible to people with special needs. • WCAG is part of the series of web accessibility guidelines published by the w3c's web accessibility initiative.	Mandatory	4.4.17 Web Access standard
Web browser		
• Web browsers should support HTM L 4.01, XHTML1.0, CSS 2.1,ECMAScript and Dom level 3 • Extensible Style sheet Language (XSL) is the language for defining how a browser will display XML content to the user.	Mandatory	4.4.18 Web browser
Work stations		
• A workstation is high level performing equipment used for technical and scientific applications. • Desktops, lap top and other computer terminal used by end users /employees daily should comply with configuration so as to serve the application needs for a minimum period of 3 years.	Mandatory	
Biometric Data Interchange		
For Biometric Data Interchange the following standards are Recommendatory • OASIS XCBF 1.1	Recommendatory	4.4.19 Biometric Data Interchange

Access		
specification • ISO/IEC 19785-1 Information Technology - Common Biometric Exchange Formats Framework • ISO/IEC 19785-2 Information Technology - Common Biometric Exchange Formats Framework • ISO/IEC 19794-1 Information Technology - Biometric data interchange formats • ISO/IEC 19794-2 Information Technology - Biometric data interchange formats • ISO/IEC 19794-3 Information Technology - Biometric data interchange formats • ISO/IEC 19794-4 Information Technology - Biometric data interchange formats • ISO/IEC 19794-5 Information Technology - Biometric data interchange formats • ISO/IEC 19794-6 Information Technology - Biometric data interchange formats • ISO/IEC 19794-7 Information Technology - Biometric data interchange formats • ISO/IEC 10918-1: 1994 Information Technology - Digital compression and coding of continuous-tone still images: Requirements and Guidelines • ISO/IEC 10918-2: 1995 Information Technology - Digital compression and coding of continuous-tone still images: Compliance testing • ISO/IEC 10918-3: 1997 Information Technology - Digital compression and coding of continuous-tone still images: Extension • ISO/IEC 10918-4: 1999 Information Technology - Digital compression and coding of continuous-tone still images • ISO/IEC 15444-1: 2004 Information Technology - JPEG 2000 image coding system • ISO/IEC 15444-2: 2004 Information Technology - JPEG 2000 image coding system • ISO/IEC 15444-4: 2004 Information Technology - JPEG 2000 image		

Access		
coding system • ISO/IEC 15444-12: 2004 Information Technology - JPEG 2000 image coding system • ISO/IEC 10918-3:1997/ Amd 1:1999 • ISO/CD 19092-1 and 2 Financial Services – Biometrics • ISO/IEC DIS 19784-1.2 Information Technology - Biometric application programme interface • Common Biometric Exchange File Format (CBEFF) April 5, 2004 • ANSI X9.84-2003 Biometric Information Management and Security for the Financial Services Industry • Biometric Device Protection Profile (DBPP) • Biometric Security Guidance		
Smart Travel Documents		
For smart travel documents the following standards are Recommendatory • ISO/IEC 7501-1 Identification cards – Machine readable travel documents • ISO/IEC 7501-2 Identification cards – Machine readable travel documents • ISO/IEC 7501-3 Identification cards – Machine readable travel documents	Recommendatory	4.4.20 Smart Travel Documents

6.4.1 Access Token

Description:

A security token (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) is a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens.

Security tokens are used to prove one's identity electronically (e.g. a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. Device protects cryptographic keys and performs cryptographic operations. Use of the hardware token normally requires entry of activation data such as a password or biometric. Hardware tokens are typically small enough to be carried in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys, such as a digital signature, or biometric data, such as a fingerprint minutia. Some designs feature tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number. Special designs include a USB connector, RFID functions or Bluetooth wireless interface to enable transfer of a generated key number sequence to a client system. There are different types of tokens such as, disconnected tokens, connected tokens (e.g. Smartcards Contactless tokens (e.g. Bluetooth tokens, GSM cellular phones) and Single sign-on software tokens. For the advantages of constant view, Ease of use and speed; it is Recommendatory to have connected token and single sign on token for this version of the eGIF.

Details of Standards:

Processing standards are published as Federal Information Processing Standards (FIPS). FIPS – 197 is the Advanced Encryption Standard (AES), for example. FIPS are published by the National Institute of Standards and Technology (NIST). The primary purpose is to develop standards for government use when there are requirements that are not met with existing voluntary standards. FIPS standards 140-1,140-2 and 186- 3 can be had as the reference standards. The details of the standards are provided in a separate Zip file name xxAccess token FIPS standards. The essence of the standard is it requires a two-factor authentication key that is at least a hardware token requiring per-session local activation (with a password or biometric).

- The definition of activation data should be clear
- The authentication should minimum require a two-factor authentication key wherein the hardware token requiring per-session local activation (with a password or biometric).

Resource Locator:

- FIPS – 197

  http://csrc.nist.gov/publications/PubsFIPS.html

6.4.2 Animation

Animation standards are used interchange animated files between related parties. These are file types for interchange between agencies and ministries.

6.4.2.1 Scalable Vector Graphics (SVG)

Description:

SVG is a language for describing two-dimensional graphics and graphical applications in XML. SVG 1.1 is a W3C Recommendation and is the most recent version of the full specification. Sophisticated applications of SVG are possible by use of a supplemental scripting language which accesses. SVG Document Object Model (DOM), which provides complete access to all elements, attributes and properties. A rich set of event handlers such as on mouse over and on click can be assigned to any SVG graphical object. Because of its compatibility and leveraging of other Web standards, features like scripting can be done.

SVG Tiny 1.2 is a W3C Recommendation, and targets mobile devices. SVG drawings can be interactive and dynamic. Animations can be defined and triggered either declaratively (i.e., by embedding SVG animation elements in SVG content) or via scripting.

Details of the Standards:

There are various SVG modules under development which will extend previous versions of the specification, and which will serve as the core of future SVG developments. The SVG Working Group is currently working in parallel on a set of modules, for extending prior specifications, and a new specification. Scalable Vector Graphics (SVG) Version 1.1 defines the features and syntax.

SVG Tiny 1.2 is a format suitable for everything from mobile devices to embedded multimedia systems to desktop browsers. It is already deployed widely on mobile phones and other devices around the world, where it is used both to browse Web content and as the main user interface for the device. Scalable Vector Graphics is used as both a Web-viewable interchange format and as an interactive multimedia platform, and is a key part of the sustainable Web. SVG 1.2 Tiny is a profile of SVG intended for implementation on a range of devices, from cellphones and PDAs to laptop and desktop computers, and thus includes a subset of the features included in SVG 1.1

Resource Locator:

- SVG 1.1 specifications

  http://www.w3.org/TR/SVG11/REC-SVG11-20030114.pdf

  http://www.w3.org/TR/SVG/

- SVG tiny 1.2

  http://www.w3.org/TR/SVGTiny12/

6.4.2.2The Graphics Interchange Format- GIF(sm)

Description:

GIF defines a protocol intended for the on-line transmission and interchange of raster graphic data in a way that is independent of the hardware used in their creation or display.

The GIF is defined in terms of blocks and sub-blocks which contain relevant parameters and data used in the reproduction of a graphic. A GIF Data Stream is a sequence of protocol blocks and sub-blocks representing a collection of graphics. GIF provides high-quality, high-resolution graphics to be displayed on a variety of graphics hardware and is intended as an exchange and display mechanism for graphics images.

Standard Details:

Compuserve released the technical specification for GIF89a is generally accepted as the technical specification. Format is defined with the assumption that an error-free Transport Level Protocol is used for communications; the Format makes no provisions for error-detection and error-correction.

The GIF Data Stream must be interpreted in context, that is, the application program must rely on information external to the Data Stream to invoke the decoder process. A typical GIF89a File Structure looks like the following

- GIF89a HEADER
- LOGICAL SCREEN DESCRIPTOR BLOCK
  - may include an optional GLOBAL COLOR TABLE (99.5% of the time this will be present)
- optional APPLICATION EXTENSION BLOCK(:-> surprise)
- a stream of graphics (each graphic being composed of the following)
  - an optional GRAPHIC CONTROL BLOCK (one preceding each IMAGE)

    - a single IMAGE DESCRIPTOR or PLAIN TEXT BLOCK
        - which can include an optional LOCAL COLOR TABLE for an image
        - and the actual IMAGE or TEXT data table
- GIF TRAILER ends the series of images

Resource Locater:

- GIF

  http://www.w3.org/Graphics/GIF/spec-gif89a.txt

6.4.3 Compression

Compression is used to ease the size of files for interchange in between related parties. The compression happens by reducing the overall number of bits and bytes in a file so that files can be transmitted faster over slower Internet connections or take up less space on a disk. Once you download the file, the computer uses programs and the compression standards are nothing but these various programs that help in this process.

Most types of computer files are fairly redundant. File-compression programs simply get rid of the redundancy. Instead of listing a piece of information repeatedly, a file-compression program lists that information once and then refers back to it whenever it appears in the original program.

For e.g. Let us take an imaginary statement "Ask not what ICT can do for you – instead ask what you can do for ICT."

The quote has 17 words, made up of 52 letters, 16 spaces and one dash. If each letter, space or punctuation mark takes up one unit of memory, we get a total file size of 67 units. To get the file size down, we need to look for redundancies.

Immediately, we notice that:

"ask" is repeated twice

"what" is repeated twice

"your" is repeated twice

"ICT" is repeated twice

"can" is repeated twice

"do" is repeated twice

"for" is repeated twice

"you" is repeated twice

If we examine roughly half of the phrase is redundant. Only Nine words – ask, not, what, your, ICT, can, do, for, you –is needed. To construct the second half of the phrase, we just point to the words in the first half and fill in the spaces and punctuation.

6.4.3.1 GNU ZIP (.gz).

Description:

GNU Gzip is a popular data compression program originally written by Jean-loup Gailly for the GNU project. Mark Adler wrote the decompression part, the development of Gzip, and GNU in general, is a volunteer effort, and everyone can contribute to the development. It is free software; users can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation.

Standard Deatils

gzip reduces the size of the named files using Lempel-Ziv coding (LZ77). Whenever possible,

Each file is replaced by one with the extension '.gz', while keeping the same ownership modes, access and modification times. (The default extension is '-gz' for Virtual Memory System, 'z' for MSDOS, OS/2 FAT and Atari.) If no files are specified or if a file name is "-", the standard input is compressed to the standard output. Gzip will only attempt to compress regular files. In particular, it will ignore symbolic links.

If the new file name is too long for its file system, gzip truncates it. Gzip attempts to truncate only the parts of the file name longer than 3 characters. (A part is delimited bydots.) If the name consists of small parts only, the longest parts are truncated. For example, if file names are limited to 14 characters, gzip.msdos.exe is compressed to gzi.msd.exe.gz.

Names are not truncated on systems which do not have a limit on file name length. By default, gzip keeps the original file name and time stamp in the compressed file. These are used when decompressing the file with the '-N' option. This is useful when the compressed file name was truncated or when the time stamp was not preserved after a file transfer. However, due to limitations in the current gzip file format, fractional seconds are discarded. Also, time stamps must fall within the range 1970-01-01 00:00:00 through2106-02-07 06:28:15 UTC, and hosts whose operating systems use 32-bit time stamps are further restricted to time stamps no later than 2038-01-19 03:14:07 UTC. The upper bounds assume the typical case where leap seconds are ignored.

Compressed files can be restored to their original form using 'gzip –d' or gunzip orzcat. If the original name saved in the compressed file is not suitable for its file system, anew name is constructed from the original one to make it legal.gunzip takes a list of files on its command line and replaces each file whose name endswith '.gz', '.z' '-gz', '-z', or '_z' (ignoring case) and which begins with the correct magic number with an uncompressed file without the original extension. Gunzip also recognizes the special extensions '.tgz' and '.taz' as shorthands for '.tar.gz' and '.tar.Z' respectively. When compressing, gzip uses the '.tgz' extension if necessary instead of truncating a file with a '.tar' extension.

Gunzip can currently decompress files created by gzip, zip, compress or pack. The detection of the input format is automatic. When using the first two formats, gunzip checks a 32 bit CRC (cyclic redundancy check). For pack, gunzip checks the uncompressed length. The compress format was not designed to allow consistency checks. However gunzip is sometimes able to detect a bad '.Z' file. If you get an error when uncompressing a '.Z'file, do not assume that the '.Z' file is correct simply because the standard uncompress does not complain. This generally means that the standard uncompress does not check its input,and happily generates garbage output. The SCO 'compress –H' format (LZH compression method) does not include a CRC but also allows some consistency checks.

Files created by zip can be uncompressed by gzip only if they have a single member compressed with the 'deflation' method. This feature is only intended to help conversion of 'tar.zip' files to the 'tar.gz' format. To extract a zip file with a single member, use a command like 'gunzip <foo.zip' or 'gunzip –S .zip foo.zip'. To extract zip files with several members, use unzip instead of gunzip.

Zcat is identical to 'gunzip –c'. zcat uncompresses either a list of files on the command line or its standard input and writes the uncompressed data on standard output. Zcat will uncompress files that have the correct magic number whether they have a '.gz' suffix or not. Gzip uses the Lempel-Ziv algorithm used in zip and PKZIP. The amount of compression obtained depends on the size of the input and the distribution of common substrings. Typically, text such as source code or English is reduced by 60-70%. Compression is generally much better than that achieved by LZW (as used in compress), Huffman coding (as used in pack), or adaptive Huffman coding (compact).

Compression is always performed, even if the compressed file is slightly larger than the original. The worst case expansion is a few bytes for the gzip file header, plus 5 bytes every 32K block, or an expansion ratio of 0.015% for large files.

Resource Locator

- GZIP.pdf

  http://www.gnu.org/software/gzip/

6.4.3.2Tape Archive (TAR)

Description

In computing, tar is both a file format and the name of a program used to handle such files. The format was standardized by POSIX.1-1988 and later POSIX.1-2001.

Standard Details:

Initially developed to be written directly to sequential I/O devices for tape backup purposes, it is now commonly used to collect many files into one larger file for distribution or archiving, while preserving file system information such as user and group permissions, dates, and directory structures.

Resource Locator:

- TAR

  http://www.gnu.org/software/tar/

6.4.4 Kiosk

Description

Kiosk is a computer/VDU that displays e services information for people at various locations such as shopping malls, Bus/train stations/Airports.

More sophisticated kiosks let users interact and include touch screens, sound, and motion video. A number of companies specialize in creating multimedia kiosks. A simple kiosk can be created using HTML pages and graphics, setting the typesize large enough to attract people from a short distance, and removing the Web browser's tool bar so that the display screen. The presentation can be designed to simply loop through a series of pages or to allow user interaction and exploration.

Standard Details:

- The kiosk machine should support the Content management and personalization technologies used for delivering services.

- The Kiosk should support the application needs for a minimum period of 5 years
- Transponder on the server side should have the capability to effect the required transformation of content for delivering it through kiosk.

Resource Locator: http://en.wikipedia.org/wiki/Kiosk

6.4.5 Other Delivery Channel

6.4.5.1 Hypertext Web Content

Description

Hypertext Web Content standards are required to specify the development and formatting of hypertext documents for presentation on browsers via a range of delivery channels including Internet and Intranet.

Standard Details:

Recommended standards / specifications:

- HTML v4.01 – Hypertext Markup Language version 4.01 : HTML is a simple markup language used to create hypertext documents that are platform independent. It is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. HTML markup can represent hypertext news, mail, documentation, and hypermedia; menus of options; database query results; simple structured documents with in-lined graphics; and hypertext views of existing bodies of information.
- XHTML v1.0 – Extensible Hypertext Markup Language version 1.0: W3C describes XHTML (eXtensible Hypertext Markup Language) as "a reformulation of HTML v4.0 as an application of the XML." XHTML v1.0 reproduces and extends HTML v4 as XML and promises, with the advent of XHTML modularization, to simplify future extensions and to enable support for multiple devices. XHTML v1.0 was designed to enable easy migration of HTML content to XHTML and XML.

Resource Locator:

- HTML

  http://www.w3.org/TR/html401/
- XHTML

  http://www.w3.org/TR/xhtml1

6.4.5.2Document

Description

Standards on Document are required to define the format and file types of documents for interchange between agencies and departments as well as third parties.

Standard Details:

Recommended standards / specifications:

- Plain Text format (.txt) – It is the de facto standard for plain/unformatted text extensively supported by word processing packages, publishing tools, content management applications, e-mail applications etc.
- Rich Text format (.rtf) version 1.6 – The Rich Text Format (RTF) specification provides a format for text and graphics interchange that can be used with different output devices, operating environments, and operating systems. RTF uses the American National Standards Institute (ANSI),PC-8, Macintosh, or IBM PC character set to control the representation and formatting of a document, both on the screen and in print. With the RTF specification, documents created under different operating systems and with different software applications can be transferred between those operating systems and applications.
- Portable Document format (.pdf) version 3, 4, 5 – The Portable Document Format (PDF), developed by Adobe Systems Inc., is a computer file format designed to publish and distribute electronic documents. PDF is related to the Postscript language, and may be used with text, image, and/or multimedia files. PDF files may be created and used on most any type of computer e.g. Windows, Macintosh, UNIX, or OS/2. Unlike other electronic file formats such as HTML or XML, the PDF captures all of the elements of a printed document as an electronic image and preserves the exact layout, font attributes, and formatting of the document from which it was created, ensuring that the electronic version of a document appears just like the original. Users can view, navigate, print and forward to other users.
- Microsoft Word Document (.doc) – This is proprietary Microsoft Word document format. This format is to be used in inter-departmental information interchange between users of Microsoft Word. However In future Open Document Format for Office Applications formats can be considered.

Resource Locator:

- RTF

  http://msdn.microsoft.com/library/?url=/library/enus/dnrtfspec/html/rtfspec.asp?frame=true

- PDF

  http://www.adobe.com/products/acrobat/adobepdf.html

- Word Document

  http://www.microsoft.com/office/word/default.asp

6.4.5.3 Spreadsheet

Description

Standards on Spreadsheet are required to define the format and file types of spreadsheets for interchange between agencies and departments as well as third parties.

Standard Details:

Recommended standards / specifications:

- Comma Separated Variable/Delimited files format (.csv) – for spreadsheet interoperable across spreadsheet applications. .csv is the de facto standard for delimited files for use in interdepartmental information interchange.

- Microsoft Excel Spreadsheet (.xls) – Excel 2003 or higher. Microsoft Excel is one of the major spreadsheet applications both in public and private sector. It is supported by open source alternatives. However In future Open Document Format for Office Applications formats can be considered.

Resource Locator:

- Excel

  http://www.microsoft.com/office/excel/default.asp

6.4.5.4 Presentation

Description

Standards on Presentation are required to define the format and file types of presentations for interchange between agencies and departments as well as third parties.

Standard Details:

Recommended standards / specifications:

- Hypertext Document format (.htm) – for presentation interoperable across dominant browsers
- Portable Document format (.pdf) – for read-only presentation
- Microsoft PowerPoint Presentation (.ppt) – PowerPoint 2003 or higher. .ppt presentation file type is the proprietary Microsoft PowerPoint presentation format. This format is to be used in inter-departmental information interchange between users of Microsoft PowerPoint. However In future Open Document Format for Office Applications formats can be considered.

Resource Locator:

- Excel

  http://www.microsoft.com/office/powerpoint/default.asp

6.4.5.5 Character Sets and Encoding

Description

Character Sets and Encoding standards define the character sets to be used for content to be interchanged in English or Nepali, as well as how those characters are to be encoded.

Standard Details:

Recommended standards / specifications:

- ASCII – American Standard Code for Information Interchange : ASCII is a character set and a character encoding based on the Roman alphabet as used in modern English. It is most commonly used by computers and other communication equipment to represent text and by control devices that work with text.
- ISO/IEC 10646-1:2000 (revision of ISO 10646): ISO 10646 is an ISO standard to encode the characters of the major languages of the world into a single character set. ISO 10646 is code-for-code compatible with Unicode which can be considered as an implementation of 10646. Unicode can be encoded in

different ways. Data messages (e.g. XML messages) encoded in Unicode should adopt UTF-8 as the encoding standard unless the Government specifies otherwise.

- UTF-16 – Universal Character Set (UCS) Transformation Format 16 Bit : The Unicode Standard [UNICODE] and ISO/IEC 10646 [ISO-10646] jointly define a coded character set (CCS), hereafter referred to as Unicode, which encompasses most of the world's writing systems. UTF-16, the object of this specification, is one of the standard ways of encoding Unicode character data; it has the characteristics of encoding all currently defined characters (in plane 0, the BMP) in exactly two octets and of being able to encode all other characters likely to be defined (the next 16 planes) in exactly four octets.
- UNICODE version 3 : The Unicode Standard is the universal character encoding scheme for written characters and text. It defines a consistent way of encoding multilingual text that enables the exchange of text data internationally and creates the foundation for global software. As the default encoding of HTML and XML, the Unicode Standard provides a sound underpinning for the World Wide Web and new methods of business in a networked world. Required in new Internet protocols and implemented in all modern operating systems and computer languages such as Java, Unicode is the basis of software that must function all around the world.

Resource Locator:

- ASCII

  http://www.columbia.edu/kermit/ascii.html
- ISO/IEC 10646

  http://www.iso.ch/iso/en/ISOOnline.frontpage
- UTF 16

  http://www.ietf.org/rfc/rfc2279.txt
- UNICODE

  http://www.unicode.org/

  http://www.unicode.org/versions/Unicode5.2.0/

6.4.6 Mobile devices

Description:

The mobile devices referred here are devices used to access e service/application on mobility such as PDAs/Smart phones/Digital TV etc. Open Mobile Alliance(OMA) standards are emerging in this space. OMA facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks while allowing businesses to compete through innovation and differentiation.

Standard Details:

Some of the key requirements of Mobile devices from ensuring interoperability perspective are

- Application schedule be compatible for delivering service on with the mobile devices such as PDA's Wi-Fi , Digital TV

- Transponder on the server side should have the capability to effect the required transformation of content for the target delivery device.

- Compliance of Mobile phones to OMA standard which are open standards for the mobile phone industry should be encouraged. The OMA has various specifications A checklist of such specification during the procurement will help ensuring the enforcement of this standard. The specifications include:

    - Browsing specifications, now called "Browser and Content", previously called WAP browsing. In their current version, these specifications rely essentially on XHTML Mobile Profile.
    - MMS specifications for multimedia messaging
    - OMA DRM specifications for Digital Rights Management
    - OMA Instant Messaging and Presence Service (OMA IMPS) specification, which is a system for instant messaging on mobile phones (formerly known as Wireless Village).
    - OMA SIMPLE IM Instant messaging based on SIP-SIMPLE
    - OMA CPM Converged IP Messaging
    - OMA Client Provisioning (OMA CP) specification for Client Provisioning.
    - OMA Data Synchronization (OMA DS) specification for Data Synchronization using SyncML.
    - OMA Device Management (OMA DM) specification for Device Management using SyncML.
    - OMA BCAST specification for Mobile Broadcast Services.
    - OMA PoC specification for Push to talk Over Cellular.
    - OMA Presence SIMPLE specification for Presence based on SIP-SIMPLE.
    - OMA Service Environment
    - FUMO Firmware update
    - SUPL, an IP-based service for assisted GPS on handsets.

Resource Locator

- OMA Standards

  http://www.openmobilealliance.org/Technical/PublicMaterial.aspx

6.4.7 Scripting

Description:

ECMA Script is a vendor- neutral scripting language, standardized by ECMA international in the ECMA-262 specification and ISO/IEC 16262. The language is widely used on the web, especially in the form of its three best-known dialects, JavaScript, Action Script, and J Script. ECMA Script is an object-oriented programming language for performing computations and manipulating computational objects within a host environment. ECMA Script as defined here is not intended to be computationally self-sufficient; indeed, there are no provisions in this specification for input of external data or output of computed results. Instead, it is expected that the computational environment of an ECMA Script program will provide not only the objects and other facilities described in this specification but also certain environment-specific host objects, whose description and behavior are beyond the scope of this specification except to indicate that they may provide certain properties that can be accessed and certain functions that can be called from an ECMA Script program. ECMA Script was originally designed to be a Web scripting language, providing a mechanism to enliven Web pages in browsers and to perform server computation as part of Web-based client-server architecture. ECMA Script can provide core scripting capabilities for a variety of host environments, and therefore the core scripting language is specified in this document apart from any particular host environment.

Standard Details:

A conforming implementation of ECMA Script shall

- provide and support all the types, values, objects, properties, functions, and program syntax and semantics described in this specification.

- interpret characters in conformance with the Unicode Standard, Version 3.0 or later and ISO/IEC 10646-1 with either UCS-2 or UTF-16 as the adopted encoding form, implementation level 3. If the adopted ISO/IEC 10646-1 subset is not otherwise specified, it is presumed to be the BMP subset, collection 300. If the adopted encoding form is not otherwise specified, it presumed to be the UTF-16 encoding form.

- provide additional types, values, objects, properties, and functions beyond those described in this specification. In particular, a conforming implementation of ECMAScript is permitted to provide properties not described in this specification, and values for those properties, for objects that are described in this specification.

- support program and regular expression syntax not described in this specification. In particular, a conforming implementation of ECMA Script is permitted to support program syntax that makes use of the “future reserved words” listed in 7.6.1.2 of this specification.

Resource Locator:

- ECMA-262

  www.ecma-international.org/publications/standards/Ecma-262.HTM

6.4.8 Java Script

Description:

JavaScript is an object-oriented client-side Scripting language used to enable programmatic access to objects within both the client application and other applications. It is implemented as an integrated component of the web browser, allowing the development of enhanced user interfaces and dynamic websites. JavaScript is a dialect of the ECMA Script standard and is characterized as a dynamic, weakly typed, prototype-based language with first-class functions.

JavaScript was influenced by many languages and was designed to look like Java, but to be easier for non-programmers to work with. There are comprehensive frameworks and libraries of JavaScript programming practices that make it not only popular but also. Because JavaScript is the only language that the most popular browsers share support for, it has become a target language for many frameworks in other languages, even though JavaScript was never intended to be such a language.

Standards details:

Java script features conform to ECMA Script implementations. As of 2009, the latest version of the language is JavaScript 1.8.1. It is a superset of ECMA Script (ECMA-262) Edition 3. Extensions to the language, including partial E4X (ECMA-357) support and experimental features considered for inclusion into future ECMA Script editions.

JavaScript code can run locally in a user's browser and it can respond to user actions quickly, JavaScript code can detect user actions (such as individual keystrokes) which HTML will not be able to do.

DOM interfaces for manipulating web pages are not part of the ECMA Script standard, or of JavaScript. Officially, they are defined by a separate standardization effort by the W3C; in practice, browser implementations differ from the standards and not all browsers execute JavaScript.

To deal with these differences, an attempt to write standards-compliant code which will also be executed correctly by most browsers can be done alternatively code can be written to check for the presence of certain browser features and behaves differently. Programmers may use libraries or toolkits which take browser differences into account.

While programming the script care should be taken to check the browser for the following things:

- if a browser is old or rare browser with incomplete or unusual DOM support,
- if any incompatibility exist for PDA or mobile phone browser which cannot execute JavaScript,
- if there are any security precaution that will disable JavaScript execution

Resource Locator:

- Java Script

  https://developer.mozilla.org/En/New_in_JavaScript_1.8.1

6.4.9 Smart Cards – Physical

Description:

Smart cards have lot of access related standards such as for Physical layout location/dimension/configurations, for the electrical (integrated circuits) related aspects and for specification relating to initialization and transmission of smart cards infrastructure.

Standard Details:

The following standards are Recommendatory for physical layout location/dimension/configurations:

ISO/IEC 7810

This standard is one of a series of standards describing the characteristics of identification cards. It is the purpose of ISO/IEC 7810:2003 to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements.

ISO/IEC 7810:2003 specifies:

- four different sizes of identification cards with a nominal thickness of 0,76 mm and dimensions of:
  - ID-000 25 mm x 15 mm
  - ID-1 85,60 mm x 53,98 mm
  - ID-2 105 mm x 74 mm
  - ID-3 125 mm x 88 mm
- the conditions for conformance
- the dimensions and tolerances of the identification cards
- the construction and materials of the identification cards
- the physical characteristics of the cards such as bending stiffness, flammability, toxicity, resistance to chemicals, dimensional stability, adhesion or blocking, warpage, resistance to heat, surface distortions, and contamination.
- ISO/IEC 7810:2003, together with a standard for test methods, provides for interchange between various types of identification card processing devices and system**s.**

ISO 7811-1

- ISO/IEC 7811 is one of a series of standards describing the parameters for identification cards as defined in the definitions clause and the use of such cards for international interchange. This part of ISO/IEC 7811 specifies requirements for embossed characters on identification cards. The embossed characters are intended for transfer of data either by use of imprinters or by visual or machine reading. It takes into consideration both human and machine aspects and states minimum requirements. It is the purpose of this series of standards to provide criteria to which cards shall perform. No consideration is given within these standards to the amount of use, if any, experienced by the card prior to test. Failure to conform to specified criteria should be negotiated between the involved parties.
- ISO/IEC 7811 consists of the following parts, under the general title Identification cards — Recording technique:
  - Embossing
  - Magnetic stripe — Low coercivity
  - Magnetic stripe — High coercivity

ISO/IEC 7816-1

This standard specifies the Physical Characteristics of the Card.

ISO/IEC 7816-2

This part has been revised to reduce some of its options, especially in the area of embossing (which has been shown to be detrimental to embedded silicon) and phasing out of the original contact positions.

ISO/IEC 14443-1

ISO/IEC 14443 defines a proximity card used for identification, and the transmission protocols for communicating with it. ISO/IEC 14443-1:2008 defines the physical characteristics of PICCs, commonly known as proximity cards. It is to be used in conjunction with other parts of ISO/IEC 14443.

