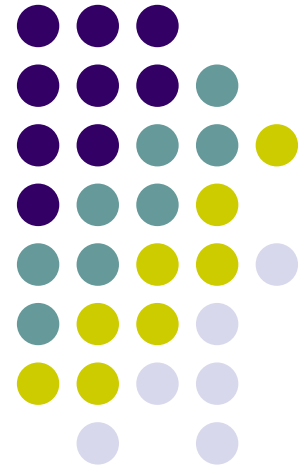


Electronic Transaction Act 2008

Rajesh Kumar Shakya
Chairman, Hitechvalley iNet Pvt. Ltd.
Executive Member, IT Professional Forum (ITPF)
Reengineering Specialist (e-Governance), ADB

NITC/Ministry of Environment, Science and
Technology)
March 15, 2007





Introduction

- Electronic document
 - produced by a computer, stored in digital form. so easy to copy, distribute, retrieve and archive. Ideal for e-commerce and e-governance
- But...
 - It can be deleted, modified and rewritten without leaving a mark
 - Integrity of an electronic document is “genetically” impossible to verify
 - A copy is indistinguishable from the original
 - It can't be sealed in the traditional way, where the author affixes his signature

Creating Trust in Electronic World



Requirements:

- Confidentiality
- Integrity
- Authenticity
- Non-Repudiability

Threat to Authenticity

- Masquerading

Counter Measures

- Digital Signature - Cryptographically generated credentials.

Creating Trust in Electronic World



Enablers:

- Cryptographic technologies
- Supporting Infrastructure:
 - Processes & Systems
 - Legal Frameworks
 - Standards

Electronic Transaction Act 2063 - Role of Comptroller of Certification (CCA) Authority for secure e-Commerce and e-Governance



- Authentication of entities in cyberspace
- Prevention of deliberate or accidental Disclosure and/or Amendment/Deletion of data
- Licensing of CAs and establishment of PKI



Encryption:

- Transformation of data to Prevent information being read by unauthorized parties.
- Sender and Receiver have to know the rules which have been used to encrypt the data.
- Based on Algorithms which are mathematical functions for combining the data with a string of digits called the Key. The result is the encrypted text.

*Eg of **Symmetric Encryption**: Adding a fixed number of characters, say 5, to each character in the message that is being encrypted.*

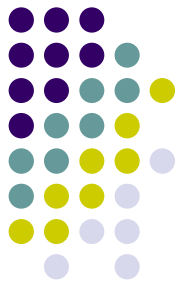
*The word **SECURITY** then becomes the encrypted text **XJHZWNYD***

Public key cryptography (Asymmetric Cryptography)

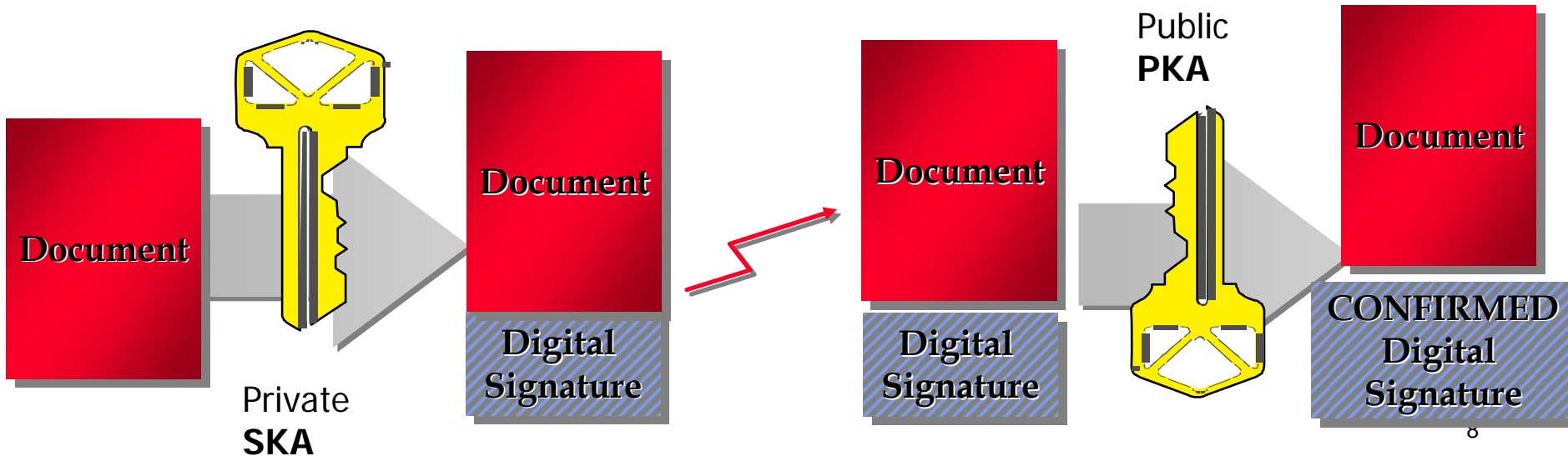


- Each party is assigned a pair of keys –
 - private** - known only by the owner
 - public** - known by everyone
- Information encrypted with the private key can only be decrypted by the corresponding public key & vice versa
- Fulfills requirements of confidentiality, integrity, authenticity and non-repudiability
- ***No need to communicate private keys***

Digital Signature



- ❖ The message is encrypted with the sender's private key
- ❖ Recipient decrypts using the sender's public key