ISO/IEC 15693-1

It is an ISO standard for "Vicinity Cards", i.e. cards which can be read from a greater distance as compared to Proximity cards. ISO/IEC 15693 systems operate at the 13.56 MHz frequency, and offer maximum read distance of 1-1.5 meters. As the vicinity cards have to operate at a greater distance, the necessary magnetic field is less (0.15 to 5 A/m) than that for a proximity card (1.5 to 7.5 A/m).

BS EN 1332-2

BS EN 1332-2 is used where embossing is not used and there is a requirement for the user to present the card in a particular orientation, a tactile identifier should be provided as an aid to those with impaired vision.

Resource Locator:

- ISO/IEC 7810:2003

  http://www.iso.org/iso/catalogue_detail?csnumber=31432
- ISO 7811-1

  http://webstore.iec.ch/preview/info_isoiec7811-1%7Bed3.0%7Den.pdf
- ISO 7816-1

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=29257
- ISO/IEC 14443-1

  http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693
- ISO/IEC 15693-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30995

6.4.10 Smart Cards - Electrical (Integrated Circuits)

Standard Details:

Following standards are Recommendatory for the Electrical (integrated circuits) related aspects:

ISO/IEC 7816-10

This part of the standard specifies the power, signal structures, and the structure for the answer to reset between an integrated circuit card(s) with synchronous transmission and an interface device such as a terminal.

ISO/IEC 7816-12

ISO/IEC 7816-12:2005 specifies:

- the electrical conditions when a USB-ICC is operated by an interface device - for those contact fields that are not used, when the USB interface is applied;
- the USB standard descriptors and the USB-ICC class specific descriptor;
- the data transfer between host and USB-ICC using bulk transfers or control transfers;
- the control transfers which allow two different protocols named version A and version B;
- the (optional) interrupt transfers to indicate asynchronous events;

- Status and error conditions.

ISO/IEC 7816-12:2005 provides two protocols for control transfers. This is to support the protocol T=0 (version A) or to use the transfer on APDU level (version B). ISO/IEC 7816-12:2005 provides the state diagrams for the USB-ICC for each of the transfers (bulk transfers, control transfers version A and version B). Examples of possible sequences which the USB-ICC must be able to handle are given in an informative annex.

ISO/IEC 14443-2:

Standard pertains to Contactless integrated circuit(s) cards -- Proximity cards and Radio frequency power and signal interface.

ISO/IEC 15693-2:

ISO/IEC 15693-2:2006 defines the power and communications interface between the vicinity card and the reading device.

Resource Locator:

- ISO/IEC 7816-10

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=30558
- ISO/IEC 7816-12

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40604
- ISO/IEC 14443-2:

  http://www.iso.org/iso/catalogue_detail?csnumber=28729
- ISO/IEC 15693-2:

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39695

6.4.11 Smart Cards - Data Definition

Standard Details:

The following standards are Recommendatory for data definition:

ISO/IEC 7816-6

ISO/IEC 7816-6 specifies interindustry data elements for interchange. It specifies the Data Elements (DEs) used for interindustry interchange based on integrated circuit cards (ICCs) both with contacts and without contacts. It gives the identifier, name, description, format, coding and layout of each DE and defines the means of retrieval of DEs from the card.

ISO/IEC 7812-1

ISO/IEC 7812-1 specifies a numbering system for the identification of issuers of cards that require an issuer identification number to operate in international, interindustry and/or intra-industry interchange.

CEN-ISSS: CWA 13987-1

CWA 13987-1 defines the concept of card association (defines roles and responsibilities) and also deals with the optimisation of use of existing smartcard infrastructure.

EN 1545-1

EN 1545-1 defines the codification of data elements used for public transport (such as date, time, validation event, transport contact, etc.)

EN 1545-2

Resource Locator:

- ISO/IEC 7816-6

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38780

- ISO/IEC 7812-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39698

6.4.12Smart Cards - Applications including Multi-Applications

Standard Details:

The following standards are Recommendatory for applications including multi-applications:

ISO/IEC 7816-4

This standard specifies the contents of command-response, means of data retrieval, structure of operational characteristics of the card, structure of application data, methods of file access. A secure architecture defining access rights to files and data in the card, means and mechanisms for identifying and addressing applications in the card, methods for secure messaging, access methods to the algorithms processed by the card. It does not describe these algorithms.

ISO/IEC 7816-5

A register of application providers is kept by KTAS† in Denmark and used for application selection through the use of unique application identifier numbers. Registration in the UK is via BSI, and has been delegated to APACS. The current edition was published in June 1994. There is also an amendment ISO/IEC 7816-5/AM1 Registered application provider identifiers (RIDs) which was published in December 1996

ISO/IEC 7816-7

It defines Extended Card Data Base (ECDB).

ISO/IEC 7813

This International Standard specifies the data structure and data content of track data used to initiate financial transactions. It takes into consideration both human and physical aspects and states minimum requirements of conformity. It references layout, recording techniques, numbering systems, registration procedures, but not security requirements.

ISO/IEC 7812-2

ISO/IEC 7812-2 is one of a series of International Standards describing the parameters for identification cards, and the use of such cards for international and/or inter-industry interchange.

EN 1332-1

This standard is one of a series of International Standards describing the parameters for identification cards, and the use of such cards for human-machine interface. It details the design principles for the user interface.

EN 1332-4

This standard is one of a series of International Standards describing the parameters for identification cards, and the use of such cards for man-machine interface. It details the coding of user requirements for people with special needs.

ITSO Specification TS 1000

These standards are Crown copyright and have been developed for use in the public transport sector. Applications developed using these standards can reside on multi-application cards. Some elements of these standards could be used in areas other than transport

Resource Locator:

- ISO/IEC 7816-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36134
- ISO/IEC 7816-5

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34259
- ISO/IEC 7816-7

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=28869
- ISO/IEC 7813

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317
- ISO/IEC 7812-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39699

6.4.13Smart Cards - Communication Protocols

Standard Details:

The following standards are Recommendatory for communication protocols:

ISO/IEC 7816-3:

ISO/IEC 7816-3:2006 specifies the power and signal structures, and information exchange between an integrated circuit card and an interface device such as a terminal. It also covers signal rates, voltage levels, current values, parity convention, operating procedure, transmission mechanisms and communication with the card. It does not cover information and instruction content, such as identification of issuers and users, services and limits, security features, journaling and instruction definitions.

ISO/IEC 14443-3/4:

- ISO/IEC 14443-3 deals with Initialization and anticollision of proximity cards(Contactless integrated circuit(s) cards)

- ISO/IEC 14443-4:2008 specifies a half-duplex block transmission protocol featuring the special needs of a contact less environment and defines the activation and deactivation sequence of the protocol. ISO/IEC 14443-4:2008 is intended to be used in conjunction with other parts of ISO/IEC 14443 and is applicable to proximity cards or objects of Type A and Type B.

ISO/IEC 15693-3:

ISO/IEC 15693-3:2009 specifies:

- protocol and commands,
- other parameters required to initialize communications between a vicinity integrated circuit card and a vicinity coupling device,
- methods to detect and communicate with one card among several cards ("anticollision"),
- Optional means to ease and speed up the selection of one among several cards based on application criteria.

ISO 8583-1

ISO 8583-1 defines the interchange message specification.

Resource Locator:

- ISO/IEC 7816-3

  http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=38770
- ISO/IEC 14443-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=28730
- ISO/IEC 14443-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50648
- ISO/IEC 15693-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43467
- ISO 8583-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31628

6.4.14Smart Cards – Security

Standard Details:

The following standards are Recommendatory for security configurations:

ISO/IEC 7816-8

ISO/IEC 7816-8 specifies commands for security operations.

ISO/IEC 7816-9

ISO/IEC 7816-9 specifies commands for card management.

ISO/IEC 7816-11

ISO/IEC 7816-11 specifies personal verification through biometric methods.

ISO/IEC 7816-15

ISO/IEC 7816-15 specifies cryptographic information application.

CEN-ISSS

It is used for secure networks and smart cards.

CWA 14355

This specifies the guidelines for the implementation of Secure Signature-Creation Devices.

CWA 14170

This lists the security requirements for Signature Creation Systems.

CWA 14169

This specifies Secure Signature-Creation Devices, version 'EAL 4+'.

CWA 14167

This specifies the security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
Part 1: System Security Requirements

Part 2 Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

CWA 14890

It defines the application Interface for smart cards used as Secure Signature Creation Devices

Part 1: Basic Requirements

Part 2: Additional Service

ISO 9564-1

It lists the basic principles and requirements for online PIN handling in ATM and POS systems.

ISO 9564-2

It goes into the details of approved algorithm(s) for PIN encipherment.

ISO 9564-3

ISO 9564-3 specifies the requirements for offline PIN handling in ATM and POS systems.

ISO 9564-4

ISO 9564-4 deals with Personal Identification Number management and security.

Resource Locator:

- ISO/IEC 7816-8

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37989

- ISO/IEC 7816-9

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37990
- ISO 9564-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29374
- ISO 9564-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36289
- ISO 9564-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35124
- ISO 9564-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36761

6.4.15Smart Cards - Terminal Infrastructure

Standard Details:

The following standards are Recommendatory for physical layout location/dimension/configurations:

EN 1332-3

This covers the ergonomic layout and usability of keypads. The keypad may consist of numeric, command, function and alphanumeric keys. On the basis that keypad layout impacts performance (keying speed and errors), this standard aims to enhance usability; ensure ease of use through consistency; increase customer confidence; reduce customer error; improve operating time; ensure ergonomic data entry. It also specifies the arrangement, the number and location of numeric, function and command keys, including placement of alphabetic characters on numeric keys. Design recommendations are also provided. This standard applies to all identification card systems equipped with a numeric keypad for use by the public

PC/SC Standards, Consortium standards

This is used for terminal equipment via personal computer systems with MS Windows operating system.

Unified POS Retail Peripheral Architecture

This is used for point-of-sale terminal equipment via personal computer systems and point-of-sale systems.

GSC-IS V2.1

The US Government Smart Card Interoperability Specification also referred to as NISTIR 6887.

6.4.16Directory Access

Description:

Directory access protocol is required in order to define how to locate and access information stored in standard directories, i.e. directories that provide a centralised or distributed repository of organisation, organisational units (e.g. divisions and departments), people, IT resources (e.g. printers), together with associated attributes such as user name, printer name, email address, etc.

Standards details:

LDAP is designed to provide access to X.500 or other directories, with less resource usage required than Directory Access Protocol (DAP). It is specifically targeted at management applications and browser applications that provide read/write interactive access to directories. LDAP is the dominant directory access protocol supported by all the major directory software providers. Version 3 is the latest version of LDAP and has been widely adopted.

Resource Locator:

http://datatracker.ietf.org/doc/rfc4510/

http://datatracker.ietf.org/doc/rfc4517/

http://datatracker.ietf.org/doc/rfc4523/

http://datatracker.ietf.org/doc/rfc4512/

http://datatracker.ietf.org/doc/rfc4514/

http://datatracker.ietf.org/doc/rfc4515/

http://datatracker.ietf.org/doc/rfc4516/

http://datatracker.ietf.org/doc/rfc4519/

http://datatracker.ietf.org/doc/rfc4513/

http://datatracker.ietf.org/doc/rfc4511/

6.4.17 Web Access Standard

Description:

For those unfamiliar with accessibility issues pertaining to Web page design, consider that many users may be operating in contexts very different from your own:

- They may not be able to see, hear, move, or may not be able to process some types of information easily or at all.
- They may have difficulty reading or comprehending text.
- They may not have or be able to use a keyboard or mouse.
- They may have a text-only screen, a small screen, or a slow Internet connection.
- They may not speak or understand fluently the language in which the document is written.
- They may be in a situation where their eyes, ears, or hands are busy or interfered with (e.g., driving to work, working in a loud environment, etc.).
- They may have an early version of a browser, a different browser entirely, a voice browser, or a different operating system.

Content developers must consider these different situations during page design. While there are several situations to consider, each accessible design choice generally benefits several disability groups at once and the Web community as a whole.

Standard Details:

WCAG should be the standard for making information accessible to people with special needs. WCAG is part of the series of web accessibility guidelines published by the w3c's web accessibility initiative. The guidelines discuss accessibility issues and provide accessible design solutions. They address typical scenarios that may pose problems for users with certain disabilities.

Resource Locator:

- Web access Standard

  http://www.w3.org/WAI/

6.4.18Web Browser

Description:

A Web browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content. Hyperlinks present in resources enable users to easily navigate their browsers to related resources.

Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by Web servers in private networks or files in file systems.

Standard Details:

Web browsers should support HTM L 4.01, XHTML1.0, CSS 2.1, ECMA Script and Dom level 3.Extensible Style sheet Language (XSL) is the language for defining how a browser will display XML content to the user. The major web browsers are Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, and Opera for Windows and Apple Safari, Mozilla Firefox and Opera for Macintosh.

Resource Locator: http://en.wikipedia.org/wiki/Web_browser

6.4.19Biometric Data Interchange

Description:

The Biometric Data Interchange Formats Package provides the security requirements for data to interchange in the format of hand geometry, face recognition, signatures, finger image, iris image and finger patterns.**The motivation for interchange standards are**

- Exchange of biometric data in nonproprietary format among multiple vendors/applications
- Compile biometric databases for use in evaluating multiple algorithms
- Produce enrollment databases that enable re-enrollment using future algorithms or algorithm enhancements

Standard Details:

The following standards are Recommendatory for smart travel documents:

OASIS XCBF 1.1 specification

These are the secure XML encodings for the patron formats specified in CBEFF, the Common Biometric Exchange File Format (NISTIR 6529).

ISO/IEC 19785-1

ISO/IEC 19785-1 provides the data elements specification for evolving international standards for biometric data interchange, format based on CBEFF.

ISO/IEC 19785-2

ISO/IEC 19785-2 provides procedures for the Operation of the Biometric Registration Authority for evolving international standards for the operation of the biometric registration authority.

ISO/IEC 19794-1

ISO/IEC 19794-1 provides the framework for evolving international standards for the operation of the biometric data interchange format.

ISO/IEC 19794-2

ISO/IEC 19794-2 provides the framework for evolving international standards for the operation of the biometric data interchange format using finger minutiae data.

ISO/IEC 19794-3

ISO/IEC 19794-3 provides the framework for evolving international standards for the operation of the biometric data interchange format using finger pattern spectral.

ISO/IEC 19794-4

ISO/IEC 19794-4 provides the framework for evolving international standards for the operation of the biometric data interchange format using finger image data.

ISO/IEC 19794-5

ISO/IEC 19794-5 provides the framework for evolving international standards for the operation of the biometric data interchange format using face image data.

ISO/IEC 19794-6

ISO/IEC 19794-6 provides the framework for evolving international standards for the operation of the biometric data interchange format using iris image data.

ISO/IEC 19794-7

ISO/IEC 19794-7 provides the framework for evolving international standards for the operation of the biometric data interchange format using signature/sign behavioural data.

ISO/IEC 10918-1

ISO/IEC 10918-1 defines requirements and guidelines for digital compression and coding of continous-tone still images.

ISO/IEC 10918- 2

ISO/IEC 10918-2 specifies procedure for compliance testing for digital compression and coding of continous-tone still images.

ISO/IEC 10918-3

ISO/IEC 10918- 3 provides extensions for digital compression and coding of continous-tone still images.

ISO/IEC 10918- 4

ISO/IEC 10918- 4 says about registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, Appn markers, SPIFF compression types and Registration Authorities (REGAUT) for digital compression and coding of continous-tone still images.

ISO/IEC 15444-1,2,4 and 12

JPEG 200 (JP2) is an ISO image compression standard support by biometrics data exchange standards for image compression, providing superior performance as compared to JPEG for the compression of facial images. In addition, JP2 provides several other features useful for the capture and storage of facial images for biometric applications

ISO/IEC 15444-1 deals with the core coding system, ISO/IEC 15444-2 with extensions , ISO/IEC 15444-4 with conformance testing and ISO/IEC 15444-12 with ISO base media file format.

ISO/IEC 10918-3

This is applicable to continuous-tone - grayscale or colour - digital still image data and to a wide range of applications which require use of compressed images. This defines extensions [including variable quantization, selective refinement, tiling, and a Still Picture Interchange File Format (SPIFF)] to processes for converting source image data to compressed image data; extensions to processes for converting compressed image data to reconstructed image data; coded representations for compressed image data; gives guidance and examples on how to implement these extensions in practice and also describes compliance tests for these extensions.

ISO/CD 19092-1

It is an ISO standard that specifies the security framework.

ISO/CD 19092- 2

It is an ISO standard that specifies the Crytographic techniques.

ISO/IEC DIS 19784-1.2

It provides a defined interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies. It includes a high-level generic biometric authentication model suited to a broad range of biometrically enabled applications and to most forms of biometric technology. An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider Interfaces (SPIs), and associated data structures.

Common Biometric Exchange File Format (CBEFF)

This is a US standard published by National Institute of Standards and Technology (NIST) as NISTIR 6529-A

ANSI X9.84-2003

This is a US standard for safeguarding the security and privacy of all biometric data in the financial services industry

Biometric Device Protection Profile (BDPP)

The Biometric Device Protection Profile (BDPP) supports policies for identification, verification, auditing, and integrity. The BDPP includes requirements concerning the connection between the individual and the Biometric Device, and the connection between the Biometric Device and the portal.

Biometric Security Guidance

For security Guidance Central government departments should refer to the Manual of Protective Security. Other parts of the public sector should refer to the e-Government strategy framework and guidance

Resource Locator:

- ISO/IEC 19785-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41047
- ISO/IEC 19785-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41048
- ISO/IEC 19794-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38745
- ISO/IEC 19794-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38746
- ISO/IEC 19794-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38747
- ISO/IEC 19794-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38748
- ISO/IEC 19794-5

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38749
- ISO/IEC 19794-6

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38750
- ISO/IEC 19794-7

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38751
- ISO/IEC 10918-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902
- ISO/IEC 10918-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=20689
- ISO/IEC 10918-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30961
- ISO/IEC 10918-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=25431

- ISO/IEC 15444-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37674
- ISO/IEC 15444-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33160
- ISO/IEC 15444-4

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39079
- ISO/IEC 15444-12

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51537

6.4.20 Smart Travel Documents

Description:

Smart travel documents are for the purpose of international travel, the identity and nationality of its holder.

Travel documents may be issued by a national government with the use of information and communication technology to provide improved services.

Standard Details:

The following standards are Recommendatory for smart travel documents:

ISO/IEC 7501-1

This document is equivalent to ICAO 9303 part 1 for Passports.

ISO/IEC 7501-2

This document is equivalent to ICAO 9303 part 2 for Visas.

ISO/IEC 7501-3

This document is equivalent to ICAO 9303 part 3 for Official Travel Documents (Cards).

Resource Locator:

- ISO/IEC 7501-1

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45562
- ISO/IEC 7501-2

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29074
- ISO/IEC 7501-3

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42771

6.5 Collaboration

Collaboration covers components and technical specifications required to enable users to collaborate, to share information and services electronically e.g. Email.

Table 6-15: Collaboration

Collaboration		
Standards Proposed	Mandatory/ Recommendatory	Reference & Links to Collaboration Technical Standards Details
Email System		
Internet standards (STD) for mailing:- • SMTP:-Internet standard for electronic mail transmission around IP networks • POP3:- Application layer internet standard protocol used by local e-mail clients to retrieve email from a server over TCP/IP. • IMAP4rev1: Protocol for retrieving e-mails over TCP/IP • The Message Transfer Agent (MTA) in e-mail systems should be LDAP enabled. • Appropriate rules and policies set in the email to protect the same from spams and other intrusions. • Any web access to e-mail can be provided only if adequate access security preventing unauthorized access and leakage of mail. • Commercial email regulations of Nepal should comply with the above standards	Mandatory	4.5.1 Email System
IP Telephony		
• IP telephony should comply withH.323 and. The Session Initiation Protocol (SIP) protocols to provide audio-visual communication sessions on any packet network.	Recommendatory	4.5.3 IP telephony
Video Conferencing		
• Simultaneous audio & video transmission through telecommunication technologies. • Also used to share documents, computer-displayed information, and whiteboards.	Recommendatory	4.5.4 Video Conferencing

6.5.1 Email System

Description:

Electronic Mail (email) is a method of composing, sending, storing, and receiving messages over electronic communication systems or Email Systems. Email Systems are both software and hardware systems that transport electronic mail messages from one computer user to another.

Standard Details:

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks where as IMAP 4 and POP3 are used to receive (retrieve) email sent across the networks. Unlike Post Office Protocol (POP3), IMAP4 provides the user the option of storing and manipulating messages on the mail server. IMAP4 allows the user to select which specific messages to download. Multi-purpose Internet Mail Extensions (MIME) has a SMTP message structure and it is the standard used for the attachment of audio, video, image, application programs, and ASCII text messages.

Extensible Style sheet Language (XSL), a family of transformation languages, allows one to describe how to format or transform files encoded in the XML standard. It Provides users flexibility for presentation style and content.

Resource Locator:

- SMTP Standards

  http://datatracker.ietf.org/doc/rfc5335/

  http://datatracker.ietf.org/doc/rfc5336/

- MIME Standards

  http://datatracker.ietf.org/doc/rfc2045/

  http://datatracker.ietf.org/doc/rfc2046/

  http://datatracker.ietf.org/doc/rfc2047/

  http://datatracker.ietf.org/doc/rfc2048/

  http://datatracker.ietf.org/doc/rfc2049/

- POP3 Standards

  http://datatracker.ietf.org/doc/rfc1939/

  http://datatracker.ietf.org/doc/rfc1957/

  http://datatracker.ietf.org/doc/rfc2445/

- IMAP4

  http://www.ietf.org/rfc/rfc2060.txt

  http://www.ietf.org/rfc/rfc2342.txt

  http://www.ietf.org/rfc/rfc2971.txt

- www.w3.org/XsL

6.5.2 IP Telephony (VoIP)

Description:

Voice over Internet Protocol (VoIP, Voice over IP) is a general term for a family of methodologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

Standards details:

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codec which encode speech allowing transmission over an IP network as digital audio via an audio stream. Technologies used to implement Voice over Internet Protocol are H.323, IP Multimedia Subsystem, Session Initiation Protocol and Real-time transport Protocol. These standards/protocols are responsible for call setup and call signaling.

- ✓ Assembly : Standards for the assembly of Audio, Video, Data and Control (AVDC),ITU H.323 (07/03), version 5
- ✓ Gateway control : The following define standards for multimedia gateways:
    - Media Gateway Control Protocol (MGCP): RFC 3661
    - Media Gateway: RFC 2805
    - Simple Gateway Control Protocol: RFC 5125
    - Megaco Protocol version 1.0: RFC 3015
    - Signalling System 7 (SS7) Message Transfer Part 3 (MTP3) User Adaptation Layer (M3UA): RFC 4666
    - Megaco: ITU H.248
- ✓ Application layer signalling : An application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants,Session Initiation Protocol (SIP): RFC 3261
- ✓ Resource setup : A resource reservation setup protocol designed for an integrated services Internet. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows,Resource ReSerVation Protocol (RSVP): RFC 2205 and RFC 2750.
- ✓ Transport and control protocol : RTP and RTCP provide end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services,Real Time Protocol (RTP) and Real Time Control Protocol (RTCP): RFC 3550
- ✓ Delivery control : RTSP is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video, Real Time Streaming Protocol (RTSP): RFC 2326
- ✓ Announcement protocol : An experimental RFC for multicast announcement of session description information and defines an announcement protocol,Session Announcement Protocol (SAP): RFC 2974
- ✓ Session description : SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.Session Description Protocol (SDP): RFC 2327, Other SDP RFCs include RFC 3524
- ✓ Extended RTCP : Defines the Extended Report (XR) packet type for the RTP Control Protocol (RTCP), and defines how the use of XR packets can be signalled by an application if it employs the Session Description Protocol (SDP),RTP Control Protocol Extended Reports (RTCP XR): RFC 3611

Resource Locator:

http://www.itu.int/rec/T-REC-H.323-200606-I/en

http://www.rfc-editor.org/rfc/rfc3661.txt

http://www.rfc-editor.org/rfc/rfc2805.txt

http://www.rfc-editor.org/rfc/rfc5125.txt

http://www.rfc-editor.org/rfc/rfc3015.txt

http://www.rfc-editor.org/rfc/rfc4666.txt

http://www.rfc-editor.org/rfc/rfc3261.txt

http://www.rfc-editor.org/rfc/rfc2205.txt

http://www.rfc-editor.org/rfc/rfc2750.txt

http://www.rfc-editor.org/rfc/rfc3550.txt

http://www.rfc-editor.org/rfc/rfc2326.txt

http://www.rfc-editor.org/rfc/rfc2974.txt

http://www.rfc-editor.org/rfc/rfc2327.txt

http://www.rfc-editor.org/rfc/rfc4666.txt

http://www.rfc-editor.org/rfc/rfc3524.txt

http://www.rfc-editor.org/rfc/rfc3611.txt

6.5.3 Video Conferencing

Description:

Video Conferencing enables two or more locations to interact two –way video and audio transmissions simultaneously through telecommunication technologies. Videoconferencing uses telecommunications of audio and video to bring people at different sites together for a meeting. This can be as simple as a conversation between two people in private offices (point-to-point) or involve several sites (multi-point) with more than one person in large rooms at different sites. Besides the audio and visual transmission of meeting activities, videoconferencing can be used to share documents, computer-displayed information, and whiteboards.

Standard Details:

ITU H .323 versions 5 is used for the assembly of Audio, Video, Data and Control (AVDC).The minimum audio standards required are ITU G.723.1 and G.722. The video standards required are ITU H.261 and H.263. The data standards required are ITU T.120. The control and signaling standards required are ITU T.H.225 and H.245. The call control signaling standards required are ITU T.Q.931 when call control is required. The H.323 standards are important building blocks for a broad new range of collaborative, LAN-based applications for multimedia communications. It includes parts of H.225.0 - RAS, Q.931, H.245 RTP/RTCP and audio/video codec, such as the audio codec (G.711, G.723.1, G.728, etc.) and video codec (H.261, H.263) that compress and decompress media streams.

Resource Locator:

- H.323

  http://www.itu.int/rec/T-REC-H.323-200606-I/en

- G series

  http://www.itu.int/net/itu-t/sigdb/speaudio/Gseries.htm

- G.722

  http://www.itu.int/rec/T-REC-G.722-198811-I/en

- H.261

  http://www.itu.int/rec/T-REC-H.261-199303-I/en

- Q.931

  http://www.itu.int/rec/T-REC-Q.931-199805-I/en

- H.263

  http://www.itu.int/rec/T-REC-H.263-200501-I/en

6.6 Application Design and development

Application standards will include standards and specification pertaining to design & development of Application. The conformance to the standards and their use will ensure longer lifecycle of applications. These standards are not protocols or specification, these standards are typically a Recommendatory approach and guideline to design/procure and implement applications of various types. It is important to have key recommendations in terms of application design and development because:

- Nepal has few legacy applications. New application design and development can be based on latest standards
- There will be tremendous growth in applications in the coming years due to operationalize BPR and moving towards e-Services. These application standards will serve as a guidance to ensure interoperability.

Table 6-16: Application Design & Development

Application Design & Development		
Standards Proposed	**Mandatory / Recommendatory**	**Reference & Links to Application Design & Development Technical Standards Details**
Application Development For Handheld Devices		
• Technologies must be compatible with the standards adopted for mobile operating systems. • There are specialized application development platforms for handheld devices. • Ministries/agencies developing or purchasing new, wireless departmental or enterprise applications that will be accessed primarily via wireless phones and PDAs (blackberry) must utilize these customized application development platforms	Recommendatory	4.6.1 Application Development for Handheld Devices
Application development framework		
• Provide the agencies with distinct approaches to address different application needs/ requirements. • Ministries/agencies should utilize an enterprise framework in the development of applications and services. • Technologies should provide capability for reuse of existing components and services • Technologies should provide support for creating of web services and should be compatible with standards adopted for web services.	Mandatory	4.6.2 Application Development Framework
Business Rules, Logic and Objects		
• There should be Meta data for every document /object • For naming and design rules for schema	Recommendatory	4.6.3 Business Rules, logic and objects

Application Design & Development		
design Universal Business Language (UBL) can be used. • W3C standards and Uniform Resource Name (URN) should be used for namespaces i.e. defining each element type and attribute name in an XML document.		
Commercial, off-the-shelf applications(COTS)		
• The COTS application should comply with open standards, industry standards in a manner that it interoperates with complementary products from other vendors • Availability and access to training and all round support • The application should allow Parameterization and customization for local needs e.g. payroll • Minimum or no locking with proprietary products	Recommendatory	4.6.4 Commercial off the shelf applications
Geographic Information System		
• Technology/ software products that comply with OGC's OpenGIS Specifications and protocol such as include Web Map Service (WMS) and Web Feature Service (WFS). • Describes any information system that integrates, stores, edits, analyzes, shares, and displays geographic information	Recommendatory	4.6.5 Geographic Information System
Modeling design and development		
• The standards (frameworks) adopted for application design and development should be compatible with the technologies used for implementing applications. • Process Modeling should be done using BPMN standards, for workflow • For Notation specifying business process behavior based on Web Services Business Process Execution Language(BPEL4WS) for Web Services • Entity-Relationship diagram (ERD should be the diagramming notation for data modeling for relational data bases. • UML 2.0 and above (Unified modeling language) should be the standard used for requirement specification for application development • XML Schema v1.0 should be used for creating tags to define the structure, content and semantics of XML documents(define, transit, validate, and	Recommendatory	4.6.6 modeling Design & Development

Application Design & Development		
interpret data) • WML v2.0 – Wireless Markup Language version 2.0 should be used for development of content for mobile/pda.		
Programming language for Application Development		
• Scripting languages should allow Code portability, code collaboration, and browser compatibility and should follow ASCII as the basis. • Languages for development of mobile applications should be thus compatible with mobile network standards such as GSM, CDMA, TDMA and packet-switched and data standards such as GPRS, IS95B and 3G). • Technologies used should be compatible with the application development framework adopted as standards. The application would include web application as well. • Various technologies exist to support the basic frameworks and programming languages used for application development that will support or improve the software user's work.	Recommendatory	4.6.7 Programming Language for Application Development
Reporting tools		
• They should be platform independent • They should provision for integrating with Amharic language/provide language support • The reporting tools should support database connectivity, spreadsheet connectivity and access mechanisms accepted as standards. • Version control features and change control features should be available.	Recommendatory	4.6.8 Reporting Tools
Software configurations Management (SCM)		
• The SCM tool should provide for all parts of the software development, deployment and maintenance lifecycle • The technology should enable project set up execution and monitoring features. • It should provide features for collaborative work	Recommendatory	4.6.9 Software Configurations Management
Service Oriented Architecture		
• It is Recommendatory to use w3c standards for web services • UDDI version 3 used for describing,	Mandatory	4.6.10 Service Oriented Architecture

Application Design & Development		
publishing, and discovering network-based software components. • WSDL v 1.1 used for specifying the location of the service and the operations, or methods, the service exposes • SOAPv1.2 and above should be used to for Web Services transport. • ebXML Version 2.0 (now ISO/TS 1500 series) used for Standard Message Service Specification • WSRM 1.1 should be used for message delivery to applications or Web services. • Web Services Business Process Execution Language should be used to describe business process activities as web services and define how they can be connected to accomplish specific tasks. • Basic Profile Version 1.0 (BdAD Final Material) as defined by the Web Services Interoperability Organisation (WS-I) should be used as web services basic interoperatibility profile		
Smart Card Applications		
• The following standards are Recommendatory for smart card applications design and development: - ISO/IEC 7816-4 - ISO/IEC 7816-5 - ISO/IEC 7816-7 - ISO/IEC 7812-2 - ISO/IEC 7813 - EN 1332-1 - EN 1332-4	Recommendatory	4.6.11 Smart Card Applications

6.6.1 *Application for Handheld Devices*

Description:

Application for handheld devices is an application for PDAs etc. similar to the applications on notebooks, desktops and the like. There are specialized application development platforms for handheld devices. Ministries/agencies developing or purchasing new, wireless departmental or enterprise applications that will be accessed primarily via wireless phones and PDAs (blackberry) must utilize these customized application development platforms

Standard Details:

Operating system is the key to wireless application. Technologies must be compatible with the standards adopted for mobile operating systems. For development of application in handheld devices it is Recommendatory to use Wireless Application Protocol (WAP). It is an open standard for application to communicate in wireless network. Similar to a web browser through a computer a WAP browser designed to operate within the restrictions of a mobile phone, such as its smaller view screen. Users can connect to WAP sites: websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser. These standards should also be read along with WML standards/specifications. The WAP specification spans across different functional areas such as Architecture, Client ID, Client Provisioning, External Functional Interface (EFI),General formats, Multimedia Messaging Service (MMS), Persistence, Pictogram, Push, Synchronization, User Agent Profile (UAProf), Wireless Application Environment, Wireless Protocols, Wireless Security and Wireless Telephony Application (WTA).

Resource Locator:

- Application for handheld devices

  http://www.wapforum.org

6.6.2 Application Development Framework

Description:

Application Development framework is the guidelines or model used to develop applications on. It provides the agencies with distinct approaches to address different application needs/ requirements. There are many frameworks for developing application, however the requirements of interoperability has to be address while selecting and implementing such application framework

Standard Details:

- From a standards perspective there are few key requirement that are Recommendatory to follow which will help towards interoperability. As it is tough to name a single platform or framework it is important that application development frameworks should provide the agencies with distinct approaches to address different application needs/ requirements.
- An enterprise framework in the development of applications and services should be preferred and technologies should provide capability for reuse of existing components and services
- Technologies or platform used should also provide support for creating of web services as there might be development of service oriented application at a later stage.
- Technologies should provide capability for reuse of existing components and services and should provide support for creating of web services and should be compatible with standards adopted for web services.

Resource Locator: http://en.wikipedia.org/wiki/Web_application_framework

6.6.3 Business Rules, Logic & Objects

Description:

Business Rules, Logic and Objects standards describe the services and data from an organization point of view, this component defines the standards/requirement that will help in. Mapping the technical components to useful ministry/agency information.

Standard Details:

- There should be Meta data for every document /object. The details of the Meta data are given in the Meta data standards.
- Universal Business Language (UBL) can be used for naming and design rules for schema design. UBL will provide library of XML based standards. UBL was developed by an OASIS Technical Committee with participation from a variety of industry data standards organizations. UBL is designed to reuse of existing business, legal, auditing, and records management practices. It helps to eliminate the redundancy in entering data. UBL version 2.0 is Recommendatory to be used. UBL is owned by OASIS and is currently available to all, with no royalty fees. The UBL library contains markup language with validators, authoring software, parsers and generators.
- W3C standards and Uniform Resource Name (URN) should be used for namespaces i.e. defining each element type and attribute name in an XML document. URNs area part of a larger Internet information architecture, which comprises of, a Uniform Resource Characteristics(URCs), and Uniform Resource Locators (URLs). URNs are used for identification, URCs for including meta-information, and URLs for locating or finding resources

Resource Locator:

- UBL

  http://docs.oasis-open.org/ubl/os-UBL-2.0-update-delta.zip
- URN

  http://tools.ietf.org/html/rfc1737

  http://tools.ietf.org/html/rfc2141

  http://tools.ietf.org/html/rfc3406

  http://www.ietf.org/rfc/rfc4350.txt

6.6.4 Commercial-off- the-shelf applications (COTS)

Description:

Commercial, off-the-shelf (COTS) is a term for software or hardware, that are ready-made and available for sale/license to public. They are often used as alternatives to developing in-house. Many government and business uses COTS, as they may offer significant savings in procurement, Upgrade & maintenance and best practices. However, since COTS software specifications are written by external vendors, government agencies are sometimes reserved to use these products because they fear that future changes to the product will not be under their control

Standard Details:

There are no predefined standards for COTS. The evaluation and selection process for COTS should be done based on Specification and requirements of the organization

6.6.5 Geographic information system

Description:

Geographical Information systems describes any information system that integrates, stores, edits, analyzes, shares, and displays geographic information. Technology/ software products that comply with OGC's OpenGIS Specifications and protocol such as include Web Map Service (WMS) and Web Feature Service (WFS).

Standard Details:

A Web Feature Service allows performing data manipulation operations on a set of geographic features. Data manipulation operations include the ability to get or query features based on spatial and non-spatial constraints, create a new feature, delete a feature and update a feature.

A Web Map Service (WMS) is a standard protocol for serving georeferenced map images over the Internet that are generated by a map server using data from a GIS database. The specification was developed and first published by the Open Geospatial Consortium in 1999. The standard provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images (returned as JPEG, PNG, etc) that can be displayed in a browser application. The interface also supports the ability to specify whether the returned images should be transparent so that layers from multiple servers can be combined or not.

KML

KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look.

KML is complementary to most of the key existing OGC standards including GML (Geography Markup Language), WFS (Web Feature Service) and WMS (Web Map Service). Currently, KML 2.2 utilizes certain geometry elements derived from GML 2.1.2. These elements include point, line string, linear ring, and polygon.

it is used to display geographic data in an Earth browser such as Google Earth, Google Maps, and Google Maps for mobile. KML uses a tag-based structure with nested elements and attributes and is based on the XML standard. These features include placemarks, descriptions, ground overlays, paths, and polygons.

WCS

The OpenGIS® Web Coverage Service Interface Standard (WCS) defines a standard interface and operations that enables interoperable access to geospatial "coverages".The term "grid coverages" typically refers to content such as satellite images, digital aerial photos, digital elevation data, and other phenomena represented by values at each measurement point.

GML

The Geography Markup Language (GML) is an XML grammar for expressing geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet. As with most XML based grammars, there are two parts to the grammar – the schema that describes the document and the instance document that contains the actual data.

Allows users and developers to describe generic geographic data sets that contain points, lines and polygons. However, the developers of GML envision communities working to define community-specific application schemas that are specialized extensions of GML. Using application schemas, users can refer to roads, highways, and bridges instead of points, lines and polygons. If everyone in a community agrees to use the same schemas they can exchange data easily and be sure that a road is still a road when they view it. GML is also an ISO standard (ISO 19136:2007).

GeoXACML

Geospatial eXtensible Access Control Markup Language Encoding Standard (GeoXACML) defines a geospatial extension to the OASIS standard “eXtensible Access Control Markup Language

GeoXACML is a policy language that supports the declaration and enforcement of access rights across jurisdictions and can be used to implement interoperable access control systems for geospatial applications such as Spatial Data Infrastructures. GeoXACML is not designed to be a rights expression language and is therefore not an extension of the OGC GeoDRM Reference Model

Simple Features

Simple Features Interface Standard (SFS) provides a well-defined and common way for applications to store and access feature data in relational or object-relational databases, so that the data can be used to support other applications through a common feature model, data store and information access interface. OpenGIS Simple Features are geospatial features described using vector data elements such as points, lines and polygons.

WPS

Web Processing Service (WPS) Interface Standard provides rules for standardizing how inputs and outputs (requests and responses) for geospatial processing services, such as polygon overlay. The standard also defines how a client can request the execution of a process, and how the output from the process is handled. It defines an interface that facilitates the publishing of geospatial processes and clients’ discovery of and binding to those processes. The data required by the WPS can be delivered across a network or they can be available at the server.

OWS

The OpenGIS® Web Services Common (WS-Common) Interface Standard specifies parameters and data structures that are common to all OGC Web Service (OWS) Standards. The standard normalizes the ways in which operation requests and responses handle such elements as bounding boxes, exception processing, URL requests, URN expressions, and key value encoding. Among its uses, this document serves as a normative reference for other OGC Web Service standards, including the OpenGIS Web Map Service (WMS),Web Feature Service (WFS)and Web Coverage Service (WCS)standards. Rather than continuing to repeat this material in each such standard, each standard will normatively reference parts of this document.

CSW

Catalogue Services Interface Standard (CAT) supports the ability to publish and search collections of descriptive information (metadata) about geospatial data, services and related resources. Providers of resources use catalogues to register metadata that conform to the provider's choice of an information model; such models include descriptions of spatial references and thematic information. Client applications can then search for geospatial data and services in very efficient ways.

Apart from the Open GI standards following requirement are Recommendatory for GIS/LIS (Land information system)

- The technologies selected should not only allow integrating the various spatial and non-spatial datasets, but also should enable online gathering, recording, warehousing, retrieving, disseminating & employing the data.
- The application should be web-based GIS system using technology appropriate for integration and dissemination of map and multi-lingual attribute data
- The data base should be a RDBMS. GIS data can be created using techniques such as satellite imaging, aerial survey, Auto CAD techniques and GTGN (Getty Thesaurus of Geographic Names).

- Geoprocessing techniques are used to convert this data into Raster or Vector data set
- JPEG, TIFF should be the data format for archiving and digitizing records. Land XML, OGIS, are some of the international standards and the data file format should be such that the property records can be opened in any of the commercially available software.
- Even if tools selected have proprietary formats the system should be capable of transalating the proprietary formats in open standards vice versa
- Post geo processing, data is converted in form of visual maps. For mapping it should allow Mouse method. The system should allow Multi-Points method wherein user can connect a number of points plotted already in the order specified by the user. The user should also be able to connect the required points by drawing a line between them, while at the same time placing the user defined dimension as well as the actual dimension of the line drawn.
- The system should also allow the user to connect any two given points with the option to key-in the user defined dimension for the line drawn.
- The system should allow r Readers of standalone applications and linked to server or are embedded as web application to allow user to convert data into visual maps.
- Geocoding techniques such as spotting locations by entering Zip Code and Geolocation techniques such as Internet protocol, HTML, RFID, Embedded software number can be used for entering data into GIS which is further manipulated for map creation.
- GTGN – Getty Thesaurus of Geographic Names can be used to get information pertaining location of several places.

Resource Locator:

- WFS

  http://www.opengeospatial.org/standards/wfs
- WMS

  http://www.opengeospatial.org/standards/wms
- CSW

  http://www.opengeospatial.org/standards/cat
- OWS

  http://www.opengeospatial.org/standards/common
- WPS

  http://www.opengeospatial.org/standards/wps
- Simple Features

  http://www.opengeospatial.org/standards/sfa
- GML

  http://www.opengeospatial.org/standards/geoxacml

  www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32554

- WCS

  http://www.opengeospatial.org/standards/wcs

  http://schemas.opengis.net/wcs/

- KML

  http://www.opengeospatial.org/projects/groups/kml2.2swg

- GeoXACML

  http://www.opengeospatial.org/standards/geoxacml

- Additional reference

  http://www.cadastraltemplate.org/fielddata/d1.htm

6.6.6 Modeling design and development

Description:

Modeling, design and development products are software applications that provide comprehensive facilities to computer programmers for software development, designing and data modeling; typically it has a class browser, an object inspector, and a class hierarchy diagram, for use with software development. Technologies should be compatible with the standards adopted for application development frameworks and technologies for application development

Standard Details:

Process Modeling should use BPMN 1.2 standards, for workflow. The Business Process Management Initiative (BPMI) has developed a standard Business Process Modeling Notation (BPMN). The primary goal of BPMN is to provide annotation that is readily understandable by all business users, from the business analysts that create the initial drafts of the processes, to the technical developers responsible for implementing the technology that will perform those processes, and finally, to the businesspeople who will manage and monitor those processes. Thus, BPMN creates a standardized bridge for the gap between the business process design and process implementation. Another goal, but no less important, is to ensure that XML languages designed for the execution of business processes, such as BPEL4WS (Business Process Execution Language for Web Services), can be visualized with a common notation.

For Notation specifying business process behavior based on Web Services Business Process Execution Language (BPEL4WS 1.1) for Web Services. It is a new language for the modeling of executable business processes. BPML4S follows the Business Process Modeling Language standards and related specifications; hence BPML can be construed as superset of BPEL4WS. BPML and BPEL4WS share an identical set of idioms and similar syntaxes as the basis for convergence. Business Process Execution Language for Web Services (BPEL4WS) provides an XML-based process definition and execution language that enables the description of rich business processes capable of consuming and providing Web services in a reliable and dependable manner. BPEL4WS enables portability and interoperability by defining constructs to implement executable business processes and message exchange protocols, thereby supporting both executable and abstract business processes. The original BPEL4WS 1.0 specification was published in August 2002 by Microsoft, IBM and BEA. In May 2003, Microsoft, IBM, BEA, SAP and Siebel released version 1.1 of the BPEL4WS specification. The BPEL4WS 1.1 specification provides a modular structure, enabling core process modeling concepts to be extended to support both executable models and business protocols. The original BPEL4WS 1.0 specification was published in August 2002 by Microsoft, IBM and BEA.

UML 2.0 and above (Unified modeling language) should be the standard used for requirement specification for application development. It can not only be limited to application structure, behavior, and architecture, but also business process and data structure. The UNL specification can help in defining a graphical language for visualizing, specifying, constructing, and documenting the artifacts of distributed object systems. Entity-Relationship diagram (ERD should be the diagramming notation for data modeling for relational databases. Detailed specification can be accessed through the url provided in the resource locator

XML Schema v1.0 should be used for creating tags to define the structure, content and semantics of XML documents (define, transit, validate, and interpret data).

WML v2.0 – Wireless Markup Language version 2.0. Should be used for development of content for in mobile/pda's Wireless Application Protocol (WAP) is an industry-wide specification for developing applications that operate over wireless communication networks. The scope for the WAP Forum is to define a set of specifications to be used by service application. WAP defines a set of protocols in transport, session, and application layers. WML2 is used for backwards compatibility only. It is not intended for content authoring. WAP2 content is created with XHTML Mobile Profile [XHTMLMP].

Resource Locator:

- BPMN

  http://www.bpmn.org/

  http://www.bpmi.org/

- BPML

  http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-bpel/ws-bpel.pdf

- UML

  www.UML..org

  http://www.omg.org/technology/documents/modeling_spec_catalog.htm#UML

- XMLv1.0

  http://www.w3.org/TR/2002/WD-xml11-20020425/

  http://www.osoa.org/xmlns/sca/1.0/sca-core.xsd

- WML

  http://www.openmobilealliance.org/tech/affiliates/wap/wap-238-wml-20010911-a.pdf

6.6.7 Programming language for application development

Description:

Programming languages can be used to create programs that control the behavior of a machine, to express algorithms precisely, or as a mode of human communication. Various programming languages exist for application development. they should be compatible with the standards adopted for application development frameworks, web services and technologies for application development. IEEE Computer, 2008, in praise of scripting, Ronald Loui author defines A scripting language as 'a script language or extension language is a programming language that allows control of one or more software applications. "Scripts" are distinct from the core code of the application, which is usually written in a different language, and are often created or at least modified by the end-user'

Standard Details:

- Scripting languages should allow Code portability, code collaboration, and browser compatibility and should follow ASCII as the basis.
- Languages for development of mobile applications should be thus compatible with mobile network standards such as GSM, CDMA, TDMA and packet-switched and data standards such as GPRS, IS95B and 3G).

6.6.8 Reporting tools

Description:

Reporting tools are necessary to write reports to a screen or to a printer or into files such as RTF, ODT, CSV and XML Files. A good reporting tool will have

- Flexibility in support for integrating data from various Databases, web services, flat files, objects etc.
- good data transformation techniques
- support business- logic to convert raw data into information useful for the use
- Good presentation mechanism such as charts, graphs, query, text etc.

Standard Details:

The reporting tools should support database connectivity, spreadsheet connectivity and access mechanisms accepted as standards. They should provide Open Data Access (ODA) framework so that anyone can build new UI and runtime support for any kind of tabular data

Version control features and change control features should be available.

They should be platform independent and should provision for integrating with Amharic language/provide language support.

6.6.9 Software Configurations Management (SCM)

Description:

Software configuration management (SCM) is a set of activities that are designed to control change by identifying the work products that are likely to change, establishing relationships among them, defining mechanisms for managing different versions of these work products, controlling changes that are imposed, and auditing and reporting on the changes that are made. Version Management (a subset of, Code management are essential).

Standard Details:

Software Configuration Management is applicable to all aspects of software development from design to delivery. When an application is developed change happens and it is essential to focus on control of that change. The SCM tool should provide for all parts of the software development, deployment and maintenance lifecycle. The technology should enable project set up execution and monitoring features. It should provide features for collaborative work.

Resource Locator: http://en.wikipedia.org/wiki/Software_configuration_management

6.6.10 Service Oriented Architecture

Description:

There are many definitions to SOA. A Simple definition and explanation according to Barry & Associates, Inc is 'A service-oriented architecture is essentially a collection of services'. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed. Service-oriented architectures are not a new thing. The first service-oriented architecture for many people in the past was with the use DCOM or Object Request Brokers (ORBs) based on the CORBA specification. Web services is the technology that helps in connecting technology of service-oriented architectures. A Web service is defined by the W3C as "a software system designed to support interoperable machine-to-machine interaction over a network. Web services span multiple across multiple technical standards are components in NeGIF technical areas. It is critical that agencies using web services agree on the implementation and semantics of data. The emergence of the WS-I Basic Profile 1.2 could be a starting point as many governments are implementing web services using the same.

Web services essentially use XML to create a robust connection. A service is the endpoint of a connection. Also, a service has some type of underlying computer system that supports the connection offered. The combination of all services of an organization makes up a service-oriented architecture.

Standard Details:

It is Recommendatory to use W3C standards for web services. Discovery and Integration (UDDI version 3) should be the open standard for describing, publishing, and discovering network-based software components. UDDI defines a universal method for enterprises to dynamically discover and invoke Web services.

Web Services Description Language Version l1.1 and above (WSDL) should be the standard to specify the location of the service and the operations, or methods, the service exposes. WSDL addresses this need by defining an XML grammar for describing network services as collections of communication endpoints capable of exchanging messages. WSDL service definitions provide documentation for distributed systems and serve as a recipe for automating the details involved in applications communication.

A WSDL document defines services as collections of network endpoints, or ports. In WSDL, the abstract definition of endpoints and messages is separated from their concrete network deployment or data format bindings. This allows the reuse of abstract definitions: messages, which are abstract descriptions of the data being exchanged, and port types which are abstract collections of operations. The concrete protocol and data format specifications for a particular port type constitute a reusable binding. A port is defined by associating a network address with a reusable binding, and a collection of ports define a service. Hence, a WSDL document uses the following elements in the definition of network services:

- **Types**– a container for data type definitions using some type system (such as XSD).
- **Message**– an abstract, typed definition of the data being communicated.
- **Operation**– an abstract description of an action supported by the service.
- **Port Type**–an abstract set of operations supported by one or more endpoints.
- **Binding**– a concrete protocol and data format specification for a particular port type.
- **Port**– a single endpoint defined as a combination of a binding and a network address.
- **Service**– a collection of related endpoints.

Simple Object Access Protocol Version 1.2 (SOAP) and above should be used to for Web Services transport. It is intended for exchanging structured information in a decentralized, distributed environment. uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.

Standard Message Service Specification should be ebXML Version 2.0 (now ISO/TS 1500 series). ebXML (Electronic Business using extensible Markup Language), is a modular suite of specifications that enables organisation of any size and in any geographical location to have transaction over the Internet. Using ebXML, organisation now have a standard method to exchange business messages, conduct trading relationships, communicate data in common terms and define and register business processes. It has XML standards for:

- Business processes
- Core data components
- Collaboration protocol agreements
- Messaging
- Registries and repositories

Web Services Reliable Messaging (WSRM) 1.1 should be used for message delivery to applications or Web services. WSDl helps to create a generic and open model for ensuring reliable message delivery for Web services. WS-ReliableMessaging is a building block that is used in conjunction with other specifications and application-specific protocols to accommodate a wide variety of requirements and scenarios related to the operation of distributed Web services. Technically this specification describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. The protocol is described in this specification in a transport-independent manner allowing it to be implemented using different network technologies. To support interoperable Web services, a SOAP binding is defined within this specification.

The protocol defined in this specification depends upon other Web services specifications for the identification of service endpoint addresses and policies. How these are identified and retrieved are detailed within those specifications and are out of scope for this document.

Web Services Business Process Execution Language should be used describe business process activities as web services and define how they can be connected to accomplish specific tasks. Framework for Web Services Implementation.

Resource Locator:

- Web Service standards and specification

  www.W3c.org

- UDDI

  http://www.oasis-open.org/specs/index.php#uddiv3.0.2

- WSDL

  http://www.w3.org/TR/2001/NOTE-wsdl-20010315#_introduction

- SOAP

  http://www.w3.org/TR/soap12-part1/

- ebXML

  www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf

  http://www.ebxml.org/geninfo.htm

- WSRM

  http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.1-spec-os-01-e1.pdf

  http://docs.oasis-open.org/ws-rx/wsrm/200608/wsrm-1.1-spec-cd-04.html

6.6.11 Smart Card

Description

Smart card standards govern physical properties, communication characteristics, and application identifiers of the embedded chip and data. Application-specific properties are being debated with many large organizations and groups proposing their standards. Interoperability can be ensured by conformance to international standards at several levels: 1). to the card itself, 2). the card's access terminals (readers). 3). The networks and 4). The card issuers' own systems.

Standard Details

I. ISO 7816 is the international standard for integrated-circuit cards (commonly known as smart cards) that use electrical contacts on the card, as well as cards that communicate with readers and terminals without contacts, as with radio frequency (RF/Contactless) technology. The following clauses of ISO 7816 are Recommendatory for design and development of smart card applications

- **ISO/IEC 7816-4**

  This specifies an Inter-industry Commands for Interchange; establishes a set of commands for CPU cards across all industries to provide access, security and transmission of card data. Within this basic kernel, for example, are commands to read, write and update records.

- **ISO/IEC 7816-5**

  This specifies a Numbering System and Registration Procedure for Application Identifiers (AID); sets standards for Application Identifiers. An AID has two parts. The first is a Registered Application Provider Identifier (RID) of five bytes that is unique to the vendor. The second part is a variable length field of up to 11 bytes that RIDs can use to identify specific applications.

- **ISO/IEC 7816-7**

  Inter-industry command for Structured Card Query Language (SCQL); This document specifies the concept of a SCQL database (SCQL = Structured Card Query Language based on SQL, see MS ISO 9075), and the related inter-industry enhanced commands

- **ISO/IEC 7812-1 and 2**

  ISO 7812-2 is one of a series of International Standards describing the parameters for identification cards, and the use of such cards for international and/or inter-industry interchange. It describes the application and registration procedures for numbers issued in accordance with ISO/IEC 7812-1. ISO/IEC 7812-1 specifies the numbering system for the identification of issuers of identification cards used in international and/or inter-industry interchange.

- **ISO/IEC 7813**

This is a standard that defines properties of financial transaction cards, eg ATM or credit cards. The standard defines:

- physical characteristics, eg size, shape, location of magnetic stripe etc
- magnetic track data structures .

- **EN 1332-1**

  Provides standards for Identification card systems - Man-machine interface –and Dimensions and location of a tactile identifier for ID-1 cards

- **EN 1332-4**

  Provides standards for Identification card systems - Man-machine interface and Coding of user requirements for people with special needs

Resource Locator:

- Overall

  http://www.tiresias.org/research/standards/smartcards.htm#international

- ISO 7816

  http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

- ISO 7812

  ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system

  ISO/IEC 7812-2:2007 Identification cards -- Identification of issuers -- Part 2: Application and registration procedures

- ISO 7813

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317

- EN 1332

  http://www.tiresias.org/research/standards/smartcards.htm#international

6.7 Application Integration

Development and deployment of e-Services will require multiple applications to be composed to provide services. Composing applications requires Application integration. Application integration may also use services running on a legacy system through a thin-client browser or a service that enables the execution of multiple application functions from an integrated user interface. The methods used to achieve this integration include web services, message oriented middleware, remote procedure calls and object request brokers.

Table 6-17: Application Integration

Application Integration		
Standards Proposed	Mandatory/Recommendatory	Reference & Links to Application Integration Technical Standards Details
Message oriented Middleware		
• JMS and MSMQ may be used for application integration based on the platforms deployed.	Recommendatory	4.7.1 Message Oriented Middleware
Object request brokers		
• CORBA or COM /DCOM should be used as ORB • Web applications should use Resource Discover Framework standards	Recommendatory	4.7.2 Object request Brokers
Remote procedure calls		
• Any RPC used for non web based application should be developed using interface description language (IDL) • For all web enabled application XML-RPC should be used.	Recommendatory	4.7.3Remote Procedure calls

6.7.1 Message Oriented Middleware

Description:

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for Message Oriented Middleware designed to support reliable, high-performance messaging over the Internet. Its features are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security. It used for any distributed or business application, and supports common messaging paradigms like point-to-point, fan out, publish-subscribe, and request-response.

Standard Details:

AMQP mandates the behavior of the messaging provider and client to the extent that implementations from different vendors are truly interoperable. Any tool that can create and interpret messages that conform to this data format can interoperate with any other compliant tool irrespective of implementation language.

Resource Locator:

- Message oriented Middle ware (AMQP)

  http://jira.amqp.org/confluence/display/AMQP/AMQP+Specification

6.7.2 Objects Request Brokers

Description:

Object Request Broker (ORB) is a piece of middleware software that allows programmers to make program calls from one computer to another via a network. ORBs promote interoperability of distributed object systems because they enable users to build systems by piecing together objects- from different vendors- that communicate with each other via the ORB.

Standard Details:

ORBs handle the transformation of in-process data structures to and from the byte sequence, which is transmitted over the network. This is called marshalling or serialization. CORBA specification. ORBs often expose many more features, such as distributed transactions, directory services or real-time scheduling. In object-oriented languages, the ORB takes the form of an object with methods enabling connection to the objects being served. After an object connects to the ORB, the methods of that object become accessible for remote invocations. The ORB requires some means of obtaining the network address of the object that has now become remote.

Resource Locator:

- ORB

  http://www.service-architecture.com/web-services/articles/corba.html

  http://www.omg.org/gettingstarted/orb_basics.htm

  http://www.omg.org/technology/documents/formal/corba_2.htm

6.7.3 Remote Procedure Calls

Description:

Remote Procedure Call (RPC) is an Inter-process communication technology that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction. In simple terms is a simple extension to the procedure call in computers to create connections between procedures that are running in different applications, or on different machines.

Conceptually, there's no difference between a local procedure call and a remote one, but they are implemented differently, perform differently (RPC is much slower) and therefore are used for different things. When the software in question is written using object-oriented principles, RPC may be referred to as remote invocation or remote method invocation.

Standard Details:

An RPC is initiated by the client sending a request message to a known remote server in order to execute a specified procedure using supplied parameters. An important difference between remote procedure calls and local calls is that remote calls can fail because of unpredictable network problems. Also, callers generally must deal with such failures without knowing whether the remote procedure was actually invoked. Idempotent procedures (those which have no additional effects if called more than once) are easily handled, but enough difficulties remain that code which calls remote procedures is often confined to carefully written low-level subsystems. Even web services use RPC style however SOA is most common. There are several methods to there are several formats for marshalling the remote calls. The emerging standard especially for web applications is XML-RPC. XML will be useful to implement it. XML-RPC uses XML as the marshalling format. It allows to easily make procedure calls to software running on platform say windows and BeOS machines to other platform e.g. Linux/Mac. It can also work on PDAs. With XML it's easy to see what it's doing, and it's also relatively easy to marshal the internal procedure call format into a remote format. Whatever may be the format RPC is important as it allows choices to replace a component with another one, it offers possibilities to developers to develop solutions with packaged software that the developers didn't anticipate.

Resource Locator:

- RPC

  http://ietf.org/rfc/rfc5531.txt

- XML-RPC

  http://www.xmlrpc.com/spec

6.8 System Standards

This will include standards pertaining to system software and hardware such as server O/S.

Table 6-18: System Standards

System Standards		
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Systems Technical Standards Details**
Application Servers		
• Application servers should provide support for various standards adopted for web services • Application servers should be compatible with data connectivity and access technologies, application development frameworks and database management systems	Mandatory	6.8.1 Application Servers
Backup Recovery		
• Technologies should be compatible with standards adopted for categories such as operating systems, database management systems and storage. • Production databases shall be periodically tested for recoverability.	Mandatory	6.8.2 Backup Recovery

System Standards		
• Metadata (database schemas, structures, data definitions, etc.) shall be backed up along with the data.		
Business Intelligence		
• Technologies should support database connectivity and access technologies accepted as standards. • Technologies should provide support Graphical Interfaces for summarizing data, e.g. desktop dashboards. • Technologies should provide support for ad-hoc and “canned” queries. • Technologies should provide support for guided report creation as well as programmatic control of report creation.	Recommendatory	6.8.3 Business Intelligence
DB Connectivity and access technology		
• Frameworks and models used for database connectivity and access purposes should be based on the standards of the database environment identified.	Mandatory	6.8.4 DB Connectivity and access Technology
DBMS		
• Database Management system should provide support for the basic properties of a database transaction: (ACID) Atomicity, Consistency, Isolation, and Durability • Database Management System should provide for security of the data and built-in audit capabilities • Database technologies shall support industry or de facto standards for database connectivity mechanisms such as Java Database Connectivity (JDBC), Open Database Connectivity (ODBC) or Object Linking and Embedding Database (OLEDB) • Database Management System should be XML enabled and must provide capability for web service standards. • The version/release levels of all database management systems and related tools used to develop or support ministry/agency “mission critical applications” shall have	Mandatory	6.8.5 DBMS

System Standards		
vendor or equivalent level support. • Ministries should preferably have database for transactional and analytical processing in separated DBMS source • Database cluster, the clustering software should support heterogeneous Operating systems from different OEM's. • The Volume Manager and File system should support heterogeneous Storage models from different OEMs.		
Desktop O/S		
• Desktop operating system should provide graphical user interface and should be compatible with the hardware platform.	Mandatory	6.8.6 Desktop O/S
Hardware Platforms		
• Ministries/agencies should consider deploying 64 bit hardware platforms • X86 instruction set architecture should be used. X86-32 for the 32 bit hardware platforms, and x86-64 for the 64 bit hardware platforms.	Mandatory	6.8.7 Hardware Platforms
IT Operations Management		
• Technologies should be compatible with standards adopted for categories such as operating systems, database management systems, and storage application servers. • The systems should be compatible with Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).	Mandatory	6.8.8 IT Operations Management
Mobile O/S		
• Mobile operating system should provide for graphical user interface. • Mobile operating systems should provide support for the adopted standards for application development frameworks for handheld devices.	Recommendatory	6.8.9 Mobile O/S
Portal servers		
• Portal servers must adhere to Organization for the Advancement of Structured Information Standards	Mandatory	6.8.10 Portal Servers

System Standards		
(OASIS) Web Services for Remote Portlets (WSRP) specifications.		
Server O/S		
• Operating system should be providing graphical user interface, should be compatible with the hardware platform and should upgrade based on requirements and support. • POSIX standards for O/S should be applicable • Operating system should be based on the requirement of the application or system to function • Server O/S should minimize server operating system configuration variations as this helps to reduce risks and support and maintenance costs • Server O/S should configure all servers supporting mission critical applications, including desktop applications, to minimize service interruption.	Mandatory	6.8.11 Server O/S
Storage Devices		
• Storage hardware used should adhere to the storage interface available/adopted • Local Redundant Array of Independent Disks (RAID)/ Storage Area Network (SAN)/ Network-attached storage (NAS) should be used as the system storage technology. • Optical disks and tapes are also a suitable choice from the available latest technology and this can be considered.	Mandatory	6.8.12 Storage Devices
Web Server		
• A web server provides World Wide Web services on the Internet. If a web server is used internally and not by the public it may be known as an "intranet server." • It is responsible for accepting HTTP requests from clients and serving them HTTP responses along with optional data content.	Mandatory	6.8.13 Web Server
Keyboard layout		

System Standards		
• The United States keyboard layout is used as default in the currently most popular operating systems: Windows, Mac OS X and Linux. • The most wide spread & common modern day keyboard layout for Latin scripts is QWERTY • Devanagari is the main script used to write Hindi & Nepali (non-Latin scripts). INSCRIPT (Indian Script) is the standard keyboard layout for Devanagari. An InScript keyboard is inbuilt in most modern operating systems including Windows, Linux and Mac OS.	Recommendatory	6.8.14 Keyboard Layout

6.8.1 Application Servers

Description:

An application server is a server program in a computer in a distributed network that provides the business logic for an application program. The application server makes it possible for a server to generate a dynamic, customized response to a client request.

Application would be required as middle tier for various web based applications. Application server would take care of the necessary workflow and web server would be required for the interfacing with the end user. Both the web and application server would be seamlessly integrated to provide high availability and performance.

Standard Details:

In an n-tier environment, a separate component performs the business logic, although some part may still be handled by the user's machine is referred as Application Server, it serves an Application Programming Interface (API) to expose business logic and business processes for use by third-party applications. Application servers should provide support for various standards adopted for web services. Application servers should be compatible with data connectivity and access technologies, application development frameworks and database management systems. There are open standards such as Soapad which provides open-source, open standards for application server. However an eGIF standard does not provide the choice of application server.

Resource Locator:

6.8.2 Backup Recovery

Description:

Backup refer to making copies of data so that these additional copies may be used to restore the original after a data loss event. These additional copies are typically called backups. Backups are useful primarily for recovering the lost data when some kind of disaster happens.

Backup server would be used for backing up the data at regular interval. The backing up of the data would be an automated process. Whenever desired the backed up data can be restored/retrieved to the desired system configuration.

Standard Details:

Data backup and recovery defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state. The key requirements are

- Technologies should be compatible with standards adopted for categories such as operating systems, database management systems and storage.
- Production databases shall be periodically tested for recoverability.
- Metadata (database schemas, structures, data definitions, etc.) shall be backed up along with the data.
- However apart from ensuring the requirement mentioned in the table it is important to concentrate on the process of maintenance of database, routine of back up and recovery and the health of the data. .It is not just the data files that need to be part of the backup process backup of transaction log can also be done.

6.8.3 Business Intelligence

Description:

BI is a broad category of applications and technologies for gathering, storing, analyzing, and providing access to data to help enterprise users make better business decisions. It refers to tool, technologies and frameworks that are used to help an organization to have a better understanding of its performance. It is a culmination of information. BI applications include the activities of decision support systems, query and reporting, online analytical processing (OLAP), statistical analysis, forecasting, and data mining.

Standard Details:

BI technologies provide past, present, and future prediction on the operations. It often aims to support better business decision-making. Thus a BI system can be called a decision support system (DSS). Technologies should support database connectivity and access technologies accepted as standards. Technologies should provide support Graphical Interfaces for summarizing data. Technologies should provide support for ad-hoc and "canned" queries. Technologies should provide support for guided report creation as well as programmatic control of report creation. Any tools which supports Online analytical processing (OLAP) should support Multidimensional OLAP(MOLAP), Hybrid OLAP (HOLAP) and Relational OLAP (ROLAP) depending on the nature of reporting system that needs to be developed.

Key Features of a good Business Intelligence Architecture are:

- **Simple Integration and Deployment**

  This will enable Industry standard enterprise business intelligence architecture, ensuring interoperability and compatibility with your existing platforms and systems.

- **High Performance and Scalable**

  This will ensure consistent high performance in an easy, integrated business intelligence platform for all users Scalable, load balancing to support elevated data volumes and applications, increasing user base and user needs.

- **Secure and Centralized Administration**

Easy, centralized, browser-based administration helps manage the metadata layer, data access, security, and user group administration. Fully integrated security model. Security Support with authentication, access control and system logs.

- **Minimum Training**

  Robust, flexible with integrated enterprise reporting, analysis and query eliminate the need to learn multiple products Less training requirements resulting in better user take up and participation across all levels in the organization.

6.8.4 DB Connectivity and Access technologies

Description:

Database connectivity and access technologies are concerned with providing for technologies to connect to and access the data stored in databases. The client communicates to database server irrespective of being on the same server or different server. Frameworks and models used for database connectivity and access purposes should be based on the standards of the database environment identified.

Standard Details:

- Open Data Base Connectivity (ODBC) is based on Call-Level Interface and was defined by the SQL Access Group. Open Database Connectivity (ODBC) provides a standard software API method for using database management systems (DBMS). The designers of ODBC aimed to make it independent of programming languages, database systems, and operating systems.
- Object Linking and Embedding, Database (OLE-DB) is an open specification designed to build on the success of ODBC by providing an open standard for accessing different types of data stored in a uniform manner
- Extensible Markup Language (XML) is a set of rules for encoding documents electronically.
- Hibernate is an object-relational mapping (ORM) library for the Java language, providing a framework for mapping an object-oriented domain model to a traditional relational database.

Some platform specific standards are:

- Java Database Connectivity (JDBC) is a standard SQL database access interface. JDBC is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database. JDBC is oriented towards relational databases.
- ADO.NET is a set of computer software components that can be used by programmers to access data and data services. It is a part of the base class library that is included with the Microsoft .NET Framework.
- Microsoft's ActiveX Data Objects (ADO) is a set of Component Object Model (COM) objects for accessing data sources. A part of MDAC, it provides a layer between programming languages and OLE DB.

6.8.5 DBMS

Description:

A database is an integrated collection of logically related records or files which consolidates records into a common pool of data records that provides data for many applications. Relational Database Management Systems should; be used for hosting the databases.

The database/repository provides all the relevant information required to process any Citizen/Government request or to render any e-Governance services. Database servers would be required to store and access data with ease. This would also be integrated with multiple applications, residing with department. Database servers should be configured in highly available mode.

Standard Details:

- Database Management system should provide support for the basic properties of a database transaction: (ACID) Atomicity, Consistency, Isolation, and Durability
- Database Management System should provide for security of the data and built-in audit capabilities
- Database technologies shall support industry or de facto standards for database connectivity mechanisms such as Java Database Connectivity (JDBC), Open Database Connectivity (ODBC) or Object Linking and Embedding Database (OLEDB)
- Database Management System should be XML enabled and must provide capability for web service standards.
- The version/release levels of all database management systems and related tools used to develop or support ministry/agency "mission critical applications" shall have vendor or equivalent level support.
- Ministries should preferably have database for transactional and analytical processing in separated DBMS source

Resource Locator:

- DBMS

  http://www.ansi.org

  http://www.iso.org

6.8.6 Desktop Operating System

Description:

An operating system (O/S) is an interface between hardware and user. An OS is responsible for the management and coordination of activities and the sharing of the resources of the computer. Operating system should be providing graphical user interface and should be compatible with the hardware platform. An OS running on a PC is called a desktop operating system. A computer being secure depends on a number of technologies working properly. A modern operating system provides access to a number of resources, which are available to software running on the system, and to external devices like networks via the kernel. Most operating systems support a variety of networking protocols, hardware, and applications for using them. This means that computers running dissimilar operating systems can participate in a common network for sharing resources such as computing, files, printers, and scanners using either wired or wireless connections. Networks can essentially allow a computer's operating system to access the resources of a remote computer to support the same functions as it could if those resources were connected directly to the local computer

Standard Details:

Desktop operating system should be provide graphical user interface and should be compatible with the hardware platform.

6.8.7 Hardware Platforms

Description:

Hardware Platform (computer architecture) is the conceptual design and fundamental operational structure of a computer system. It is a blueprint and functional description of requirements and design implementations for the various parts of a computer, focusing largely on the way by which the central processing unit (CPU) performs internally and accesses addresses in memory. Instruction set, a primary category of hardware platform is a list of all the instructions, and all their variations, that a processor (or in the case of a virtual machine, an interpreter) can execute.

Standard Details:

Each hardware platform, or CPU family, has a unique machine language. All software presented to the computer for execution must be in the binary coded machine language of that CPU.64 bit hardware platforms are strategic for future deployment by ministries/agencies.x86 is the most commercially successful instruction set architecture in the history of personal computing. x86-32 is the architecture for the 32 bit hardware platforms, where the x86-64 for the 64 bit hardware platforms.

Resource Locator:

6.8.8 IT Operations Management

Description:

Operations management refers to enterprise-wide administration of the operations of distributed computer systems. It includes management of software inventory and installation, performance management, availability and fault management, asset management and configuration management and helpdesk management. Its main objective is to monitor and control the IT services and IT infrastructure. The process IT Operations Management executes day-to-day routine tasks related to the operation of infrastructure components and applications. This includes job scheduling, backup and restore activities, print and output management, and routine maintenance.

Standard Details:

IT Operations Management is part of ICT Infrastructure Management in ITIL V2, where some operational aspects are described in more detail as in the new ITIL V3 books. Interfaces between IT Operations Management and the other ITIL processes were adjusted in order to reflect the new ITIL V3 process structure.

Resource Locator:

- IT operations management

  http://www.itil-officialsite.com/home/home.asp

6.8.9 Mobile Operating System

Description:

An operating system for mobile devices, is the software platform on top of which other programs, called application programs, can run on mobile devices such as mobile phones, Smartphone's, PDAs, and handheld computers. It controls a mobile device—similar to desktop operating system. Mobile operating system should provide for graphical user interface. Mobile operating systems should provide support for the adopted standards for application development frameworks for handheld devices. Mobile OS are simpler, and deal more with the wireless versions of broadband and local connectivity, mobile multimedia formats, and different input methods.

Standard Details:

- Operating systems should deal with deal more with the wireless versions of broadband and local connectivity, mobile multimedia formats, and different input methods.
- Mobile operating system should provide for graphical user interface.
- Mobile operating systems should provide support for the adopted standards for application development frameworks for handheld devices.

Resource Locator:

6.8.10 Portal Servers

Description:

Portals are applications to can manage content and information. They provide a one point entry for all users. A portal page is displayed as a collection of non-overlapping portlet windows, where each portlet window displays a portlet. Hence a portlet (or collection of portlets) resembles a web-based application that is hosted in a portal. Some examples of portlet applications are email, weather reports, discussion forums, and news.

Standard Details:

Portal servers must adhere to Organization for the Advancement of Structured Information Standards (OASIS) Web Services for Remote Portlets (WSRP) specifications.

Resource Locator:

- Organization for the Advancement of Structured Information Standards (OASIS)

  http://www.oasis-open.org

6.8.11 Server Operating System

Description:

An operating system (O/S) is an interface between hardware and user. An OS is responsible for the management and coordination of activities and the sharing of the resources of the computer. Operating system should be providing graphical user interface and should be compatible with the hardware platform.

Standard Details:

- POSIX standards for O/S should be applicable.
- Operating system should be based on the requirement of the application or system to function. Operating system should upgrade based on requirements and support. Example: Operating system

should take into account the upgrade requirements and support (especially if it is proprietary) as we have observed in the Baseline some of the ministries still use Windows NT.

- Server O/S should minimize server operating system configuration variations as this helps to reduce risks and support and maintenance costs
- Server O/S should configure all servers supporting mission critical applications, including desktop applications, to minimize service interruption

Resource Locator:

- POSIX, IEEE Standards Association

  http://standards.ieee.org/regauth/posix

6.8.12Storage Devices

Description:

Storage devices are designed to provide information to direct attached servers or provide non-volatile digital storage media to support information processing in a local and a network environment. These devices provide extended storage capabilities to the network with reduced costs compared to traditional file servers. A storage device may hold information, process information, or both. A device that only holds information is a recording medium. Devices that process information (data storage equipment) may either access a separate portable (removable) recording medium or a permanent component to store or retrieve information. Backup software should support policy based backup for full, Incremental and differential backup.

Backup software shall support free pool concepts so that media can be picked from the free pool in case of non-availability of media in the designated pools.

Standard Details:

There are different categories to storage devices such as primary, secondary and tertiary storage. A primary storage (memory) is the only one directly accessible to the CPU. A secondary or tertiary storage may connect to a computer utilizing computer networks. This concept does not pertain to the primary storage, which is shared between multiple processors in a much lesser degree. The following are some standards in this area:

- RAID (Redundant Array of Independent Disks) is used as an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. The different schemes/architectures are named by the word RAID followed by a number, as in RAID 0, RAID 1, etc. RAID's various designs involve two key design goals: increased data reliability or increased input/output performance.
- A Storage Area Network (SAN) is a storage model typically characterized by a use of switching and transmission facilities that are separate from the local area network where the server of data to be stored and retrieved resides. The network communications for a SAN may include fibre channel, iSCSI, Ethernet or other technologies. The SAN also includes the storage management, storage device and storage access technologies.
- Network-attached storage (NAS) systems are generally computing-storage devices that can be accessed over a computer network (usually TCP/IP), rather than directly being connected to the computer (via a computer bus such as SCSI). The protocol used with NAS is a file based protocol such as NFS or Microsoft's Common Internet File System (CIFS).

- Optical Disks and Tapes Technologies such as CD, DVD,SDLT,LTP,DLT, magnetic tapes are also used for backups and storage . there are ISO standard such as ISO 9660 etc for CDs DVDs
- There are many storage interface technologies and standards such as fibre Channel – FC, FICON, FCIP, iSCSI, 10GigE, SCSI, PCI Express, SAS, USB SATA etc that should be compatible with the storage devices.(i.e. storage device should adhere to such standards.)

Resource Locator: http://en.wikipedia.org/wiki/Data_storage_device

6.8.13Web Server

Description:

A web server provides World Wide Web services on the Internet. If a web server is used internally and not by the public it may be known as an "intranet server." Web server is responsible for accepting HTTP requests from clients (user agents such as web browsers), and serving them HTTP responses along with optional data contents, which usually are web pages such as HTML documents and linked objects (images, etc.).

Web based applications are easily accessible from any sort of the network, Intranet, internet or extranet. Most of the new application are having web interface, which requires web servers for such services. The web servers would also be used for web hosting for different department. The things that need to be ensured that the entire windows platform based server(s) which would be access through Internet shall have proper license of the component.

Standard Details:

A web server can be either implemented into the OS kernel, or in user space (like other regular applications). Web servers that run in user-mode have to ask the system the permission to use more memory or more CPU resources. Not only do these requests to the kernel take time, but they are not always satisfied because the system reserves resources for its own usage and has the responsibility to share hardware resources with all the other running applications.

A web server (program) has defined load limits, because it can handle only a limited number of concurrent client connections (usually between 2 and 80,000, by default between 500 and 1,000) per IP address (and TCP port) and it can serve only a certain maximum number of requests per second depending on its own settings; HTTP request type; content origin, caching and the hardware/software limits of the OS where it is working.

When a web server is near to or over its limits, it becomes overloaded and thus unresponsive.

Resource Locator:

- Web Server

  http://www.ietf.org

6.8.14Keyboard Layout

Description:

A keyboard layout is any specific mechanical, visual, or functional arrangement of the keys, legends, or key–meaning associations (respectively) of a computer.

1. Mechanical layout - The placements and keys of a keyboard

2. Visual layout - The arrangement of the legends (labels, markings, engravings) that appear on the keys of a keyboard
3. Functional layout - The arrangement of the key–meaning associations, determined in software, of all the keys of a keyboard

Today, most keyboards use one of three different mechanical layouts, usually referred to as simply ISO, ANSI, and JIS, referring roughly to the organizations issuing the relevant worldwide, United States, and Japanese standards, respectively. Keyboard layout in this sense may refer either to this broad categorization or to finer distinctions within these categories.

Mechanical layouts only address tangible differences among keyboards. When a key is pressed, a keyboard sends a message such as the left-most main key of the home row is depressed, not A. (Technically, each key has an internal reference number, "raw keycodes", and these numbers are what is sent to the computer when a key is pressed or released.) The keyboard and the computer each have no information about what is marked on that key, and it could equally well be the letter A or the digit 9. In fact, it is up to the user of the computer to identify the visual layout of the keyboard, a question usually presented when installing the operating system.

Visual layouts vary by language, country, and user preference, and the same mechanical layout can be produced with a number of different visual layouts. For example, the "ISO" keyboard layout is used throughout Europe, but typical French, German, and U.K. variants of mechanically-identical keyboards appear different because they bear different legends on their keys. Even blank keyboards—with no legends—are sometimes used to learn typing skills or by user preference.

Usually the functional layout is set to match the visual layout of the keyboard being used, so that pressing a key will produce the expected result, corresponding to the legends on the keyboard. However, most operating systems have software that allows the user to easily switch between functional layouts, such as the language bar in Microsoft Windows. Functional layouts can be redefined or customized within the operating system, by reconfiguring operating system keyboard driver, or with a use of a separate software application. Transliteration is one example of that whereby letters in other language get matched to visible Latin letters on the keyboard by the way they sound.

Standard Details:

The United States keyboard layout is used as default in the currently most popular operating systems: Windows, Mac OS X and Linux.

The most wide spread & common modern day keyboard layout for Latin scripts is QWERTY

Devanagari is the main script used to write Hindi & Nepali (non-Latin scripts)**.** INSCRIPT (Indian Script) is the standard keyboard layout for Devanagari. An InScript keyboard layout is inbuilt in most modern operating systems including Windows, Linux and Mac OS which can be used to input unicode Devanāgarī characters. It is also available in some mobile phones. The modern operating systems directly support INSCRIPT key-layout for keying in Hindi, Marathi, Nepali, Sanskrit text encoded in Unicode.

Pls. note these are the general standard followed worldwide with InScript layout being the specific standard followed by Indian Government Agencies for keying in Indian/Devanagari scripts. It is advisable to judiciously consider the standards as applicable in the context of Nepal & Nepali language.

Resource Locator:

- QWERTY : http://en.wikipedia.org/wiki/QWERTY
- InScript : http://en.wikipedia.org/wiki/InScript
- http://en.wikipedia.org/wiki/Keyboard_layout

6.9 Business Area Specifications

There are various standards bodies, business communities and other groups working on specifications for the exchange of specific content-related information. They fall into two broad classes: one represents particular business objects, such as invoices or resumés; the other class defines a transaction, for example the submission of an invoice or a deposit into a particular account. Some specifications focus on common business objects and some on standardising complex transactions. Further, some proposed specifications include a single schema for a single business object, while others are frameworks that propose rules and structure for classes of schemas and may include more than 100 individual schemas.

This will include some of the important business area which usually require standardization

Table 6-19: Business area specification

Specification for specific business areas		
Standards Proposed	**Mandatory/Recommendatory**	**Reference & Links to Application Integration Technical Standards Details**
Specification for specific business areas – Finance		
• XBRL should be used for XML based forms and tax taxonomy • RIXML also can be considered to prepare financial content	Recommendatory	4.9.1.1 XBRL 4.9.1.2 RIXML
Specification for specific business areas - Workflow and Web Services		
• Wf-XML should be used to exchange information among workflow management system • ebXML Business Process Specification Schema and OASIS Business Transaction Protocol can also be considered to provide coordination between different system	Recommendatory	4.9.2.1 Wf-XML 4.9.2.2 ebXML 4.9.2.3 OASIS BTP
Specification for specific business areas - e-Health		
• HL7 should be adopted • SNOMED Clinical Terms should be used	Recommendatory	4.9.3.1 HL7 4.9.3.2 SNOMED Clinical Terms
Specification for specific business areas - e-Learning		
Following standard should be followed • IMS standards for Content Packaging Information Model, XML Binding, Test Interoperability, Digital repositories,Simple sequencing, Learning design • SCORM • IEEE 1484.12.1: 2002 LOM	Recommendatory	4.9.4.1 IMS Standards 4.9.4.2 SCORM 4.9.4.3 IEEE 1484.12.1: 2002 LOM 4.9.4.4 BS7988

Specification for specific business areas		
• BS7988		
Specification for specific business areas – Legal		
• Legal XML can be considered if schema suitable for Nepal is available	Recommendatory	4.9.5.1 Legalxml
Specification for specific business areas – HR		
• HR-XML can be considered for human resources exchange application	Recommendatory	4.9.6.1 HR XML
Specification for specific business areas - e-News		
• News XML can be considered to broadcast eNews	Recommendatory	4.9.7.1 NITF
Specification for specific business areas - e-Payments		
• PCI can be considered for cardholder data and PIN security for Online payments as well as best practices for payment application development • EMV can be considered for physical and electronic requirements of payment system IC cards • 3D Secure can be considered for further identity verification	Recommendatory	4.9.8.1 ISO 8583 4.9.8.2 PCI-DSS 4.9.8.3 PCI PED 4.9.8.4 PA DSS 4.9.8.5 EMV 4.9.8.6 3D-Secure

6.9.1 Specification for specific business areas – Finance

6.9.1.1 eXtensible Business Reporting Language(XBRL)

Description:

XBRL (eXtensible Business Reporting Language) is a language for electronic communication of business and financial data which is revolutionising business reporting around the world.

Standard Details:

XBRL International has provided the specification and technical standard for it which is available in the following resource locator

Resource Locator:

- XBRL

  http://www.xbrl.org

6.9.1.2 RIXML

Description:

The RIXML standard provides extensive capabilities to tag any piece of research content, in any form or media with enough detail for end users to be able to quickly search, sort and filter aggregated research.

Standard Details:

RIXML.org has provided the specification and technical standard for it which is available in the following resource locator

Resource Locator:

- RIXML

  www.rixml.org

6.9.2 *Specification for specific business areas – Workflow and Web Services*

6.9.2.1 Wf-XML

Description:

Wf-XML is designed and implemented as an extension to the OASIS Asynchronous Service Access Protocol. Wf-XML offers a standard way for a BPM engine to invoke a process in another BPM engine.Wf-XML completes the job by giving a standard way to pass the process definition between the design tool and the execution engine.

Standard Details:

Wf-XML is a BPM standard developed by the Workflow Management Coalition.The standards are available in the resource locator

Resource Locator:

- Wf-**xml**

  http://www.wfmc.org/wfmc-wf-xml.html

6.9.2.2ebXML

Description:

XML-based standards that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners.

Standard Details:

ebXML is joint initiative between the United Nations Centre for Trade facilitation and Electronic Business (UN/CEFACT) and Organization for the Advancement of Structured Information Standards (OASIS). This standards adopted by ISO and OASIS to provide formal XML-enabled mechanisms that can be implemented directly.

Resource Locator:

- ebXML

http://www.ebxml.org/

6.9.2.3OASIS BTP

Description:

The Business Transaction Protocol, or "BTP," provides a common understanding and a way to communicate guarantees and limits on guarantees between organizations. The formal rules are necessary for the distribution of parts of business processes outside the boundaries of an organization.

Standard Details:

The standards for this have been provided by OASIS which can be found in the following resource locator

Resource Locator:

- OASIS BTP

  http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=business-transaction

6.9.3 Specification for specific business areas – e-Health

6.9.3.1 HL7

Description:

Health Level Seven (HL7) involved in development of international healthcare standards.HL7 and its members provide a framework (and related standards) for the exchange, integration, sharing, and retrieval of electronic health information. The HL7 version 3 Clinical Document Architecture (CDA) is an XML-based markup standard intended to specify the encoding, structure and semantics of clinical documents for exchange.

Standard Details:

HL7 develops Conceptual Standards (e.g., HL7 RIM), Document Standards (e.g., HL7 CDA), Application Standards (e.g., HL7 CCOW), and Messaging Standards (e.g., HL7 v2.x and v3.0). Messaging standards are particularly important because they define how information is packaged and communicated from one party to another. Such standards set the language, structure and data types required for seamless integration from one system to another.

Resource Locator:

- HL7

  http://www.hl7.org/implement/standards/index.cfm

6.9.3.2SNOMED Clinical Terms

Description:

SNOMED CT (Systematized Nomenclature of Medicine -- Clinical Terms), is a systematically organized computer processable collection of medical terminology covering most areas of clinical information such as diseases, findings, procedures, microorganisms, pharmaceuticals etc. It allows a consistent way to index, store, retrieve, and aggregate clinical data across specialties and sites of care. It also helps organizing the content of medical records, reducing the variability in the way data is captured, encoded and used for clinical care of patients

Standard Details:

IHTSDO develops and promotes use of SNOMED CT to support safe and effective health information exchange. SNOMED CT is considered to be the most comprehensive, multilingual healthcare terminology in the world.

Resource Locator:

- SNOMED CT

  http://www.ihtsdo.org/snomed-ct/

6.9.4 *Specification for specific business areas – e-Learning*

6.9.4.1 IMS Standards

Description:

IMS specifications and standards cover most of the data elements used in "distributed and collaborative learning." IMS specifications promote the adoption of learning and educational technology and allow selection of best of breed products that can be easily integrated with other such products. These include a wide variety of technologies that support or enhance the learning experience, such as web-based course management system, learning management systems, virtual learning environments, instructional management systems, student administrative systems, ePortfolios, assessment systems, adaptive tutoring systems, collaborative learning tools, web 2.0 social learning tools, learning object repositories, and so forth.

Standard Details:

The details about the standards are provide in link mentioned in the resource locator below.

Resource Locator:

- IMS Project

  http://www.imsglobal.org/

6.9.4.2SCORM

Description:

Sharable Content Object Reference Model (SCORM) is a collection of standards and specifications for web-based e-learning. It defines communications between client side content and a host system called the run-time environment, which is commonly supported by a learning management system.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- SCORM

  http://www.scorm.com/scorm-explained/technical-scorm/

6.9.4.3IEEE 1484.12.1: 2002 LOM

Description:

Learning Object Metadata is a data model, usually encoded in XML, used to describe a learning object and similar digital resources used to support learning. The purpose of learning object metadata is to support the reusability of learning objects, to aid discoverability, and to facilitate their interoperability, usually in the context of online learning management systems (LMS).

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- IEEE 1484.12.1: 2002 LOM

  http://ltsc.ieee.org/wg12/20020612-Final-LOM-Draft.html

6.9.4.4BS7988

Description:

BS 7988 is a standard originally published by the British Standards Institution (BSI) in 2002.

The standard is aimed at universities, colleges, awarding bodies, corporations and other organizations delivering exams and sets out sensible principles for doing so.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- BS7988

  http://www.bsi-global.com/

6.9.5 *Specification for specific business areas – Legal*

6.9.5.1 legalXML

Description:

The OASIS LegalXML Member Section develops open, non-proprietary technical standards for structuring legal documents and information using XML and related technologies.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- LegalXML

http://www.legalxml.org/

6.9.6 Specification for specific business areas – HR

6.9.6.1 HR-XML

Description:

The HR-XML Consortium dedicated to the development and promotion of a standard suite of XML specifications to enable e-business and the automation of human resources-related data exchanges and specify global HR interoperability standards..

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- HR-XML

  http://www.hr-xml.org/

6.9.7 Specification for specific business areas – e-News

6.9.7.1 News Industry Text Format (NITF)

Description:

NITF uses the eXtensible Markup Language to define the content and structure of news articles. Because metadata is applied throughout the news content, NITF documents are far more searchable and useful than HTML pages.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- NITF

  http://www.iptc.org/

6.9.8 Specification for specific business areas – e-Payment

6.9.8.1 ISO 8583

Description:

ISO 8583 (Financial transaction card originated messages — Interchange message specifications) is the International Organization for Standardization standard for systems that exchange electronic transactions made by cardholders using payment cards.

A card-based transaction typically travels from a transaction acquiring device, such as a point-of-sale terminal or an ATM, through a series of networks, to a card issuing system for authorization against the card holder's account. The transaction data contains information derived from the card (e.g., the account number), the terminal (e.g., the merchant number), the transaction (e.g., the amount), together with other data which may be generated dynamically or added by intervening systems. The card issuing system will either authorize or decline the transaction and generate a response message which must be delivered back to the terminal in a timely manner. ISO 8583 defines a message format and a communication flow so that different systems can exchange these transactions

Standard Details:

The standard has 3 parts:

- Part 1: Messages, data elements and code values
- Part 2: Application and registration procedures for Institution Identification Codes (IIC)
- Part 3: Maintenance procedures for messages, data elements and code values

The details about the standards are provide in link mentioned in the resource locator below.

Resource Locator:

- ISO 8583

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31628

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=23632

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35363

6.9.8.2 Payment Card Industry Data Security Standard (PCI DSS)

Description:

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

Validation of compliance can be performed either internally or externally, depending on the volume of card transactions the organization is handling, but regardless of the size of the organization, compliance must be assessed annually. Organizations handling large volumes of transactions must have their compliance assessed by an independent assessor known as a **Qualified Security Assessor (QSA),** while companies handling smaller volumes have the option of self-certification via a **Self-Assessment Questionnaire (SAQ).** In some regions these SAQs still require signoff by a QSA for submission.

In July 2009, the PCI Security Standards Council published wireless guidelines for PCI DSS recommending the use of **Wireless Intrusion Prevention System (WIPS)** to automate wireless scanning for large organizations. Wireless guidelines clearly define how wireless security applies to PCI DSS 1.2 compliance. These guidelines apply to the deployment of Wireless LAN (WLAN) in cardholder data environments, also known as CDEs.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- PCI DSS 1.2

  https://www.pcisecuritystandards.org/security_standards/supporting_documents_home.shtml

  http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

6.9.8.3 Payment Card Industry PIN Entry Device (PCI PED) (a.k.a PIN Transaction Security (PCI PTS))

Description:

PCI PED applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions. Merchants should use only PIN entry devices that are tested and approved by the PCI SSC.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- PCI PED (PCI PTS)

  https://www.pcisecuritystandards.org/security_standards/ped/index.shtml

6.9.8.4 Payment Application DSS (PA DSS)

Description:

The PA-DSS (formerly known as, **Payment Application Best Practices (PABP)**) is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants and third party agents to use payment applications that are validated independently by a PA-QSA company and accepted for listing by the PCI SSC..

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- PA DSS

  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

6.9.8.5Europay, MasterCard and Visa (EMV)

Description:

EMV is a standard for interoperation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions. The name EMV comes from the initial letters of Europay, MasterCard and VISA, the three companies that originally cooperated to develop the standard.

Visa and MasterCard have also developed standards for using EMV cards in devices to support **card-not-present transactions over the telephone and Internet**. **MasterCard** has the Chip Authentication Program (CAP) for secure e-commerce. Its implementation is known as **EMV-CAP** and supports a number of modes. **Visa** has the **Dynamic Password Authentication (DPA)** scheme, which is their implementation of CAP using different default values.

The EMV standards define the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions. There are standards based on ISO/IEC 7816 for contact cards, and standards based on ISO/IEC 14443 for contactless cards.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- EMVCo

  http://www.emvco.com/specifications.aspx?id=155
- EMV

  http://en.wikipedia.org/wiki/EMV
- EMV CAP

  http://en.wikipedia.org/wiki/Chip_Authentication_Program
- Visa Codesure (DPA)

  http://www.visaeurope.com/en/about_us/what_we_do/payment_security.aspx
- ISO 7816

  http://en.wikipedia.org/wiki/ISO/IEC_7816

6.9.8.6 3D- Secure

Description:

3-D Secure is an XML-based protocol used as an added layer of security for online credit and debit card transactions. It was developed by **Visa** to improve the security of Internet payments and offered to customers as the **Verified by Visa** service. Services based on the protocol have also been adopted by **MasterCard**, under the name **MasterCard SecureCode**, and by **JCB International as J/Secure**.

3-D Secure adds another authentication step for online payments. Merchants are encouraged to use 3-D Secure to achieve higher coverage against fraud losses. When a merchant does not use 3-D Secure they are liable for fraudulent transactions even if the transaction was properly authorized. 3-D Secure should not be confused with the Card Security Code which is a short numeric code that is printed on the card.

Standard Details:

The details about the standards are provided in link mentioned in the resource locator below.

Resource Locator:

- 3D Secure (Verified By Visa)

  https://partnernetwork.visa.com/vpn/global/category.do?categoryId=85&documentId=117&userRegion=1

- 3D Secure Specifications

  https://partnernetwork.visa.com/vpn/global/category.do?categoryId=88&documentId=127&userRegion=1

6.10 Enterprise Content Management

Table 6-20: Enterprise Content Management

Enterprise Content Management		
Standards Proposed	Mandatory/ Recommendatory	Reference & Links to Collaboration Technical Standards Details
Enterprise Content Management		
• ISO 15836: 2009 - Information and documentation -- The Dublin Core metadata element set. • Open Archives Initiative Protocol for Metadata Harvesting 2.0 (OAI-PMH) for metadata collection. Protocol Version 2.0 of 2002-06-14 • RSS (RDF Site Summary) Version 1 • RSS (Really Simple Syndication) Version 2 • OpenURL 0.1 (migrating to 1.0) for context-sensitive linking • ISO 23950:1998 Information and documentation –Information retrieval (Z39.50) – Application service definition and protocol specification	Recommendatory	4.10.1 Enterprise Content Management

6.10.1 Enterprise Content Management

Description:

Content management is a critical technology that helps organizations manage important documents and other unstructured information, such as documents, images, media files, XML components, podcasts and e-mail messages. Content management vendors address a range of user needs and offer a range of functionality. Enterprise content management technologies should support database connectivity, should have integration capabilities with legacy systems and access technologies accepted as standards.

A Content Repository is a high-level information management system that is a superset of traditional data repositories. A content repository implements 'content services' such as: author based versioning, full textual searching, fine grained access control, content categorization and content event monitoring. JSR 170 & JSR 283 are standards of Content Repository for Java technology API. It is Version 2.0 of the content repository for java technology API. These two standards specify a standard API to access content repositories in java 2 independently of implementation.

Standard Details:

Enterprise content management is a vision or a strategy in an enterprise landscape. It is usually achieved through a tool based on a technology platform and provides features like document management, web content management, digital asset management, information rights management, records management and collaboration features like chat, mail/messaging, wikis, blogs etc., Along with DRT (Document Related Technologies) or DLM (Document Lifecycle Management), ECM can be considered as just one possible catch-all term for a wide range of technologies and vendors. It used to overcome the restrictions of former vertical applications and island architectures and used to manage information without regard to the source or the required use. The functionality is provided as a service that can be used from all kinds of applications. The user is basically unaware of using an ECM solution. ECM offers the requisite infrastructure for the new world of web-based IT, which is establishing itself as a kind of third platform alongside conventional host and client/server systems.

ISO 15836:2009 establishes a standard for cross-domain resource description, known as the Dublin Core Metadata Element Set. It does not limit what might be a resource.ISO 15836:2009 defines the elements typically used in the context of an application profile which constrains or specifies their use in accordance with local or community-based requirements and policies.

The Open Archives Initiative Protocol for Metadata Harvesting (referred to as the OAI-PMH in the remainder of this document) provides an application-independent interoperability framework based on metadata harvesting. There are two classes of participants in the OAI-PMH framework:

- Data Providers administer systems that support the OAI-PMH as a means of exposing metadata; and
- Service Providers use metadata harvested via the OAI-PMH as a basis for building value-added services.

A *harvester* is a client application that issues OAI-PMH requests. A harvester is operated by a service provider as a means of collecting metadata from repositories.

The RSS is a standard format for syndicating news content over the web using Dublin Core and RDF Published by the RSS-DEV Working Group. RSS (RDF Site Summary) Version 1 provides syndication hints to aggregators and others picking up this RDF Site Summary (RSS) feed regarding how often it is updated.

RSS (Really Simple Syndication) Version 2 was originally designed as an alternative standard format for syndicating news content over the web, however RSS can be and is being used to publish various types of data over the web, not just news data.

SFX is the name for a framework that allows context-sensitive linking between webresources. It finds its origin in research on linking between scholarly information resources. The SFX framework is context-sensitive in that the target of a link within the framework depends on the context of the user that follows the link. The context of the user is determined by the digital library collection that is available to him. Information resources that want to allow for such context-sensitive linking have to be made SFX-aware, by providing a hook to allow other servers to intervene dynamically in the decision regarding the target of a link. In order to allow for the delivery of context-sensitive services via an SFX-inspired framework, information resources must achieve the following:

- Implementation of a technique to make the resource understand the difference between a user that has access to a service component that can deliver context-sensitive services; and a user that does not.
- For users with access to a service component, provide an OpenURL for each metadata-object.

ISO 23950

This standard defines the Information Retrieval Application Service (section 3) and specifies the Information Retrieval Application Protocol (section 4). The service definition describes services that support capabilities within an application; the services are in turn supported by the Z39.50 protocol. The description neither specifies nor constrains the implementation within a computer system. The protocol specification includes the definition of the protocol control information, the rules for exchanging this information, and the conformance requirements to be met by implementation of this protocol. With a fully distributed search, there is no central control. Instead, there might be several second level control centers, each searching their separate domains or areas of expertise.

Identifiers:

Persistent and unique logical identifiers:

ANSI/NISO Z39.84 provides a syntax for unique identification for digital content (mechanism must be deployed to ensure that the Digital Object Identifiers (DOIs) have unique values).

Identifiers for persistent URLs:

PURLs (persistent URL) a PURL is a Persistent Uniform Resource Locator. Functionally, a PURL is a URL. However, instead of pointing directly to the location of an Internet resource, a PURL points to an intermediate resolution service.

- http://purl.org/docs/index.html

Persistent name for URLs:

URN (Uniform Resource Name) A URN is a persistent, globally unique name assigned to an object. In contrast to a URL, which changes whenever the location of an object changes, a URN has no location dependence and therefore a longer lifetime.

- http://www.w3.org/TR/2001/NOTE-uri-clarification-20010921/

Registered namespaces:

URI (Uniform Resource Identifier) a URI is a registered identification referring to Protocols or namespaces. A URN is a form of URI which uses a namespace (and associated Resolution Protocols) for persistent object names.

Scheme for site identification on the WWW:

URL (Uniform Resource Locator) a URL is the address of a resource which is retrievable using the Internet. A URL has to provide sufficient information to locate an object using a specified scheme. In the case of HTTP URLs, the scheme is 'http', and the scheme-dependent part specifies the name of the HTTP Server as well as the path of the object on the HTTP Server.

Identifiers for digital objects using ASN.1:

Object Identifier (OIDs) are used in ASN.1 based protocols.

- ISO/IEC 9834-2:1993 Information technology -- Open Systems Interconnection -- Procedures for the operation of OSI Registration Authorities -- Part 2: Registration procedures for OSI document types

- ISO/IEC 8824-1:2003
  Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation
- ISO/IEC 8824-2:2003
  Information technology -- Abstract Syntax Notation One (ASN.1): Information object specification

Radio tracking identification:

Radio Frequency Identification RFID use tracking and access applications where bar codes and labels are not suitable. RFID has established itself in a wide range of markets including livestock identification and automated vehicle identification (AVI) systems because of its ability to track moving objects. For further information see ISO/IEC SC31 RFID Related Standards including ISO/IEC 15434, 15459, 15961-3, 18000, 18001, 18046.18047, 19789 and 24710.

Codes for physical object as used in the retail industry:

EAN.UCC (European Article Number/Uniform Code Council) was the first bar code symbology widely adopted. An industry standard bar code symbology for product marking.

Resource Locator:

- EMC content management products

  http://www.emc.com/products/category/content-management.htm
- Open Text

  http://www.opentext.com/
- ISO 15836

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142
- OAI-PMH 2.0

  http://www.openarchives.org/OA/openarchivesprotocol.html
- RSS Version 1

  http://web.resource.org/rss/1.0/
- ISO 23950

  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=27446

6.11 Network Architecture

Network Architecture contains the framework of the physical components of the network. It contains the principle and procedure of the components.

Network Architecture		
Standards Proposed	Mandatory/ Recommendatory	Reference & Links to Collaboration Technical Standards Details
Network Components		
• Network interface cards	Mandatory	4.11.1 Network interface cards
• Switches	Mandatory	4.11.2 Switches
• Repeaters	Mandatory	4.11.3 Repeaters
• Bridges	Mandatory	4.11.4 Bridges
• Routers	Mandatory	4.11.5 Routers

6.11.1 Network Interface Cards

Description:

A network interface card (NIC) is installed in a computer so that it can be connected to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology. For wireless network the network card connects to radio based computer network.

Standards:

Standards for these components are provided in the following resource locator

Resource Locator:

http://standards.ieee.org/about/get/802/802.3.html

http://dx.doi.org/10.1109%2FIEEESTD.2009.5307322

www.ietf.org/rfc/rfc2640.txt

6.11.2 Switches (Layer 2/Layer 3)

Description:

A network switch is a device that connects different multiple networks. It should have the following features.

- ✓ Easy switch replacement using removable memory, allowing the user to replace a switch without having to reconfigure
- ✓ High availability, guaranteed determinism, and reliable security

- ✓ Support for IEEE1588v2, a precision timing protocol with nanosecond-level precision for high-performance applications
- ✓ Improved ring resiliency with the support of Resilient Ethernet Protocol (REP)
- ✓ Transparent IT integration with the support of Layer 3 routing protocols (IP Services)
- ✓ PROFINET v2 certification, with PROFINET conformance class B compliance

Standards:

Standards for the components are provided in the following resource locator

Resource Locator:

https://datatracker.ietf.org/doc/rfc4665/

https://datatracker.ietf.org/doc/rfc4031

https://datatracker.ietf.org/doc/rfc4834/

https://datatracker.ietf.org/doc/rfc4110/

6.11.3 Repeaters

Description:

Repeaters are used to retransmit the signal in higher power. Because while transmitting data it can only cover a limited distance before the quality of signal degrades. Using repeater one can preserve the signal strength. Following features must be supported while using a repeater.

- ✓ Should support for VOIP - and this would imply compliance to several protocols which should include - H.323, MGCP, MEGACO H.248
- ✓ Should be a Hardened Product - Hardened products are designed to withstand extreme conditions. Their casings provide protection from weather-related conditions and can act as a heat sink, directing high temperatures away from sensitive components. Hardened products use more reliable components than commercial products and are often used in telecommunications applications.
- ✓ Should be Stackable - The network equipment is stackable.
- ✓ Should be Rack Mountable - The network equipment can be mounted in a rack.
- ✓ Should have LED Indicator - The network equipment has a LED indicator light.
- ✓ Should support Full Duplex - Full duplex refers to the ability of a device or line to transmit data simultaneously in both directions.
- ✓ Should support VPN - virtual private network (VPN) is a connection that has the appearance and many of the advantages of a dedicated link, but occurs over a shared network. Using a technique called tunneling, data packets are transmitted across a public, routed network in a private "tunnel" that simulates a point-to-point connection and allows network protocols to traverse incompatible infrastructures.

6.11.4 Bridges

Description:

In networking bridges are used to filter network traffic. It inspects the network traffic and decides whether to allow it or not. It reduces the network traffic by creating a logical partition in the LAN. While using a bridge it should have the following features.

- ✓ Support IPv6 for smarter routing
- ✓ Support VPN
- ✓ Support Full Duplex
- ✓ It should also have the characteristic of repeaters

6.11.5 Routers

Description:

Router is a device that decides the next network point for a packet data. Routers connect at least two networks and decide which way to forward data. This should also support the features of a network interface card.

Standards:

Standards for these components are provided in the following resource locator

Resource Locator:

http://standards.ieee.org/about/get/802/802.3.html

http://dx.doi.org/10.1109%2FIEEESTD.2009.5307322

www.ietf.org/rfc/rfc2640.txt

6.12 Open Source Software

Description:

Open-source software (OSS) is computer software that is available in source code form for which the source code and certain other rights normally reserved for copyright holders are provided under a software license that permits users to study, change, and improve the software. Open source licenses often meet the requirements of the Open Source Definition. Some open source software is available within the public domain. Open source software is very often developed in a public, collaborative manner. Open-source software is the most prominent example of open-source development and often compared to (technically defined) user-generated content or (legally defined) open content movements.

By developing and adopting a local open source policy, that addresses when and if OSS can be used based with an understanding and formal acknowledgement of the potential risks of using open source software, member firm employees will benefit from a having a process that provides them with guidelines to evaluate the potential benefits that open source software may bring to projects. The benefits of open source policy are:

- **Minimize the Business and Technical Risks of Deploying OSS**

  By having a policy in place, developers and managers will better understand the process that should be followed to evaluate the use of open source software, the risks that may be involved, and the steps that should be taken to mitigate the risks.

- **Maximizing Benefits of OSS**

  By developing and adopting a local open source policy, member firm employees will benefit from a having a process that provides them with guidelines to evaluate the potential benefits that open source software may bring to projects.

- **Agreement for Use of OSS**

  A clearly stated policy can help ensure staff in the member firms is aware of the local OSS strategy regarding the use of OSS.

The Open Source Definition:

The Open Source Definition is used by the Open Source Initiative to determine whether or not a software license can be considered open source. The distribution terms of open-source software must comply with the following criteria:

- **Free Redistribution**

  The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

- **Source Code**

  The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

- **Derived Works**

  The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

- **Integrity of The Author's Source Code**

  The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

- **No Discrimination Against Persons or Groups**

  The license must not discriminate against any person or group of persons.

- **No Discrimination Against Fields of Endeavor**

  The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

- **Distribution of License**

  The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

- **License Must Not Be Specific to a Product**

  The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

- **License Must Not Restrict Other Software**

  The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

- **License Must Be Technology-Neutral**

  No provision of the license may be predicated on any individual technology or style of interface.

Open Standards Requirement for Software:

The Requirement

An "open standard" must not prohibit conforming implementations in open source software.

The Criteria

To comply with the Open Standards Requirement, an "open standard" must satisfy the following criteria. If an "open standard" does not meet these criteria, it will be discriminating against open source developers.

- **No Intentional Secrets:**

  The standard MUST NOT withhold any detail necessary for interoperable implementation. As flaws are inevitable, the standard MUST define a process for fixing flaws identified during implementation and interoperability testing and to incorporate said changes into a revised version or superseding version of the standard to be released under terms that do not violate the OSR.

- **Availability:**

  The standard MUST be freely and publicly available (e.g., from a stable web site) under royalty-free terms at reasonable and non-discriminatory cost.

- **Patents:**

  All patents essential to implementation of the standard MUST:

  - be licensed under royalty-free terms for unrestricted use, or
  - be covered by a promise of non-assertion when practiced by open source software

- **No Agreements:**

  There MUST NOT be any requirement for execution of a license agreement, NDA, grant, click-through, or any other form of paperwork to deploy conforming implementations of the standard.

- **No OSR-Incompatible Dependencies:**

  Implementation of the standard MUST NOT require any other technology that fails to meet the criteria of this requirement.

Open Standards Compliance

To assist governments and other bodies in recognizing and adopting standards that conform to this Requirement, the OSI defines two levels of compliance:

- **OSR Compatible**

  This indicates that the owner of the standard has self-certified that their standard complies with this Requirement, and all Compliance Criteria. Anyone may ask the OSI to review an OSR Compatible standard; if the OSI finds that the standard is incompatible, the owner must either modify the standard or stop using the OSR Compatible mark.

- **OSR Conformant**

  This indicates the OSI has reviewed a standard, as submitted by the owner, and certified that it fully conforms to the OSR. The OSI may charge a fee to offset the costs of this certification.

Resource Locator:

- The Open Source Initiative

  http://opensource.org/

7. NeGIF Data Standards

7. NeGIF Data Standards

7.1 Metadata & Data Standard

Government information is a valuable economic asset. To make the most of this asset and thereby provide better services to the citizens and businesses it should be readily available, can be easily located and exchanged between ministries, citizens and businesses in a seamless and coherent way, taking account of privacy and security obligations.

For the government data to be truly interoperable defining the standards and rules governing the data and the metadata used across the eGovernance applications and services is very much essential. The following structure is proposed as a part of NeGIF v1.0 to be adopted and developed by the metadata and data standards working, as e-Governance emerges/progresses.

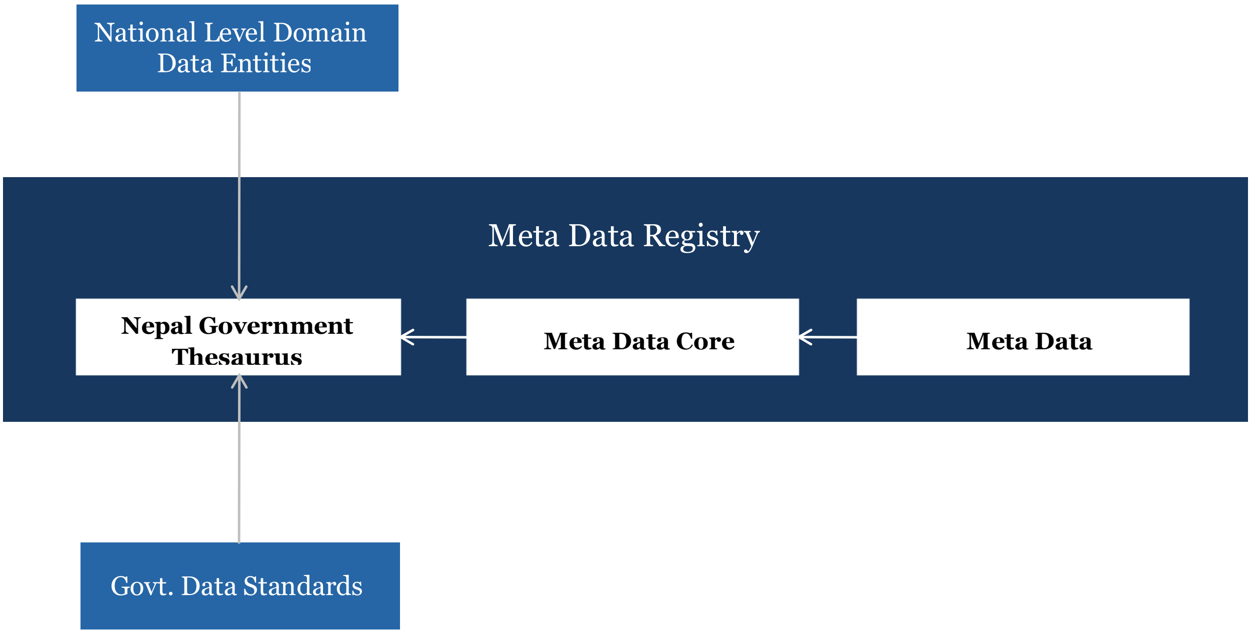

National Level Domain Data Entities
Meta Data Registry
Nepal Government Thesaurus
Meta Data Core
Meta Data
Govt. Data Standards

Figure 5-1: Meta Data and Data Standards

Nepal Government Thesaurus (NGoT)

The standards to use for these have to be developed as per a defined process which ensures coordination. NGoT – Nepal Government Thesaurus will provide the starting point. The Thesaurus will contain data entities (data items) of national interest which will help in seamless information exchange across the interoperability framework.

Broadly the data entities could be categorized as –

- Generic (Common) Data Entities
    - These are the common data entities that will be useful for information exchange across the Govt. of Nepal ministries & departments

  - Some of the generic data entities include Person, Person Name, Company, Address, Party Address, Party Identifier etc.

- Ministry / Department Specific Data Entities
  - These are the data entities specific to the business process of the ministry and based on the National Level Domain Data Entities identified
  - Some of the specific data entities includes Vehicle, Vehicle Type, Vehicle Owner, Driving License, License Category for Department of Transport Management etc

The data entities/items have been gleaned from current department specific ICT applications, planned/ in progress ICT applications and future ICT applications (e-Services). The Thesaurus will have structure reflecting the generic and the special segment. The Thesaurus will have to be updated as per an established process with maintenance tools.

Data Standards

The e-Government Interoperability Framework (e-GIF) mandates the adoption of XML and the development of XML schemas as the cornerstone of the government interoperability and integration strategy. A key element in the development of XML schemas is an agreed set of Government Data Standards (GDS). The data standards provide the detailed description of the data entity structure and its data elements as identified in NGoT. The detail may also include as appropriate high level representation for access and use.

Meta Data Core

These are core set of Metadata that may be described using XML. To publish and make available and facilitate access, metadata about data standards as per Dublin core with elements and qualifiers is Recommendatory for use. RDF standards may also be used. These Metadata will be used for any type of document.

Meta Data

These will comprise attributes about data additional to the Dublin core in accordance with the elements and qualifiers of the Dublin core e.g. in library management, Contact, document form, citation, channels etc. These Metadata can be domain specific which will get reflected on any document including data standards.

National level Domain Data Entities

In the National Enterprise Architecture for Nepal e-Governance, we envision creation and maintenance of national level data domain entities in accordance with a coordinated process. These data entities will establish and keep upto date the NGoT. The entities are domain specific e.g. Tax Administration, Transport, Land Reforms & Management, Municipality, Judiciary, Telecom Regulations etc.

Meta Data Registry

The Meta data core, Meta Data and NGoT will be held in a Registry (Meta Data Registry) which may be conceptually understood as a catalogue in a Library of books. By using tools the registry can be searched for selection and retrieval in application development thus enabling reuse. Adding resources to the Registry enables collaboration. There are tools to manage the master data that is stored in the database and keep it synchronized with the transactional systems.

The meta data standards given in this NeGIF version 1.0 is a structure with details on Meta data core, sample meta data, sample data standards structure and initial set of Government Thesaurus with common entities.

The following should be entrusted to the Meta data working group

- Endorsement of Elements of Dublin core and its adoption

- Develop a Nepal Government Thesaurus (NGoT)
- Define National Level Domain entities (ministry wise or common)
- Define Govt. Data Standards, and
- Develop a registry.

Metadata Technologies/Standards

Metadata technologies/standards are technologies, specification and tools that are used to create, maintain and manage Metadata Framework.

Table 7-1: Meta Data

Meta Data		
Standards Proposed	**Mandatory/ Recommendatory**	**Reference & Links to Meta Data & Data Standards Details**
Nepal Government Thesaurus (NGoT)		
• Sample lists of dictionary data entity / data elements are provided below. - Person - Company - Person Name – title, first/given name, middle name, last/family name - Party Address - Party ContactMethod - telephone number, email address - Person Gender - Person Marital Status - Person Birth Date - Citizenship Certificate - Driving License Number - Permanent Account Number - Date & Time • For each of the above dictionary entities there will be a meta data attribute	Mandatory	5.1.1 Nepal Government Thesaurus
Meta Data Core		
• Meta data core based on Dublin standards are listed below: 1. Title 2. Creator/Author 3. Subject and Keywords 4. Description 5. Publisher 6. Contributor 7. Date 8. Resource Type 9. Format 10. Resource Identifier 11. Source	Mandatory	5.1.2 Metadata Core 5.1.2.1 Title 5.1.2.2 Creator/Author 5.1.2.3 Subject and Keywords 5.1.2.4 Description 5.1.2.5 Publisher 5.1.2.6 Contributor 5.1.2.7 Date 5.1.2.8 Resource Type 5.1.2.9 Format 5.1.2.10 Resource Identifier 5.1.2.11 Source 5.1.2.12 Language

Meta Data		
12. Language 13. Relation 14. Coverage 15. Rights Management 16. Accessibility 17. Addressee 18. Aggregation 19. Audience 20. Digital signature 21. Disposal 22. Location 23. Mandate 24. Preservation 25. Status		5.1.2.13 Relation 5.1.2.14 Coverage 5.1.2.15 Rights Management 5.1.2.16 Accessibility 5.1.2.17 Addressee 5.1.2.18 Aggregation 5.1.2.19 Audience 5.1.2.20 Digital Signature 5.1.2.21 Disposal 5.1.2.22 Location 5.1.2.23 Mandate 5.1.2.24 Preservation 5.1.2.25 Status
Meta Data		
• Apart from the core there can be: - other Meta data domain specific or generic) and that will be used to define Data standards or for any documentation or - Extension elements that may be required to provide information about how the meaning of an element have been refined, or about how the value (specific content) of an element should be interpreted. A sample list of Meta data are provided below - Prepared by - Based on - Is part of - Is Basis For - requires - required by - created - modified - valid till - available from - replaces - Function - Alternative - Versions - Status - Comments		
Data Standards		
• The following structure is recommendatory to define data standards: - Name	Mandatory	5.1.3 Data Standards

Meta Data		
- Description - Type - Is Part Of - Has Parts - Data Format & Size - Version - XML Schema ID - Validations - Values - Owner - Based on - Status - Date Agreed		
Meta Data Technologies/Standards		
• XrML can be used to specify metadata for resources by leveraging the standard methodology developed by the Dublin Core Metadata Initiative. • Open Archives initiative harvesting protocols(OAI-PMH)can be considered for Metadata Harvesting • MIX 2.0 can be considered as the Technical Metadata for Digital Still Images Standards • ANSI/NISO Z39.87 - Data Dictionary can be considered for Technical Metadata for Digital Still Images • ODRL 1.1 can be considered for the standardisation of expressing rights information over content	Recommendatory	5.1.4 Metadata Technology
Meta Data Registry		
• Meta data registry can organize standards concept and data items and should maintain these standards in conformity with ISO11179 standards.	Mandatory	5.1.5 Metadata Registry

7.1.1 Nepal Government Thesaurus (NGoT)

The Govt. of Nepal would require to maintain a catalog of generic and ministry specific Govt. data entities and its data element which are of nationwide interest to the Govt. of Nepal for achieving interoperability. These data entities would facilitate seamless information exchange across departments and provide citizens and businesses with better access to public services.

The ***Nepal GEA Data Entity Catalog*** provides the initial list of these generic and ministry/department data entities and its elements. The department specific entities are for the initial short listed 16 departments only. The catalog provides a details of these data entities with respect to the data elements of these entities, the XML data definition of these elements, the data entity attributes that includes the nature of the data entity indicating whether it is a shared data or codification table, the owner of the data, the storage system indicating if the data entity will be stored in Govt. database or in respective owner system.

7.1.2 Meta Data Core

The Nepal Government should lay down core sets of metadata for their information resources or design search interfaces for information systems. To start with, Dublin core Meta data standards should be followed by the Govt. of Nepal by defining the 15 core attributes for every resource/artefact/document given below before building any application. Each of the attributes have to have a value to be defined by the central Meta data working group, The attribute together with the value forms the meta data. The following tables will provide details/description to the Meta data core for the list mentioned in the table. It is recommended to add to this list as and when more applications are developed and more data are captured.

7.1.2.1 Title

Element Name:	Title
Label:	Title
Definition:	A name given to the resource.
Obligation:	Mandatory
Description:	• Title enables the user to find a resource with a particular title or carry out more accurate searches. It is commonly used as the key point of reference in the list of search results. • It should be the formal title. If the resource does not have a formal title, then it is Recommendatory to create a meaningful title. The Meta tag should be customer focused: make it brief and meaningful rather than clever and catchy. • For an alternative title, add any form of the title used as a substitute or alternative to the formal title of the resource, including a name by which the resource is normally known, abbreviations and translations. If a resource's official or formal title is one which members of the public would find incomprehensible, it is Recommendatory that an additional, meaningful name be given to it. • The title should be in the same language as the resource.
Examples:	• If the resource is an e-mail and the subject line is unclear, give a meaningful title as the main title, and use the original subject line as the alternative title. • For an e-mail with an informal and uninformative subject line • Title: Payroll Application Milestone • Alternative: PR pilot test Monday
Reference:	Title – http://purl.org/dc/elements/1.1/title Alternative – http://purl.org/dc/terms/alternative

7.1.2.2 Creator/Author

Element Name:	Creator
Label:	Creator
Definition:	An entity primarily responsible for making the content of the resource.
Obligation:	Mandatory
Description:	• Creator enables the user to find resources that were written or otherwise prepared by a particular individual or organization. • Enables a resource to be tracked when the division creating it has been disbanded or the Creator has moved on. It is often best to 'depersonalize' the Creator and give the job title

Element Name:	Creator
	rather than the person's name. • Give full contact details if possible, especially when they are not to be given elsewhere. There are, however, situations where the Creator has legal responsibilities and obligations, and personal names may be needed for audit trails. • Acronyms may be meaningless to users. Use the full official title of the organization, or link to a glossary or explanatory note. • Not to be confused with Publisher & Contributor. Creator is responsible for the intellectual or creative content of the resource; Publisher is the person or organization that makes (releases) the resource available. Whereas a Contributor plays an important role (contributes to the resource) but does not have primary or overall responsibility for the content.
Reference:	http://purl.org/dc/elements/1.1/creator

7.1.2.3 Subject and Keywords

Element Name:	Subject
Label:	Subject/Keywords
Definition:	Topic of the resource
Obligation:	Mandatory
Description:	• Enables the user to search by the topic of the resource. • It must be identified and used as the source for one or more values for the unrefined Subject element. • It should reflect the main idea/subject of the resource. • Not be confused with Type & Coverage. Type indicates what the subject matter is and Coverage contains the contents of the resource to the extent of time and place.
Reference:	http://purl.org/dc/elements/1.1/subject

7.1.2.4 Description

Element Name:	Description
Label:	Description
Definition:	Summary content of the resource
Obligation:	Mandatory
Description:	• Helps user in identifying the resource needed. • It should be kept simple and precise and shouldn't contain repeated information that would be covered in other elements. • It is capable of covering key outcomes, abstract and events occurred etc.
Reference:	http://purl.org/dc/elements/1.1/description

7.1.2.5 Publisher

Element Name:	Publisher
Label:	Publisher

Element Name:	Publisher
Definition:	An entity responsible for making the resource available.
Obligation:	Mandatory
Description:	• Enables users to find a resource published by a particular organization or individual. It can also be referred to by those wanting to re-use or republish the resource elsewhere, or to purchase a copy of the resource. • The publisher is the person or organization a user needs to contact in order to obtain permission to republish the information contained in the resource or to obtain copies in a different format. A publisher has certain legal rights and responsibilities regarding the resource, so should always be named. • Not to be confused with Creator/Contributor – The publisher is the entity that releases the resource and the user would contact to obtain new copies or discuss copyright issues; the creator, and to some extent the contributor, are responsible for the content of the resource.
Examples:	Publisher: HLCIT, Singhadurbar, Kathmandu, Nepal, info@hlcit.gov.np
Reference:	http://purl.org/dc/elements/1.1/publisher

7.1.2.6 Contributor

Element Name:	Contributor
Label:	Contributor
Definition:	An entity responsible for making contributions to the content of the resource.
Obligation:	Mandatory
Description:	• Enables users to retrieve a resource which has been contributed to by a particular person or organization. • Include all individuals or organizations that played an important or significant role in creating the content of the resource but do not qualify as Creators. • Not to be confused with Creator – Creator is the person or group responsible for the intellectual or creative content of the resource; Contributor plays an important role but does not have primary or overall responsibility for the content.
Reference:	http://purl.org/dc/elements/1.1/contributor

7.1.2.7 Date

Element Name:	Date
Label:	Date
Definition:	• The date the resource was released or made available. • A date associated with an event in the life cycle of the resource.
Obligation:	Mandatory
Description:	• Enables the user to find the resource by limiting the number of search hits according to a date. • Dates need to appear in a format that is recognizable to people all over the world and that can be interpreted by computer software. The W3C format allows accurate searching and makes it clear which is the year, month or day. The format is 'yyyy-mm-dd', where 'yyyy' is the year, 'mm' is the month and 'dd' the day.

Element Name:	Date
	• Not be confused with Coverage & Disposal– Date refers to dates relevant to the information resource itself, not the information held within the resource; coverage Is the extent he resource covers where as Disposal – Use the Disposal review refinement to indicate when the decision to keep a resource needs to be made.
Reference:	http://purl.org/dc/elements/1.1/date

7.1.2.8 Resource Type

Element Name:	Resource Type
Label:	Type
Definition:	The nature or genre of the content of the resource.
Obligation:	Mandatory
Description:	• Enables the user to find a particular type of resource. • Not to be confused with Format – Format refers to the physical format of the resource, including the software application used to create, read and edit it; Type refers to the content of the resource and Subject – refers to what the resource is about.
Examples:	Type: Text
Reference:	http://purl.org/dc/elements/1.1/type

7.1.2.9 Format

Element Name:	Format
Label:	Format
Definition:	The physical or digital manifestation of the resource.
Obligation:	Mandatory
Description:	• Allows the user to search for items of a particular format. • Not to be confused with Type – Format looks at the physical format of the resource and includes hard or electronic copy, and the software needed to access the resource; Type considers the content and describes the category of the information in the resource.
Reference:	http://purl.org/dc/elements/1.1/format

7.1.2.10 Resource Identifier

Element Name:	Resource Identifier
Label:	Identifier
Definition:	An unambiguous reference to the resource within a given context.
Obligation:	Mandatory
Description:	• Allows a user to search for a specific resource or version. • Identification codes automatically allocated by records and content management systems can be used. • Identifiers can be made 'more unique' by prefixing them with national codes that are/will be released by the government.

Element Name:	Resource Identifier
	- Not be confused *with Location* – *Location* indicates the physical location of the resource, not its electronic file path or URL.
Reference:	http://purl.org/dc/elements/1.1/identifier

7.1.2.11 Source

Element Name:	Source
Label:	Source
Definition:	A reference to a resource from which the present resource is derived.
Obligation:	Mandatory
Description:	- Enables the user to find resources that have been developed using the content of a particular resource. - The described resource may be derived from the Source resource in whole or in part. - Not to be confused with Relation – Do not use Source if it is more appropriate to put this data in the Relation element, i.e. it may be more accurate to use the Relation refinement Is version of.
Reference:	http://purl.org/dc/elements/1.1/source

7.1.2.12 Language

Element Name:	Language
Label:	Language
Definition:	A language of the intellectual content of the resource.
Obligation:	Mandatory
Description:	- Enables users to limit their searches to resources in a particular language. - The use of language codes simplifies the inputting of the Language element. Most systems can be set so that the name of the language is displayed in full, which is more user-friendly. - It will be more important for resources that will be loaded onto the internet. It is an invaluable means for people to limit their searches to items that are relevant to their own needs.
Reference:	http://purl.org/dc/elements/1.1/language

7.1.2.13 Relation

Element Name:	Relation
Label:	Relation
Definition:	A reference to a related resource.
Obligation:	Recommendatory
Description:	- Enables the user to find other resources that are related to a resource, or to group together individual resources which then form a collection. - Not be confused with Source –relation describes other document that is next to kin to this resource or documents that are part of this document, whereas source is a term where the resource could be found.

Element Name:	Relation
Reference:	http://purl.org/dc/elements/1.1/relation

7.1.2.14 Coverage

Element Name:	Coverage
Label:	Coverage
Definition:	The extent or scope of the content of the resource.
Obligation:	Mandatory
Description:	• Enables the user to limit the search to items about a particular place or time. Can be thought of as a sub-section of the Subject element. • Not to be confused with Date – The Coverage refinement Temporal refers to the time period covered by the content of the resource, not its creation or publication date. Subject – Coverage contains information about the geographical and time aspects of the content of the resource. It can be thought of as a sub-section of the Subject element. There may be times when it is appropriate to enter the same data in both elements. Location – Location describes the physical whereabouts of the resource; it has nothing to do with what the resource is about.
Reference:	http://purl.org/dc/elements/1.1/coverage

7.1.2.15 Rights Management

Element Name:	Rights Management
Label:	Rights Management
Definition:	Information about rights held in and over the resource.
Obligation:	Mandatory
Description:	• Indicates who has the right to see, copy, redistribute, republish or otherwise make use of all or part of the resource. • Not to be confused with Accessibility – Accessibility indicates whether particular users will be able to access or use the resource; Rights indicates if they are allowed to. Audience – Audience tells you who the content is designed for; Rights is the place to list the individuals or groups who are allowed to see the resource.
Reference:	http://purl.org/dc/elements/1.1/rights

7.1.2.16 Accessibility

Element Name:	Accessibility
Label:	Accessibility
Definition:	Indicates the resource’s availability and usability to specific groups.
Obligation:	Mandatory
Description:	• Enables those unable to use all information resources to limit the search to items meeting their requirements. • Not to be confused with Audience – Accessibility indicates whether particular users will be able to physically access or use the resource; Audience indicates those users for whom the

Element Name:	Accessibility
	content is designed. - Rights indicate who is allowed to see the resource; Accessibility indicates who is actually able to see it.

7.1.2.17 Addressee

Element Name:	Addressee
Label:	Addressee
Definition:	The person (or persons) to whom the resource was addressed.
Obligation:	Mandatory
Description:	- Enables the user to identify the person(s) to whom the resource was dispatched. - Note that this does not provide evidence that the intended person actually received or read it, nor that they had the right or ability to access it. It is likely that in practice this element will mainly be used when describing e-mails. It is also applicable to other types of correspondence or any resource which is distributed. - Includes those listed in 'cc' and 'bcc' lists. Use the Addressee copy refinement to list person(s) to whom the resource was copied. - Not to be confused with Audience & rights – Audience refers to the wider sector of the population for whom the resource was intended; Addressee refers to the person or group to whom it was actively sent and rights refers to the person or group who have the right to see the resource, whether or not it has actually been sent to them.
Examples:	Addressee: prasad.gurung@hlcit.gov.np

7.1.2.18 Aggregation

Element Name:	Aggregation
Label:	Aggregation
Definition:	The resource's level or position in a hierarchy.
Obligation:	Mandatory
Description:	- Aggregation allows searches to be restricted to resources at a particular level. It also helps indicate which actions can be carried out on the resource. - It shows the extent to which the resource is part of a larger resource or collection, and defines where in a hierarchy it belongs. An example of this could be a folder containing individual records, where all actions that are performed on the folder, such as a change in the security classification, automatically affect each record in the folder.
Examples:	Aggregation: EGIF Folder

7.1.2.19 Audience

Element Name:	Audience
Label:	Audience
Definition:	A category of user for whom the resource is intended.
Obligation:	Mandatory

Element Name:	Audience
Description:	- Enables the user to indicate the level or focus of the resource, as well as enabling filtering of a search to items suited to the intended audience. - Do not use Audience unless the resource is prepared with a particular group in mind. If it is for general release, leave it blank. - Not to be confused with Accessibility, Rights and Addressee – Audience indicates which users the content is aimed at; Accessibility indicates whether particular users will be able to access or use the resource whereas Rights informs the user of a list of individuals or groups who are allowed to see the resource and Addressee refers to the person(s) to whom the resource was actually sent.
Examples:	Audience: Citizens
Reference:	http://purl.org/dc/terms/audience

7.1.2.20 Digital signature

Element Name:	Digital Signature
Label:	Digital Signature
Definition:	Authentication information used for the verification of resources in transactions.
Obligation:	Mandatory
Description:	- The National Archives will examine what metadata is likely to be created by digital signature technology and how far it is of relevance/use in records management when the adoption of this technology is advanced.

7.1.2.21 Disposal

Element Name:	Disposal
Label:	Disposal
Definition:	The retention and disposal instructions for the resource.
Obligation:	Mandatory
Description:	- Helps the user manage resources and ensure that they are not kept after they are needed or disposed of before their time. - It is Recommendatory that all web pages have a review date, so webmasters can easily locate pages before they become out of date and take necessary action, - Disposal in electronic records management systems (ERMS) is generally managed at the folder level. ERMS manage the disposal of resources to ensure they are only destroyed in accordance with an agreed disposal schedule and retained for periods consistent with the need to retain the resource.

7.1.2.22 Location

Element Name:	Location
Label:	Location
Definition:	The physical location of the resource.

Element Name:	Location
Obligation:	Recommendatory
Description:	• Enables the physical form of the resource to be found. Location will mainly be used for items held in a physical format. • This is especially relevant for items listed in a metadata base (a catalogue containing the metadata of resources but not the resources themselves) cause resources which are not available in electronic format might be referred to. • Not to be confused with Identifier – The URL or filename refers to an electronic, machine-readable pathway, not a physical location. Such information should go in the Identifier element. Coverage – This element concerns what the resource is about and not where the resource is.

7.1.2.23 Mandate

Element Name:	Mandate
Label:	Mandate
Definition:	Legislative or other mandate under which the resource was produced.
Obligation:	Mandatory
Description:	• Clarifies the legislative or other mandate for the business activity producing the records. • Not to be confused with Rights – Exemption from the data subject access provisions of the DPA 1998 is covered by the Rights element.

7.1.2.24 Preservation

Element Name:	Preservation
Label:	Preservation
Definition:	Information to support the long-term preservation of a resource.
Obligation:	Mandatory
Description:	Enables users now and in the future to read, interpret and use the resource. Preservation will mainly be used by records managers and others engaged in the long-term storage of official records. It will be used to support departmental migration activity, sustainability and archival preservation of the resource, and to preserve aspects of the provenance of the resource across transfer of custody between departments and to The National Archives Record Management Department. A variety of approaches may have to be taken to sustain and preserve electronic resources and their components across technical platforms. Information on the technical environment that produced the original objects greatly improves the chances of such approaches being achieved successfully and may allow digital archaeological reconstruction where past management has been lacking (and costs are justified). Some of this information may need to be included in an archival description or custody documentation. As preservation strategies across government emerge, some of the refinements may need to be mandated in future for resources identified as being of long-term importance. Additionally, some will concern the original environment of the records (possibly requiring automatic capture at declaration stage) and others may be defined at the batch level for resources at platform or format

Element Name:	Preservation
	migration. Not to be confused with Format – This provides information about the format of the resource for current processing; Preservation provides additional information intended to facilitate long-term preservation.

7.1.2.25 Status

Element Name:	Status
Label:	status
Definition:	The position or state of the resource.
Obligation:	Mandatory
Description:	• Enables the user to search for a resource according to its status. It may also be used as a reference by a user who wants to know the resource's status. • The status of a resource includes the extent to which it has been developed or completed, the version number, purpose and approval. • This data should apply to the described resource only, not to earlier versions.

7.1.3 Data Standards

The adoption of data standards for use across government will enable easier, more efficient exchanging and processing of data. It will also remove ambiguities and inconsistencies in the use of data across the government ministries, departments & govt. agencies. These standards apply to all systems that are mandated in the NeGIF and are for use in all other public sector interfaces. Compliance with these standards should follow the e-GIF compliance rules.

7.1.3.1 Data Standard Template

Each data standard will be documented using the following template. The template is based on eGIF (e-Governance Interoperability Framework) Standard of UK

Metadata	Value
Name	The full name of the generic or common Data Type/Data Element
Description	A simple but unambiguous definition / description of the Data Type or Element
Type	Generic or Specific Data Element
Is Part of	If the data element is a part of a parent data element
Has Part	The list of sub parts or the child data elements for this parent data element
Data Format & Size	The required format of the data from the specific domain perspective. This will include the minimum and maximum number of characters if appropriate, and the structure of the data element
Version	The version number of this standard
UML Diagram	The UML representation of the data element
XML Schema ID	The identifier of the XML schema where the data standard is used. It is expected that a standard will only be used in one schema and all government schemas will be held on National Portal. The XML

Metadata	Value
	schema will show the pattern, i.e. the size and mask, of the standard
Validations	Generic validations for Types and specific validations for Items. The validation rules to be applied for acceptance of data (e.g. first alpha character must be A, B or C).
Values	List of the acceptable values (e.g. Male, Female)
Default Value	For any list of values, the default value to be used unless otherwise stated
Owner	Name(s) of those Departments who own this standard
Based on	Origin of the standard (e.g. ISO, BSI, W3C etc)
Verification	Steps taken to establish the correctness of the Data Elements. Such steps taken for different level of verifications by departments will be detailed here
Comments	Additional notes
Status	The current status of the standard (Drafted or Agreed)
Date Agreed	The date this version was agreed as a Government Data Standard

7.1.3.2 Data Standard Catalog

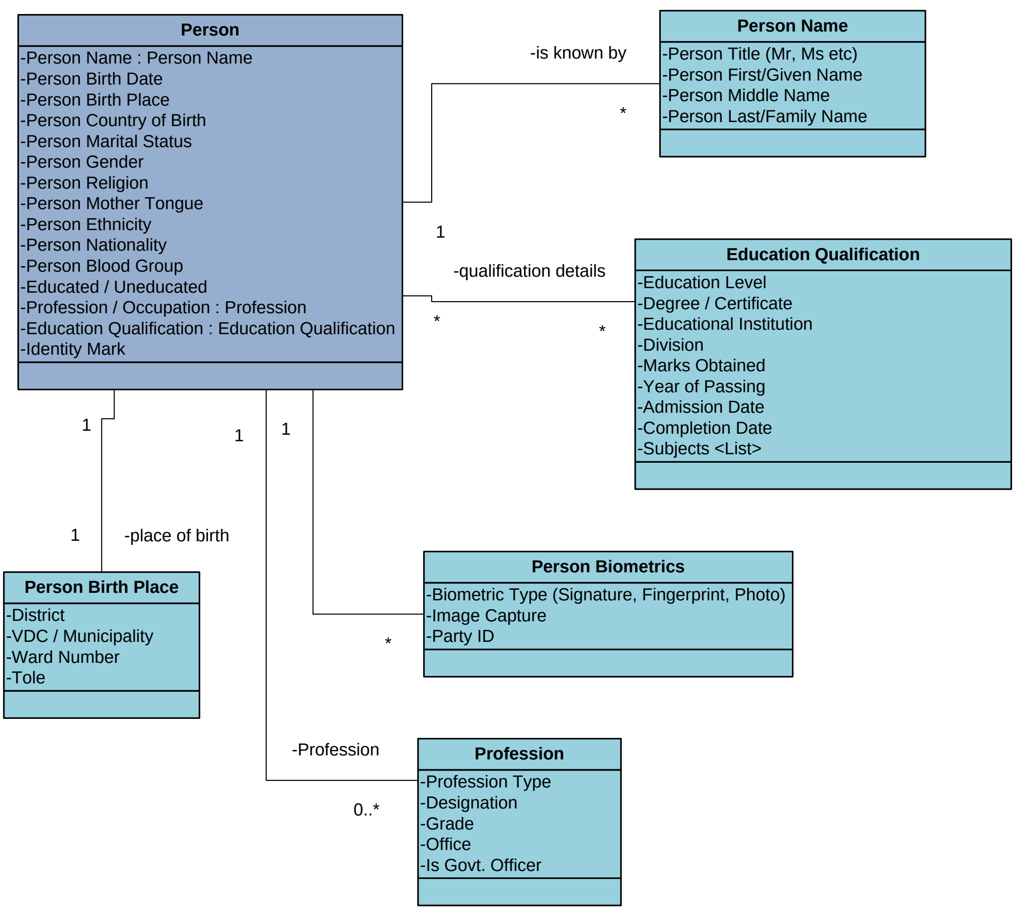
The Government Data Standards Catalogue sets out the rationale, approach and rules for setting and agreeing at the set of Government Data Standards (GDS) to be used in the Govt. Data Schemas and other electronic interchanges of data involving the public sector, developed to support the e-GIF. These standards are defined at a logical (business) level and not at a physical database storage level. However it is recommended that they be used for specifying data storage at the business level.

The ***Nepal GEA Data Standard Catalog*** provides a detailed description of the Govt. Data Standards of the common/generic data entities identified to be used across the government ministry & departments.

The following sub section lists the data standards for some of the important common data entities as an example. Refer to the Nepal GEA Data Standard Catalog document for the comprehensive list.

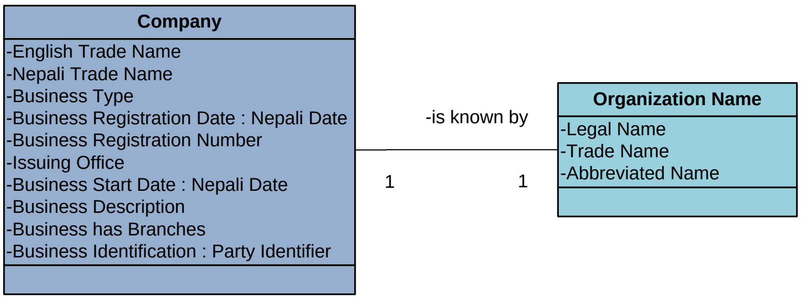
7.1.3.2.1 Person

Metadata	Value
Name	**Person**
Description	This data entity is a composition of data elements that describes an individual or person for e.g. person name, birthdate, marital status, gender, religion, profession etc. Typically Citizens (including voters, taxpayers, land owners, vehicle owners, consumers), Govt employees will be classified as Person
Type	Generic Data Element
Is Part of	Party (Supertype)
Has Part	• Person Name • Person Birth Date • Person Place of Birth • Person Country of Birth • Person Marital Status • Person Gender • Person Mother Tongue

Metadata	Value
	• Person Religion • Person Ethnicity • Person Nationality • Person Blood Group • Educated / Uneducated • Education Qualification • Profession / Occupation • Identity Mark
Data Format & Size	*Refer to format & size of individual child data elements in the Data Standard Catalog*
Version	1.0
UML Diagram	 Person -Person Name : Person Name -Person Birth Date -Person Birth Place -Person Country of Birth -Person Marital Status -Person Gender -Person Religion -Person Mother Tongue -Person Ethnicity -Person Nationality -Person Blood Group -Educated / Uneducated -Profession / Occupation : Profession -Education Qualification : Education Qualification -Identity Mark -is known by * Person Name -Person Title (Mr, Ms etc) -Person First/Given Name -Person Middle Name -Person Last/Family Name 1 -qualification details * * Education Qualification -Education Level -Degree / Certificate -Educational Institution -Division -Marks Obtained -Year of Passing -Admission Date -Completion Date -Subjects <List> 1 1 1 1 -place of birth Person Birth Place -District -VDC / Municipality -Ward Number -Tole Person Biometrics -Biometric Type (Signature, Fingerprint, Photo) -Image Capture -Party ID * -Profession 0..* Profession -Profession Type -Designation -Grade -Office -Is Govt. Officer
XML Schema ID	Refer to XML Schema (xsd) **PersonDescriptiveType** Refer to XML Definition **Person Structure**
Validations	*Refer to validations of individual child data elements in the Data Standard Catalog*
Values	*Refer to values of individual child data elements in the Data Standard Catalog*
Default Value	None
Owner	
Based on	
Verification	None

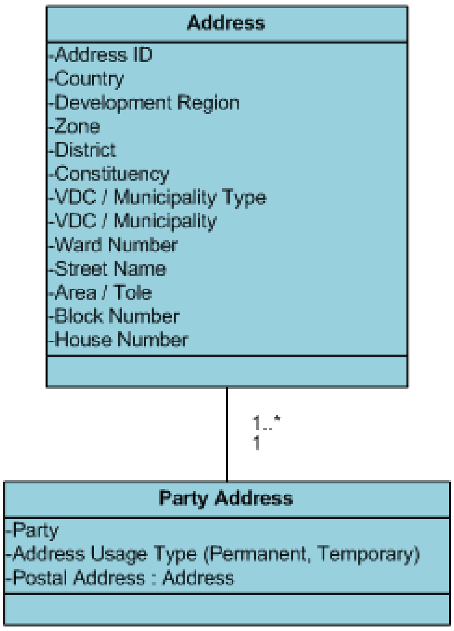
Metadata	Value
Comments	
Status	Drafted
Date Agreed	TBD

7.1.3.2.2 Company

Metadata	Value
Name	**Company**
Description	This data entity is a composition of data elements that describes a legal entity like company or organization e.g. organization name, business type, business registration number etc. Typically businesses like Private Limited Company / Public Limited Company / Partnership Firm / Charity Organization / Educational Institution are classified as Company.
Type	Generic Data Element
Is Part of	Party (Supertype)
Has Part	• Organization Name • Business Type • Business Registration Date • Business Registration Number • Registration Issuing Office • Business Start Date • Business Description • Business has Branches
Data Format & Size	*Refer to format & size of individual child data elements in the Data Standard Catalog*
Version	1.0
UML Diagram	 Company -English Trade Name -Nepali Trade Name -Business Type -Business Registration Date : Nepali Date -Business Registration Number -Issuing Office -Business Start Date : Nepali Date -Business Description -Business has Branches -Business Identification : Party Identifier -is known by 1 1 Organization Name -Legal Name -Trade Name -Abbreviated Name
XML Schema ID	Refer to XML Schema (xsd) **CompanyDescriptiveType** Refer to XML Definition **Company** Structure
Validations	*Refer to validations of individual child data elements in the Data Standard Catalog*
Values	*Refer to values of individual child data elements in the Data Standard Catalog*
Default Value	None
Owner	
Based on	
Verification	None

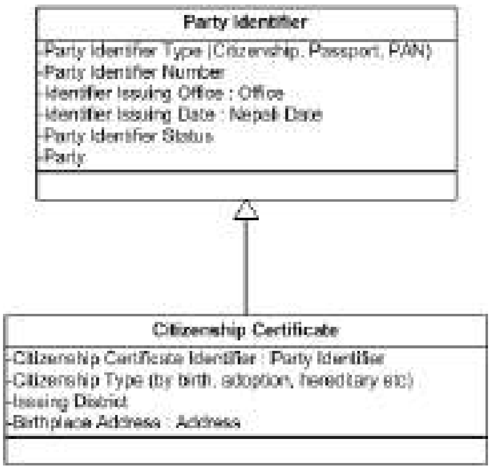
Metadata	Value
Comments	
Status	Drafted
Date Agreed	TBD

7.1.3.2.3 Address

Metadata	Value
Name	**Address**
Description	The generic data element that captures the details of the postal address of a party.
Type	Generic Data Element
Is Part of	
Has Part	• Address ID • Country Code • Development Region • Adminsitrative Zone • District • Constituency • VDC / Municipality Type • VDC / Municipality • Ward Number • Street Name • Tole • Block Number • House Number • P.O.Box
Data Format & Size	*Refer to format & size of individual child data elements*
Version	1.0
UML Diagram	

Metadata	Value
XML Schema ID	Refer to XML Schema (xsd) **AddressDescriptiveType** Refer to XML Definition **Address Structure**
Validations	*Refer to the validations of the individual child data elements*
Values	*Refer to the values of the individual child data elements*
Default Value	None
Owner	
Based on	As per the definition of the administrative units of Nepal
Verification	None
Comments	
Status	Drafted
Date Agreed	

7.1.3.2.4 Citizenship Certificate

Metadata	Value
Name	**Citizenship Certificate**
Description	This is a specialized form of Party Identifier data element that captures citizenship certificate details of a citizen of Nepal.
Type	Generic Data Element
Is Part of	Party Identifier (SuperType)
Has Part	• Citizenship Certificate Identifier (extended from Party Identifier) • Citizenship Type (by birth, adoption, hereditary etc) • Citizenship Certificate Issuing District • Birthplace Address
Data Format & Size	*Refer to the format & size of the individual child elements in the Data Standard Catalog*
Version	1.0
UML Diagram	 Party Identifier -Party Identifier Type (Citizenship, Passport, PAN) -Party Identifier Number -Identifier Issuing Office : Office -Identifier Issuing Date : Nepali Date -Party Identifier Status -Party Citizenship Certificate -Citizenship Certificate Identifier : Party Identifier -Citizenship Type (by birth, adoption, hereditary etc) -Issuing District -Birthplace Address : Address

Metadata	Value
XML Schema ID	Refer to XML Schema (xsd) **PartyIdentifierDescriptiveType** Refer to XML Definition **CitizenshipCertificate** Structure
Validations	*Refer to the validation of the individual child elements in the Data Standard Catalog*
Values	*Refer to the values of the individual child elements in the Data Standard Catalog*
Owner	Ministry of Home Affairs, Nepal
Based on	
Verification	***If Descendent*** • Birth Certificate / Educational Certificate • Citizenship Certificates of Parents • Documents showing ownership of property in the District in family's name OR Migration Certificate issued by relevant CDO Office ***If married to a Nepali man*** • Citizenship Certificate of Husband • Marriage Certificate • NOC from Country of Origin • Documents showing ownership of property in the District in Husband's family name OR Migration Certificate issued by relevant CDO Office to Husband's family • Recommendation Letter from VDC Chairperson / Mayor / Municipality Secretary
Comments	
Status	Drafted
Date Agreed	TDB

7.1.4 Meta Data Technology

7.1.4.1 XrML

Description

XrML provides a universal method for securely specifying and managing rights (and associated conditions) for all kinds of resources including digital content and services. It supports content integrity and entity authentication and confidentiality within the specification. Encodes in XML, leverages standard XML schemas, namespaces, digital signatures etc. Its customizable, and extensible and offers lot of flexibility.

Standard Details

XrML 2.0 is used to specify metadata for resources by leveraging the standard methodology developed by the Dublin Core Metadata Initiative. It has four key components namely

- Principal (person, device, application, etc.)
- Resource (work, service, name, etc.)
- Right (view, play, print, copy, forward, etc.)
- Condition (fee, time, geography, etc.).

Due to this interoperability is ensured as it can specify and "reach web services, allowing extended or more elaborate rights management for example seeking approval, reporting usage or tracking usage. Language can specify the trust environment before rights can be executed

the rights expression can ensure confidentiality and integrity which is key in government sector. The details about the standards are provide in link mentioned in the resource locator below.

Resource Locator:

- xrML

  http://www.xrml.org/

7.1.4.2 The Open Archives Initiative Protocol

Description:

The Open Archives Initiative Protocol for Metadata Harvesting (referred to as the OAI-PMH in the remainder of this document) provides an application-independent interoperability framework based on *metadata harvesting*. There are two classes of participants in the OAI-PMH framework:

- Data Providers administer systems that support the OAI-PMH as a means of exposing metadata; and
- Service Providers use metadata harvested via the OAI-PMH as a basis for building value-added services.

Standard Details:

This protocol mandates that individual archives map their metadata to the Dublin Core, a simple and common metadata set for this purpose. In other words, the relation of OAI compatibility to Dublin Core is that OAI standards allow a common way to provide content, and part of those standards is that the content has metadata that describes the items in Dublin Core format. The detailed specification and definitions are provided in the URL below.

Resource Locator

- OAI-PMH

  http://www.openarchives.org/OAI/openarchivesprotocol.html

7.1.4.3 ANSI/NISO Z39.87

Description:

This standard defines a set of metadata elements for raster digital images to enable users to develop, exchange, and interpret digital image files.

Standard Details

The dictionary has been designed to facilitate interoperability between systems, services, and software as well as to support the long-term management of and continuing access to digital image collections.

Resource Locator:

- ANSI/NISO Z39.87

  http://www.niso.org/kst/reports/standards?step=2&gid=None&project_key=b897b0cf3e2ee526252d9f830207b3cc9f3b6c2c.

7.1.4.4 MIX2.0

Description:

The Library of Congress' Network Development and MARC Standards Office, in partnership with the NISO Technical Metadata for Digital Still Images Standards Committee and other interested experts, is developing an XML schema for a set of technical data elements required to manage digital image collections. This schema is currently referred to as "NISO Metadata for Images in XML (NISO MIX)".

Standard Details

This is an XML schema that provides a format for interchange and/or storage of the data specified in the Data Dictionary - Technical Metadata for Digital Still Images (ANSI/NISO Z39.87-2006). MIX is expressed using the XML schema language of the World Wide Web Consortium. MIX is maintained for NISO by the Network Development and MARC Standards Office of the Library of Congress with input from users.

Resource Locator:

- MIX2.0

  http://www.loc.gov/standards/mix//

7.1.4.5 ODRL1.1

Description:

ODRL (Open Digital Rights Language) is an XML-based standard Rights Expression Language (REL) used in Digital Rights Management systems and open content management systems. ODRL is managed by an open organization that's open to public participation. ODRL explicitly support the use of right vocabularies from various sectors and communities. Its goal is to also support the reuse of other metadata vocabularies to supplement, e.g. the context element. For example, instead of using the context element to describe personal information, the vCard standard could be used. It has created a profile that supports Dublin Core Metadata Initiative (DCMI) metadata. It supports formal representation of ODRL data model in UML form which will improve ODRL data models.

Standard Details

ODRL is a standard language and vocabulary for the expression of terms and conditions over assets. ODRL covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations. Rights can be specified for a specific asset manifestation (i.e. format) or could be applied to a range of manifestations of the asset.

ODRL is focused on the semantics of expressing rights languages and definitions of elements in the data dictionary. ODRL can be used within trusted or untrusted systems for both digital and physical assets. However, ODRL does not determine the capabilities nor requirements of any trusted services (e.g. for content protection, digital/physical delivery, and payment negotiation) that utilises its language. Clearly, however, ODRL will benefit transactions over digital assets as these can be captured and managed as a single rights transaction. In the physical world, ODRL expressions would need an accompanying system with the distribution of the physical asset.

ODRL defines a core set of semantics. Additional semantics can be layered on top of ODRL for third-party value added services with additional data dictionaries.

ODRL does not enforce or mandate any policies for DRM, but provides the mechanisms to express such policies. Communities or organisations, that establish such policies based on ODRL, do so based on their specific business or public access requirements.

ODRL depends on the use of unique identification of assets and parties. Common identification is a very difficult problem to have agreement across sectors and is why identification mechanisms and policies are outside the scope of ODRL. Sector-specific versions of ODRL may address the need to infer information about asset and party identifiers.

The ODRL model is based on an analysis and survey of sector specific requirements (including models and semantics), and as such, aims to be compatible with a broad community base. ODRL intends to meet the common requirements for many sectors and has been influenced by the ongoing work and specifications/models of many groups including Dublin Core Metadata Initiative [DCMI] and Publisher Requirements for Industry Standard Metadata [PRISM]

ODRL proposes to be compatible with the above groups by defining an independent and extensible set of semantics. ODRL does not depend on any media types as it is aimed for cross-sector interoperability. We recommend to look forward to ODRL 2.0 which is at the draft stage currently.

The ODRL specification contains:

- the model for the ODRL expression language.
- the semantics of the ODRL data dictionary elements.
- the XML syntax used to encode the ODRL expressions and elements.
- additional ODRL data dictionaries can be defined.

Resource Locator:

- ODRL1.1

  http://www.w3.org/TR/odrl/

7.1.5 Meta Data Registry

Description

The Meta data core, Meta Data and NGoT will be held in a Registry (Meta Data Registry) which may be conceptually understood as a catalogue in a Library of books. By using tools the registry can be searched for selection and retrieval in application development thus enabling reuse. Adding resources to the Registry enables collaboration. There are standards to manage the Meta data registry.

Standard Details

ISO 11179 provides the Framework for the specification and standardization of data/metadata elements. These standards are provided for data element repositories; work on Taxonomies, Thesaurus and Dictionary. It contains various sections such as:

- Framework - This part of ISO/IEC 11179 introduces and discusses fundamental ideas of data elements, value domains, data element concepts, conceptual domains, and classification schemes essential to the understanding of this set of standards and provides the context for associating the individual parts of ISO/IEC 11179.
- Classification for administered items- This part of ISO/IEC 11179 provides a conceptual model for managing classification schemes. There are many structures used to organize classification schemes and there are many subject matter areas that classification schemes describe. So, this part also provides a two-faceted classification for classification schemes themselves
- Registry meta model and basic attributes- This part of ISO/IEC 11179 specifies a conceptual model for a metadata registry, and a set of basic attributes for metadata for use when a full registry solution is not needed
- Formulation of data definitions- This part of ISO/IEC 11179 provides guidance on how to develop unambiguous data definitions. A number of specific rules and guidelines are presented in ISO/IEC 11179-4 that specify exactly how a data definition should be formed. A precise, well-formed definition is one of the most critical requirements for shared understanding of an administered item; well-formed definitions are imperative for the exchange of information. Only if every user has a common and exact understanding of the data item can it be exchanged trouble-free
- Naming and identification principles- This part of ISO/IEC 11179 provides guidance for the identification of administered items. Identification is a broad term for designating, or identifying, a particular data item. Identification can be accomplished in various ways, depending upon the use of the identifier. Identification includes the assignment of numerical identifiers that have no inherent meanings to humans; icons (graphic symbols to which meaning has been assigned); and names with embedded meaning, usually for human understanding, that are associated with the data item's definition and value domain.
- Registration- This part of ISO/IEC 11179 provides instruction on how a registration applicant may register a data item with a central Registration Authority and the allocation of unique identifiers for each data item. Maintenance of administered items already registered is also specified in this document.

Resource Locator

- ISO11179

  http://metadata-stds.org/11179/

8. NeGIF Governance Structure

8. NeGIF Governance Structure

The overall EA Governance structure including the NeGIF governance model for the Govt. of Nepal will be finalized after discussion with HLCIT, PMC & other concerning bodies and will be provided as a separate addendum to this report.

9. Implementation Plan

9. Implementation Plan

Implementation of eGIF is not like architecture or a software system implementation. Having eGIF does not imply achievement of interoperability, ensuring the compliance to eGIF and building organisational and semantic capabilities can ensure achievement of interoperability. As a first step the principles, set of standards and policy have to be imbibed in the daily ICT processes. This implementation plan is covered under broadly 3 aspects:

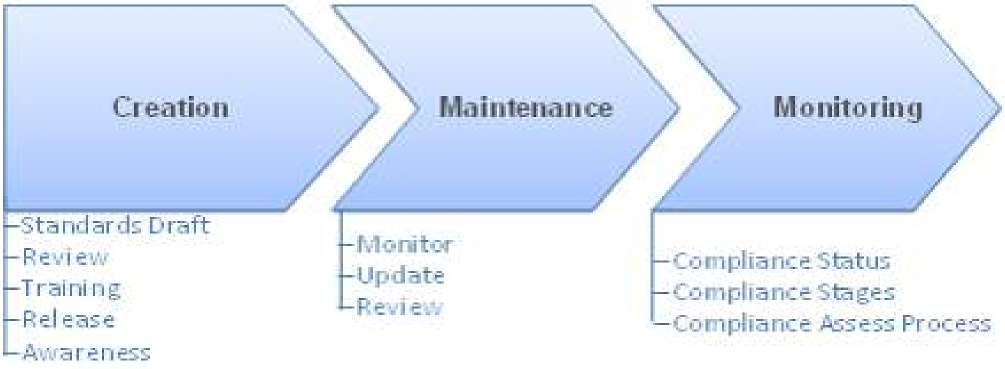


Figure 0-1: Implementation Plan

Essentially implementation of NeGIF includes creating and educating NeGIF framework (standards/ policies/ principles) across all agencies and the ministry/agency maintaining standards by updating it continually and ensuring compliance to standards across all ministries and agencies.

9.1 Creation

The following diagram depicts the roll-out process of NeGIF version 1 which also includes an indicative timeline

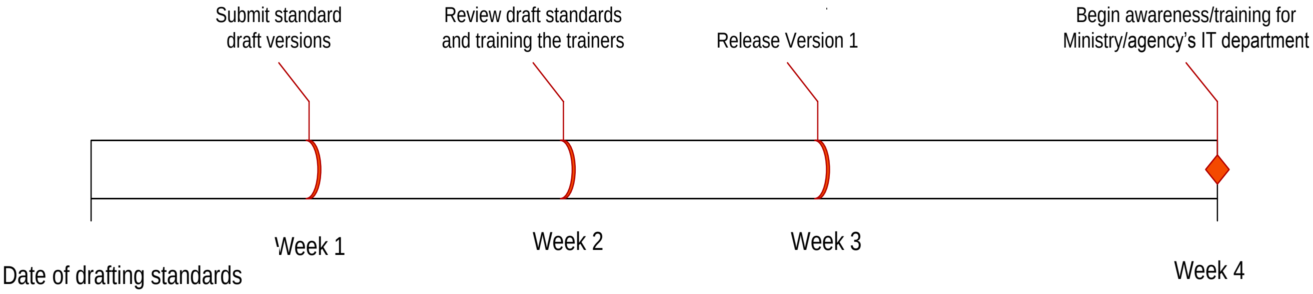

Submit standard draft versions
Review draft standards and training the trainers
Release Version 1
Begin awareness/training for Ministry/agency's IT department
Date of drafting standards
Week 1
Week 2
Week 3
Week 4

Figure: Roll out of NeGIF

9.2 Drafting NeGIF standards

The creation process involves drafting of standards that is required in Nepal context. The As-Is assessment and Best practice serves as the guidance to come up with the eGIF technical standard areas. The experts conduct a brainstorming session involving the working groups and HLCIT staff. The outcome of the brainstorming session is taken and the first set of standards, policies and principles are drafted

9.3 Review draft standards

The HLCIT has to identify a team of people who can take the responsibility to review the standards and provide valuable feedback.

9.4 Train the trainers

While the standards get reviewed the team of experts shall conduct workshops and training sessions to transfer knowledge and learning about the NeGIF. HLCIT has to identify a team for the training and in turn should make these people responsible to train others ('train the trainer' concept). PwC has identified the following training modules. A detailed training plan will be submitted before the workshop/training.

Table: Training Module

Area	Trainer	Attended By	Material used
Interconnection	Domain Expert	HLCIT eGIF team, IT heads and domain specialists	Presentations
Data Integration	Domain Expert	HLCIT eGIF team	Presentations
Access	Domain Expert	HLCIT eGIF team	Presentations
Collaboration	Domain Expert	HLCIT eGIF team	Presentations
Application Design and Development	Domain Expert	HLCIT eGIF team	Presentations
Application Integration	Domain Expert	HLCIT eGIF team	Presentations
System Standards	Domain Expert	HLCIT eGIF team	Presentations
Meta Data	Domain Expert	HLCIT eGIF team	Presentations
Security	Domain Expert	HLCIT eGIF team	Presentations
Governance and compliance mechanism	Domain Expert	HLCIT and regional HLCIT leadership team	Presentations

9.5 Release version 2

Based on review, this NeGIF version 2.0 has been released.

9.6 Awareness/training for ministry/agency's IT department and responsibility enforcement

The trained staff that HLCIT identified shall percolate their learning to every ministry/agency's IT department and regional HLCIT's will in turn percolate the same in the respective regions. Each ministry has to designate a person for getting trained ensuring compliance to standards.

We also recommend that HLCIT:

a) Consider monthly (2-3 Day) training program over the next 12 months for ministries and regions. This would address the concern that while as part of the NeGIF development "Train the Trainer" courses have been conducted, far more handholding is required over the next 9-12 months to create "Awareness", "Understanding" and "Importance" of the Standards across Ministries/regions - especially all ministries and regions that are being funded by The World Bank.

b) Create a proper website for eGIF for use by internal and external stakeholders. This website will serve as a repository for easy reference for all user of eGIF. The website has to be periodically updated as per the life cycle of various versions of NeGIF.

9.7 Maintenance

Maintenance includes management of the lifecycle of eGIF effectively. Technology change, multiple standards proliferation, requirements towards agility, development of more e-services etc. will increase the need to maintain the lifecycle of eGIF, so that it can keep pace with these changes and development. The following process is proposed for managing changes to the standards and to maintain the standards lifecycle.

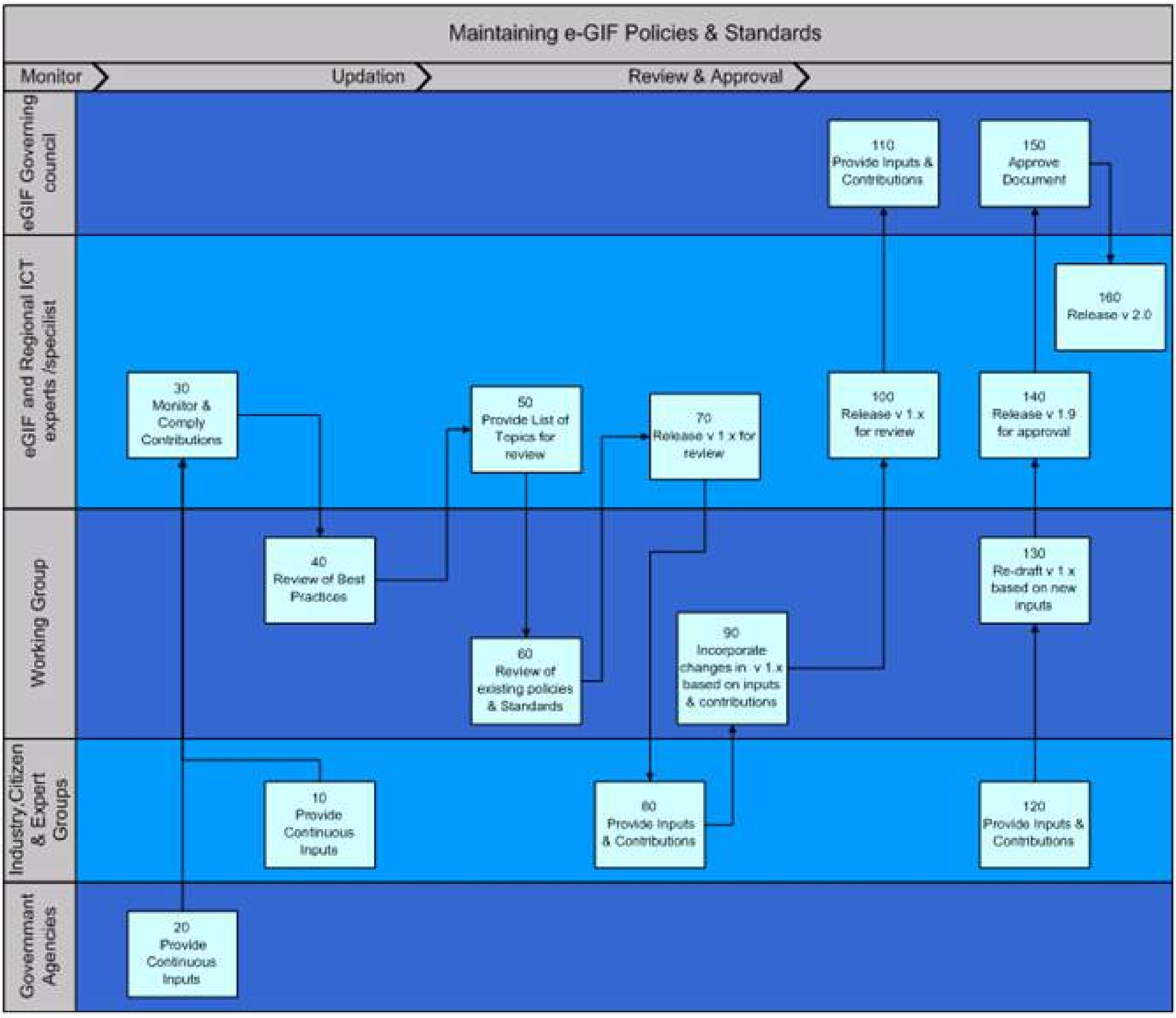

Maintaining e-GIF Policies & Standards
Monitor
Updation
Review & Approval
eGIF Governing council
eGIF and Regional ICT experts /specilist
Working Group
Industry,Citizen & Expert Groups
Government Agencies
110 Provide Inputs & Contributions
150 Approve Document
160 Release v 2.0
30 Monitor & Comply Contributions
50 Provide List of Topics for review
70 Release v 1.x for review
100 Release v 1.x for review
140 Release v 1.9 for approval
40 Review of Best Practices
130 Re-draft v 1.x based on new inputs
60 Review of existing policies & Standards
90 Incorporate changes in v 1.x based on inputs & contributions
10 Provide Continuous Inputs
80 Provide Inputs & Contributions
120 Provide Inputs & Contributions
20 Provide Continuous Inputs

Figure: Maintaining eGIF Policies & Standards

HLCIT should view the NeGIF version 2 as a living document which needs to be upgraded at frequent intervals. An approach to such review and update of NeGIF product lifecycle is provided below:

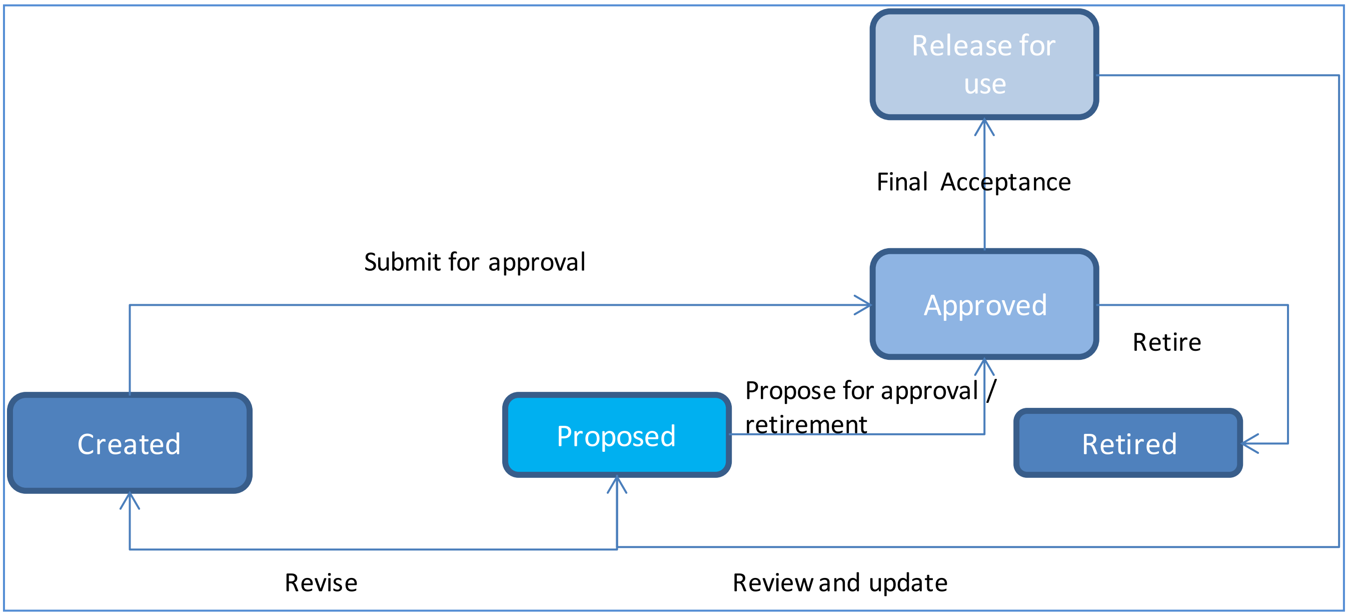


Figure: Review and update of NeGIF product lifecycle

9.8 Monitoring

Monitoring essentially involves ensuring compliance to the standards defined in the eGIF. Based on our understanding of the current situation, a strong compliance management mechanism is needed in Nepal to enforce interoperability and Compliance Framework. To ensure effectiveness of the compliance mechanism, it is proposed to have standards percolate as a policy of the respective agency and include standards in every aspect of the project lifecycle.

9.8.1 Compliance status

NeGIF applies to all ministries and agencies whenever new IT systems are built or major upgrade/migration of systems take place. It is essential for ministries to show their compliance to eGIF. The following compliance mechanism is suggested:

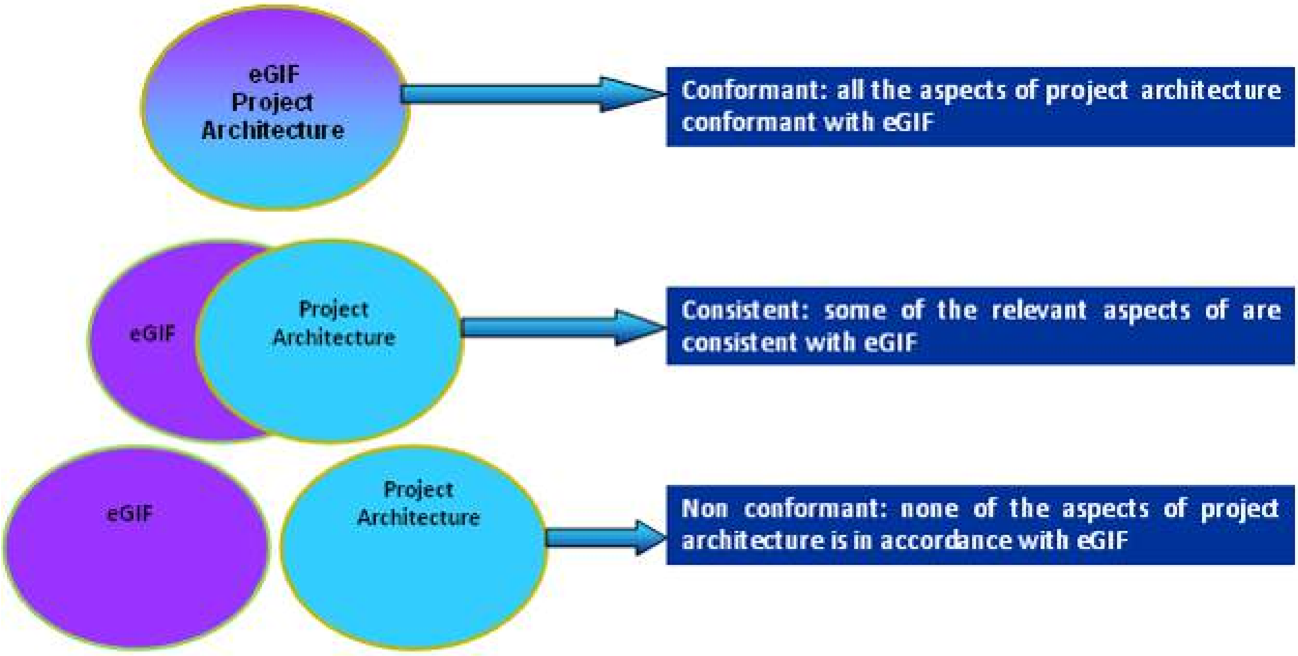

eGIF
Project
Architecture
Conformant: all the aspects of project architecture conformant with eGIF
eGIF
Project
Architecture
Consistent: some of the relevant aspects of are consistent with eGIF
eGIF
Project
Architecture
Non conformant: none of the aspects of project architecture is in accordance with eGIF

Figure: Compliance Mechanism

Every government project must show compliance to the eGIF. The above figure shows the levels of compliance.

- If the project is conforming to all aspects of the eGIF then it is termed as complaint.
- If the project is partially compliant for a good reason that could be justified, through exception process it is termed as consistent.
- Finally if the project does not show any compliance, the project is non complaint and show cause must be enforced and if need be specifications to be revised to bring the project on track.

9.8.2 Compliance Stages

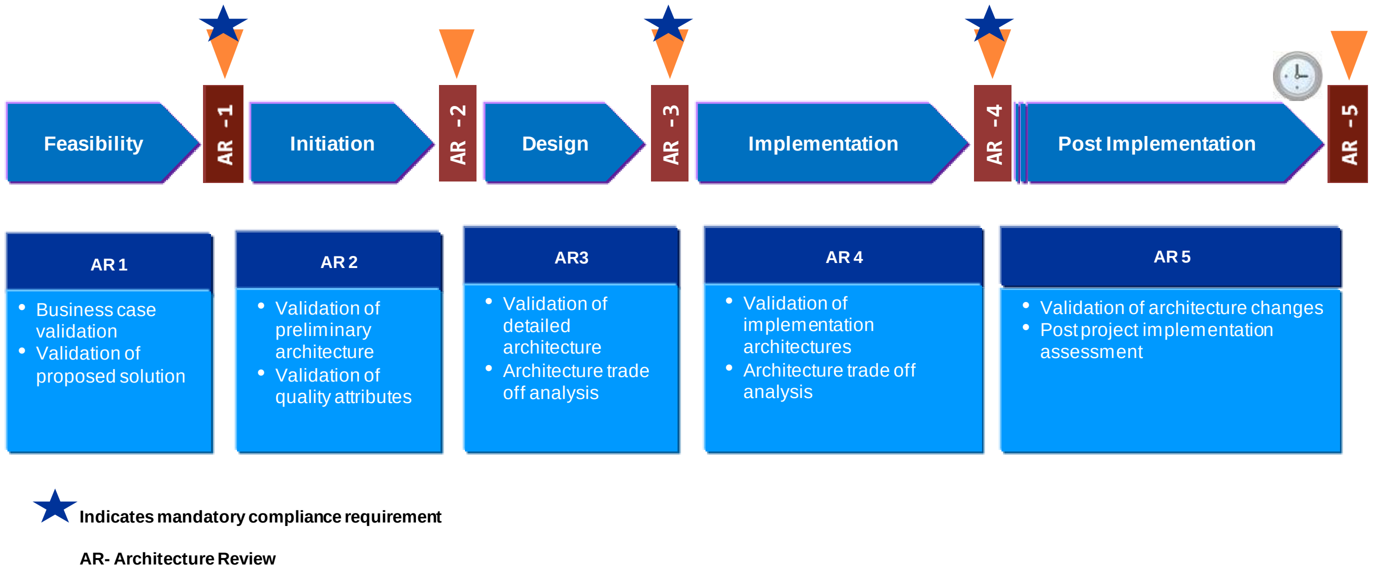

Feasibility
AR -1
Initiation
AR -2
Design
AR -3
Implementation
AR -4
Post Implementation
AR -5
AR 1
• Business case validation
• Validation of proposed solution
AR 2
• Validation of preliminary architecture
• Validation of quality attributes
AR3
• Validation of detailed architecture
• Architecture trade off analysis
AR 4
• Validation of implementation architectures
• Architecture trade off analysis
AR 5
• Validation of architecture changes
• Post project implementation assessment
★ Indicates mandatory compliance requirement
AR- Architecture Review

Figure: Compliance Stages

The above figure shows the compliance stages. Typically compliance checks can be carried out at 5 points throughout the project lifecycle. An eGIF/EA compliance review is a scrutiny of the compliance of a specific project against established architectural criteria, standards, and policies. It is important to appreciate that compliance to the NeGIF is not a one end point, acid test. Each requirement for compliance is likely to be unique. It may be necessary to demonstrate an acceptable degree of compliance at several points in a system lifecycle from conception to implementation. The assessment may be carried out some times by those commissioning the work (self-assessment) and at other times by HLCIT acting as their agents (Review of compliance).

Self assessment of compliance

Self assessment will require the respective ministry agency's IT department to ensure that the checklist of the eGIF compliance is made available upfront and they report a self assessment of compliance on the project to HLCIT at different stages of the project.

Review of compliance

A compliance team has to be formed by HLCIT to carry out eGIF reviews of the projects to check for and ensure compliance with the envisaged standards, policies and criterion. Regional HLCIT's can also be part of this for their respective regions. The compliance teams should define a framework for compliance evaluation and distribute it to all ministries so that they are aware of the compliance requirements/criteria. However it shows that it is good to have at least 2-3 mandatory check to be carried out as a compliance requirement. This is depicted in the diagram above using a star.

The compliance stages defined to prioritise the eGIF compliance effort suggest:

9.8.2.1 Feasibility

This is a phase where the business case is validated, the requirements specification is drafted and proposed solution is envisioned.

The success of ensuring compliance to eGIF is higher if requirements are identified and specifications required by eGIF are defined upfront in a project (in RFP, negotiations). This will lower non compliance.

9.8.2.2 Initiation

During the initiation phase the preliminary architecture of the solution is validated. At this stage a self assessment of adherence to eGIF and architecture principles is to be ensured. We recommend that a reporting mechanism is established wherein the project team reports the self assessment at the initiation phase to the eGIF compliance team.

9.8.2.3Design

Design is a crucial stage. The success of implementation will depend on the quality of the design. Validating the to-be system architecture will require adherence to interconnection, data integration, access for prime criteria and other relevant standards supporting interoperability will be required to be tested for compliance. This can be a self assessment or a review depending on the nature, scale and importance of the project.

9.8.2.4 Implementation

Implementation will involve deploying the system and training. At this stage a self assessment of testing the system for interoperability will be a practical way to ensure compliance.

9.8.2.5Post Implementation

In this stage, the testing results and outcomes can be measured and a complete review of the project, technology used, self assessment of compliance can be reviewed by the compliance team and report can be submitted on the compliance status of the project. Exemption process if any can also be triggered, heard and resolved during the post implementation compliance review.

9.8.3 Compliance Assessment Process

9.8.3.1 Self Assessment

The self assessment starts with gathering functional requirements at the beginning of the project determining the scope and comparing it with eGIF standards. A check list has to be prepared that can be included in the RFP. Subsequently, at the end of each stage of the project, the checklist has to be compared with the output of the respective process stage and compliance can be ensured through a simple scoring logic as follows:

Table: Compliance assessment

Scoring Logic						
Criticality of eGIF standard			Compliance Status of the Parameter			
Essential/Critical	2		Fully Complied	2		Low Risk

Scoring Logic						
Desirable/Non-Critical	1		Partially Complied	1		Medium Risk
			Not Complied	0		High Risk

9.8.3.2Review of Compliance

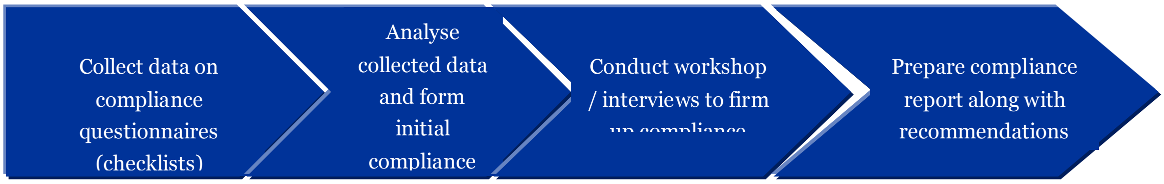

Collect data on compliance questionnaires (checklists)
Analyse collected data and form initial compliance
Conduct workshop / interviews to firm up compliance
Prepare compliance report along with recommendations

Figure: Review of compliance

Gather

The review of a process starts with collection of relevant and sufficient data/functional requirements of a project at the respective stage for which review is done. Then a comparison can be made with eGIF standards based on a pre defined compliance questionnaires (checklists).

Analyse

Once the team gathers the data it has to analyse the collected data and form initial compliance assessment. The analysis will also take into account the subjective environment, permissible exclusion, on the ground realities etc.

Validate

To validate the analyses, further meetings/interviews can be conducted with the ministry to firm up analysis.

Report

Once the assessment is over, a compliance report can be submitted on the compliance status of the project. Exemption process, if any can also be triggered, heard and resolved during the post implementation compliance review.

The result of the assessment could be:

a) To reject where the subject area (architecture or technology) are not compliant with standards. In this case the subject area can be:

- Adjusted or realigned in order to meet the compliance requirements
- To request a dispensation

When a Compliance Assessment is rejected, an alternate route to meeting the interim conformance is provided through dispensations. These are granted for a given time period and set of identified service and operational criteria that must be enforced during the lifespan of the dispensation. Dispensations are not granted indefinitely, but are used as a mechanism to ensure that service levels and operational levels are met while providing a level of flexibility in their implementation and timing. The time-bound nature of dispensations ensures that they are a major trigger in the compliance cycle. Last phase funds can be help up to ensure enforcement of the same.

b) To provide exemption in case if it is not possible to comply. In such situations an appeal for exemption must be approved by the Governing council. The exemption can be only on following grounds:

- a current standard that is going to be interoperating with another agency does not comply with the eGIF
- there is no suitable open or accepted standard for a new system that is proposed
- the current version of the eGIF cannot meet a ministry/agency's requirements
- an alternative approach to achieving interoperability has been agreed amongst all the parties exchanging data and a change is requested in the specification/requirement as an amendment.

However it is the onus of the agency to prove and demonstrate to the compliance committee that the current version of the eGIF cannot meet requirements. In case if an alternative approach is suggested by them to achieving interoperability, the compliance committee has to check the feasibility and accept if it is justified.

At times there may be good suggestions or pragmatic limitations due to which compliance could not have been achieved, the compliance committee should recommend such cases to the lead agency to consider updating the eGIF, wherever it is felt sensible.

c) Once a project is complaint with eGIF requirements it is certified complaint and the report is filed with HLCIT. Once exempted or dispensated, the project goes through the compliance requirement. The funds for the last phase can be released and a compliance report has to be submitted by the compliance team to the Governing council.

9.9 Making NeGIF work

Interoperability, like technology, is not an end but a means to an end. Technology must interact with and enable the policy and organisation dimensions to achieve interoperability. The effectiveness of eGIF will be measured by achieving the purpose and outcome. In the Nepal context the effectiveness of eGIF is to see every ministry/agency's maturity improves in terms of the key parameters such as

- how effectively multi dimensional interoperability(technical, semantic and organisational interoperability) is established and practiced
- extent of capability to create interoperability and share information
- Extent of roll out, adoption and governance of interoperability

To achieve these outcomes Nepal should do some basic steps in the initial year such as:

- define a clear e-Governance strategy
- define areas of concern, define goals of eGIF in alignment with e-Governance and define interoperability aspects (i.e NeGIFv.10 is a starting point)

- for the first few years monitor effectively the compliance to standards
- Maintain effectively the standards lifecycle.
- Align eGIF with eGov strategy and enterprise architecture
- Govern the entire process effectively.

Thus the focus of eGIF must be on the value of interoperability in terms of specific strategic objectives/purpose, the types of interoperability necessary to achieve those strategic objectives and other the decisions imperative to create the desired interoperability. Finally, governments must create capacity and Capability and govern it through proper mechanism that suits the environment but not compromise on the outcomes. Also, NeGIF is not central agency dictated common standards. It is a participative framework of principles, policies, standards and guidelines allowing scope to customize/make decisions about specific technology solutions (hardware/software etc.) at an individual agency's level.

10. Annexure & References

10. Annexure

10.1 Overview of Smartcard Standards

The eGIF technical standards mentioned in this document are the general standards followed world-wide. This section provides an overview of the specific smartcard standards and their context of usage as applicable to national identity projects as recommended by Mr. Ardaman Singh Kohli in his review report to assess the compatibility of the Nepal GEA & eGIF with NID.

Like most standards, smartcard standards have evolved to meet the evolving needs of users and the industry; therefore they do not fit into any overall structure.

Many of the standards are also specific to a type of card, e.g. standards for banking cards may not be relevant for health or identity cards, standards for single-application cards may not be relevant for multi-application cards, and standards for contact less cards may not be relevant for contact cards.

Furthermore, some smartcard standards have only been partially implemented by the industry, and some have not been implemented at all. It is also important to note that even ISO mentions that some standards may include patented technologies.

A better understanding of smartcard standards and specifications can be achieved by categorizing them into the following:

a. Fundamental, widely used, international standards: typically these are ISO standards like ISO 7816, 14443.
b. Regional standards: developed and/or used by a group of countries with specific requirements, like European, British, US standards (e.g. EN, G-8 Health card, CEN)
c. Application standards: created to meet the needs of specific applications (e.g. ICAO for electronic passports, GSM for SIM cards, EMV for financial cards)
d. Industry standards: developed by the industry when a clear need for a standard is felt, but no relevant standard exists (e.g. PC/SC for smartcard to PC communication)
e. National standards: created to fulfill some specific technical, application, or political requirements of a country
f. Partially used standards: Due to various reasons, a number of standards are not implemented or only partially implemented in available products (e.g. ISO 7816-7 is not used commercially, ISO 7816-9 may be partially used depending upon the functionality required)

10.2 Guidelines for selecting appropriate smartcard standards for NID Project

To navigate the difficult scenario of the standards, some of which are also mutually incompatible, the recommended guideline is to apply the 3 logical steps below:

STEP 1 -What are the objectives of using standards for the project?

Key objectives for using standards for the national identity card, are:

- assurance of product quality
- protection from over-dependence on an external entity
- interoperability with external entities

- compliance with legal obligations, e.g. privacy
- assurance of product security

STEP 2 - What functions are required in the application and card?

Each project has specific functional requirements, e.g. the purpose of the card, usage processes of the card, types of terminal devices to be used, types of data to be stored, types of processing required, physical security, electronic security, durability, usage environment, number and type of applications, type of data to be printed, etc.

The national identity card project is in its early phase, therefore the complete list of functions is yet to be defined (in the Detailed Project Report). A preliminary list of functions includes the following:

- Ability to hold multiple applications of different ministries
- Ability to store and process many data elements including biometrics
- Ability to work properly across the diverse geography and climatic conditions of Nepal

STEP 3 - Which standards should be selected to provide the functions and meet the objectives?

Available standards are analyzed and selected for their practical ability to meet the functionalities and objectives identified in steps 1 and 2. In the context of the Nepal national identity card, the recommended guideline is to:

a. Adopt all the relevant fundamental and partial international ISO standards. The word "relevant" is important here, because many of the ISO standards contain optional elements that may or may not apply to the NID Project solution architecture. Therefore we have to choose the right standards and the right parts of some standards, based on the Detailed Project Report of the NID Project.
b. Selectively adopt relevant Industry standards and Application standards. If an industry or application standard fills an important gap in the international standards, it is recommended to adopt it. The risk of using such standards is low because
    i. the industry remains motivated to ensure backward compatibility of the standards, as well as standardizing improved functionalities in future, and
    ii. application standards also endeavor to ensure backward compatibility, to protect the installed base of the application
c. As a guideline, it is advisable to avoid Regional and National standards. The risk of using such standards is higher because the owner of the standards is motivated purely by their own requirements, with no implicit or explicit motivation to support any other entity (like the Government of Nepal) that may also be using their standards. However, they may be used in very specific situations where it is strongly beneficial to use such a standard, but such usage must be justified with a well-documented analysis of the benefits and risks.

10.3 References

- United Kingdom e-Government Interoperability Framework (UK e-GIF) v 6.1
- New Zealand e-Government Interoperability Framework (NZ e-GIF)v 3.3
- Australian Government Technical Interoperability Framework
- Treasury Board information or technology standard (TBITS) and CLF 2.0 Standards and Guidelines
- Standards and Architectures for e-Government Applications v 2.0
- e-PING Standards of Interoperability for Electronic Government v 2.0.1
- Standards, Policies and Guidelines - Malaysian Government Interoperability Framework (MyGIF) v 1.0
- HANDBOOK ON MINIMUM INFORMATION INTEROPERABILITY STANDARDS(MIOS)
- OIO Basic Security Profile version 1.1
- FEA Consolidated Reference Model Document Version 2.2

- The open group Architecture framework(TOGAF),
- Enterprise architecture Cube(EA3),
- Standards and Architectures for e-government Applications (SAGA
- Federal Enterprise Architecture Framework (FEAF), US Department of Interiors
- ITEA of State of New Mexico
- Flashmap Systems Inc's IT infrastructure.
- European Public Administration Network, Key Principles of an Interoperability Architecture, p.5.
- An Effort to Achieve Organizational Interoperability- T. Vögele, M. Klenke, F. Kruse, H. Lehmann, C. Giffei Coordination Center PortalU at the Lower Saxony Ministry for Environment
- Australian Government Technical Interoperability Framework (AGTIF) v2. http://www.agimo.gov.au/publications/2005/04/agtifv2
- UNDP eGIF guide
- Friesen p 105
- EIF, v1, p. 16.
- Approaches to ConstructiveInteroperabilityCMU/SEI-2004-TR-020ESC-TR-2004-020Grace A. Lewis
- Lutz Wrage September 2004
- APDIP e-Note 20 / 2007
- http://www.tbs-sct.gc.ca/inf-inf/its-nit-eng.asp and http://www.tbs- sct.gc.ca/clf2-nsi2/clfs-nnsi/clfs-nnsi-2-eng.asp
- http://europa.eu.int/idabc/en/document/2317
- Page 17 Standards and Architectures for e-government Applications Version 2.0
- Standards, Policies and Guidelines -Malaysian Government Interoperability Framework (MyGIF)version 1.0
- Hans J. (Jochen) Scholl. Interoperability in e-Government: More than Just Smart Middleware.
- RAND Europe
- Based on http://www.scosta.gov.in/CertificateRelease1.htm
- http://www.itu.int/itudoc/itu-t/aap/sg15aap/history/g.694.2/index.html
- http://www.itu.int/rec/T-REC-G.992.2/en
- http://www.itu.int/rec/T-REC-G.992.5/en
- http://www.itu.int/rec/T-REC-G.993.1/en
- http://www.ieee802.org/3/av/
- http://www.pmc-sierra.com/ftth-pon/pon_standards.html
- http://www.3gpp.org/
- http://cdg.org/news/press/2009/Aug17_09.asp
- http://cdg.org/news/press/2009/Aug17_09.asp
- http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=english&wwwprog=pro-det.p&progdb=db1&He=IEC&Pu=60297&Pa=3&Se=100&Am=&Fr=&TR=&Ed=1
- http://www.tiaonline.org/standards
- http://www.iso.org/iso/iso_catalogue
- http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=61754&Pa=20&Se=11&Am=&Fr=&TR=&Ed=1
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=41532
- http://www.rfc-editor.org/rfc/rfc4271.txt
- http://www.rfc-editor.org/rfc/rfc1034.txt
- http://www.rfc-editor.org/rfc/rfc2131.txt
- http://www.rfc-editor.org/rfc/rfc3315.txt
- http://www.rfc-editor.org/rfc/rfc0959.txt
- http://www.rfc-editor.org/rfc/rfc4217.txt
- http://www.3gpp.org/ftp/Specs/html-info/29060.htm
- http://www.rfc-editor.org/rfc/rfc2616.txt
- http://www.ietf.org/rfc/rfc2818.txt
- http://www.rfc-editor.org/rfc/rfc1203.txt
- http://rfc-editor.org/rfc/2813.txt
- http://www.rfc-editor.org/rfc/rfc4510.txt

- http://www.itu.int/itudoc/itu-t/aap/sg16aap/.../h248.1/index.html
- http://www.itu.int/itudoc/itu-t/aap/sg16aap/.../h248.1/index.html
- http://www.rfc-editor.org/rfc/rfc2633.txt
- http://www.rfc-editor.org/rfc/rfc4760.txt
- http://www.rfc-editor.org/rfc/rfc3411.txt
- http://www.rfc-editor.org/rfc/rfc3977.txt
- http://www.rfc-editor.org/rfc/rfc1305.txt
- http://www.rfc-editor.org/rfc/rfc1939.txt
- http://www.rfc-editor.org/rfc/rfc2453.txt
- http://rfc-editor.org/rfc/rfc5531.txt
- http://www.rfc-editor.org/rfc/rfc3550.txt
- http://rfc-editor.org/rfc/5506.txt
- http://www.w3.org/Protocols/HTTP-NG/http-ng-scp.html
- http://rfc-editor.org/rfc/4566.txt
- http://www.rfc-editor.org/rfc/rfc3261.txt
- http://www.rfc-editor.org/rfc/rfc5321.txt
- http://www.w3.org/TR/soap12-part0/
- http://www.rfc-editor.org/rfc/rfc4251.txt
- http://www.rfc-editor.org/rfc/rfc854.txt
- http://www.rfc-editor.org/rfc/rfc1350.txt
- http://rfc-editor.org/rfc/rfc3920.txt
- http://www.rfc-editor.org/rfc/rfc4340.txt
- http://www.rfc-editor.org/rfc/rfc3168.txt
- http://www.rfc-editor.org/rfc/rfc5595.txt
- http://www.rfc-editor.org/rfc/rfc5596.txt
- http://www.rfc-editor.org/rfc/rfc2205.txt
- http://www.rfc-editor.org/rfc/rfc4960.txt
- http://www.rfc-editor.org/rfc/rfc0793.txt
- http://www.rfc-editor.org/rfc/rfc0768.txt
- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=558148
- http://www.rfc-editor.org/rfc/rfc0792.txt
- http://rfc-editor.org/rfc/rfc4604.txt
- http://rfc-editor.org/rfc/rfc3376.txt
- http://www.rfc-editor.org/rfc/rfc791.txt
- http://www.rfc-editor.org/rfc/rfc2460.txt
- http://www.rfc-editor.org/rfc/rfc1142.txt
- http://www.itu.int/itudoc/itu-t/aap/sg13aap/recaap/y1731/
- http://www.rfc-editor.org/rfc/rfc2702.txt
- http://www.rfc-editor.org/rfc/rfc3618.txt
- http://www.rfc-editor.org/rfc/rfc2362.txt
- http://www.rfc-editor.org/rfc/rfc3973.txt
- http://www.ieee802.org/1/pages/802.1P.html
- http://www.rfc-editor.org/rfc/rfc5151.txt
- http://www.rfc-editor.org/rfc/rfc4607.txt
- http://www.rfc-editor.org/rfc/rfc3768.txt
- http://rfc-editor.org/rfc/rfc5494.txt
- http://www.t13.org/Documents/UploadedDocuments/meetings/d97003.doc
- http://www.rfc-editor.org/rfc/rfc3931.txt
- http://www.rfc-editor.org/rfc/rfc3031.txt
- http://rfc-editor.org/rfc/rfc4861.txt
- http://www.rfc-editor.org/rfc/rfc5340.txt
- http://www.rfc-editor.org/rfc/rfc1661.txt
- http://rfc-editor.org/rfc/rfc2390.txt

- http://www.ieee802.org/1/pages/802.1w.html
- http://www.ieee802.org/1/pages/802.1D-2003.html
- http://www.ieee802.org/1/pages/802.1Q.html
- http://www.xcbl.org/
- http://oasis-open.org/committees/ubl/lsc/
- http://www.ifxforum.org/standards/
- http://www.emvco.com/
- http://www.columbia.edu/kermit/ascii.html
- http://www.ietf.org/rfc/rfc2279.txt
- http://www.unicode.org/
- http://www.unicode.org/versions/Unicode5.2.0/
- http://www.w3.org/RDF/
- http://www.w3.org/TR/xml11/#sec-intro
- http://www.oasis-open.org/committees/ciq/ciq.html#4
- http://www.oasis-open.org/committees/ciq/download.html
- http://www.oasis-open.org/committees/ciq/ciq.html#7
- http://www.oasis-open.org/committees/ciq/download.shtml
- http://www.omg.org/technology/documents/formal/xmi.htm
- http://www.omg.org/cgi-bin/doc?formal/2007-12-02
- http://www.iso.org/ISO8601:2004
- http://www.w3.org/TR/xslt
- http://www.eccnet.com/xmledi/guidelines-styled.xml ANSI ASC x12
- http://www.unece.org/cefact/cf_plenary/plenary98/docs/98cf4.pdf
- http://pdf.editme.com/pdfua
- http://pdf.editme.com/PDFE
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42274
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38920
- http://pdf.editme.com/PDFA
- http://pdf.editme.com/PDFX
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=42876
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office
- http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf
- http://www.remotesensing.org/libtiff/
- http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=2181
- http://www.w3.org/Graphics/GIF/spec-gif89a.txt
- http://www.jpeg.org/jpeg/index.html
- http://www.microsoft.com/downloads/details.aspx?FamilyId=DD422B8D-FF06-4207-B476-6B5396A18A2B&displaylang=en
- http://www.itl.nist.gov/fipspubs/fip177-1.htm
- http://www.uspro.org/documents/IGES5-3_forDownload.pdf
- http://www.chiariglione.org/mpeg/standards.htm
- http://www.w3.org/TR/2007/REC-webcgm20-20070130/
- http://www.w3.org/TR/html4/
- http://www.pdf-search-engine.com/iso/iec-11172-3-pdf.html
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=38538
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=38780
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=31443
- http://purl.org/dc/elements/1.1/title
- http://purl.org/dc/terms/alternative
- http://purl.org/dc/elements/1.1/creator
- http://purl.org/dc/elements/1.1/subject
- http://purl.org/dc/elements/1.1/contributor
- http://purl.org/dc/elements/1.1/publisher

- http://purl.org/dc/elements/1.1/description
- http://purl.org/dc/elements/1.1/date
- http://purl.org/dc/elements/1.1/type
- http://purl.org/dc/elements/1.1/format
- http://purl.org/dc/elements/1.1/identifier
- http://purl.org/dc/elements/1.1/source
- http://purl.org/dc/elements/1.1/language
- http://purl.org/dc/elements/1.1/relation
- http://purl.org/dc/elements/1.1/coverage
- http://purl.org/dc/elements/1.1/rights
- http://purl.org/dc/terms/audience
- http://www.xrml.org/
- http://www.openarchives.org/OAI/openarchivesprotocol.html
- http://www.niso.org/kst/reports/standards?step=2&gid=None&project_key=b897b0cf3e2ee526252d9f830207b3cc9f3b6c2c.
- http://www.loc.gov/standards/mix//
- http://www.w3.org/TR/odrl/
- http://metadata-stds.org/11179/
- http://csrc.nist.gov/publications/PubsFIPS.html
- http://www.w3.org/TR/SVG11/REC-SVG11-20030114.pdf
- http://www.w3.org/TR/SVG/
- http://www.w3.org/TR/SVGTiny12/
- http://www.w3.org/Graphics/GIF/spec-gif89a.txt
- http://www.gnu.org/software/gzip/
- http://www.gnu.org/software/tar/
- http://www.openmobilealliance.org/Technical/PublicMaterial.aspx
- http://www.ecma-international.org/publications/standards/Ecma-262.HTM
- https://developer.mozilla.org/En/New_in_JavaScript_1.8.1
- http://www.iso.org/iso/catalogue_detail?csnumber=31432
- http://webstore.iec.ch/preview/info_isoiec7811-1%7Bed3.0%7Den.pdf
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=29257
- http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30995
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=30558
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40604
- http://www.iso.org/iso/catalogue_detail?csnumber=28729
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39695
- http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=38770
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=28730
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50648
- http://www.w3.org/WAI/
- http://www.ietf.org/rfc/rfc5321.txt
- http://www.ietf.org/rfc/rfc1521.txt
- http://www.ietf.org/rfc/rfc2060.txt
- http://www.w3.org/XsL
- http://www.emc.com/products/category/content-management.htm
- http://www.opentext.com/
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cmis
- http://xml.coverpages.org/cmis.html#overview
- http://www.rfc-editor.org/rfc/rfc3261.txt
- http://www.rfc-editor.org/rfc/rfc3550.txt
- http://www.itu.int/rec/T-REC-H.323-200606-I/en
- http://www.itu.int/rec/T-REC-H.323-200606-I/en

- http://www.itu.int/net/itu-t/sigdb/speaudio/Gseries.htm
- http://www.itu.int/rec/T-REC-G.722-198811-I/en
- http://www.itu.int/rec/T-REC-H.261-199303-I/en
- http://www.itu.int/rec/T-REC-Q.931-199805-I/en
- http://www.itu.int/rec/T-REC-H.263-200501-I/en
- http://www.wapforum.org
- http://docs.oasis-open.org/ubl/os-UBL-2.0-update-delta.zip
- http://tools.ietf.org/html/rfc1737
- http://tools.ietf.org/html/rfc2141
- http://tools.ietf.org/html/rfc3406
- http://www.ietf.org/rfc/rfc4350.txt
- http://www.opengeospatial.org/standards/wfs
- http://www.opengeospatial.org/standards/wms
- http://www.bpmn.org/
- http://www.bpmi.org/
- http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-bpel/ws-bpel.pdf
- http://www.UML.org
- http://www.omg.org/technology/documents/modeling_spec_catalog.htm#UML
- http://www.w3.org/TR/2002/WD-xml11-20020425/
- http://www.osoa.org/xmlns/sca/1.0/sca-core.xsd
- http://www.openmobilealliance.org/tech/affiliates/wap/wap-238-wml-20010911-a.pdf
- http://www.W3c.org
- http://www.oasis-open.org/specs/index.php#uddiv3.0.2
- http://www.w3.org/TR/2001/NOTE-wsdl-20010315#_introduction
- http://www.w3.org/TR/soap12-part1/
- http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf
- http://www.ebxml.org/geninfo.htm
- http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.1-spec-os-01-e1.pdf
- http://docs.oasis-open.org/ws-rx/wsrm/200608/wsrm-1.1-spec-cd-04.html
- http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx
- http://www.tiresias.org/research/standards/smartcards.htm#international
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317
- http://www.tiresias.org/research/standards/smartcards.htm#international
- ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system
- ISO/IEC 7812-2:2007 Identification cards -- Identification of issuers -- Part 2: Application and registration procedures
- http://jira.amqp.org/confluence/display/AMQP/AMQP+Specification
- http://www.service-architecture.com/web-services/articles/corba.html
- http://www.omg.org/gettingstarted/orb_basics.htm
- http://www.omg.org/technology/documents/formal/corba_2.htm
- http://www.xmlrpc.com/spec
- http://ietf.org/rfc/rfc5531.txt
- http://www.ansi.org
- http://www.iso.org
- http://www.itil-officialsite.com/home/home.asp
- http://www.oasis-open.org
- http://standards.ieee.org/regauth/posix
- http://www.ietf.org
- http://www.2ab.com/pdf/AccessManagement.pdf
- http://rfc-editor.org/rfc/rfc3360.txt
- http://www.rfc-editor.org/rfc/rfc4359.txt
- http://www.w3.org/PICS/DSig/SHA1_1_0.html
- http://rfc-editor.org/rfc/rfc3851.txt

- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37972
- http://www.rfc-editor.org/rfc/rfc4772.txt
- http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- http://rfc-editor.org/rfc/rfc3360.txt
- http://www.crypto.com/papers/swipe.id.txt
- http://www.rfc-editor.org/rfc/rfc1321.txt
- http://rfc-editor.org/rfc/rfc4962.txt
- http://rfc-editor.org/rfc/rfc1492.txt
- http://www.w3.org/TR/P3P/
- http://saml.xml.org/saml-specifications#samlv11
- http://rfc-editor.org/rfc/rfc4158.txt
- http://rfc-editor.org/rfc/rfc5280.txt
- http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51625
- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1517609
- http://rfc-editor.org/rfc/rfc4303.txt
- http://rfc-editor.org/rfc/rfc4301.txt
- http://www.rfc-editor.org/rfc/rfc3931.txt
- http://www.oasis-pki.org/resources/techstandards/
- http://www.rfc-editor.org/rfc/rfc4251.txt
- http://wp.netscape.com/eng/ssl3/draft302.txt
- http://rfc-editor.org/rfc/rfc5246.txt
- http://www.rfc-editor.org/rfc/rfc4026.txt
- http://www.rfc-editor.org/rfc/rfc2764.txt
- http://www.w3.org/TR/xmldsig-core/
- http://www.oasis-open.org/committees/wss/
- http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html
- http://www.onvif.org/
- http://www.onvif.org/Documents/Specifications/tabid/284/Default.aspx
- http://www.itu.int/rec/T-REC-H.264

pwc.com/india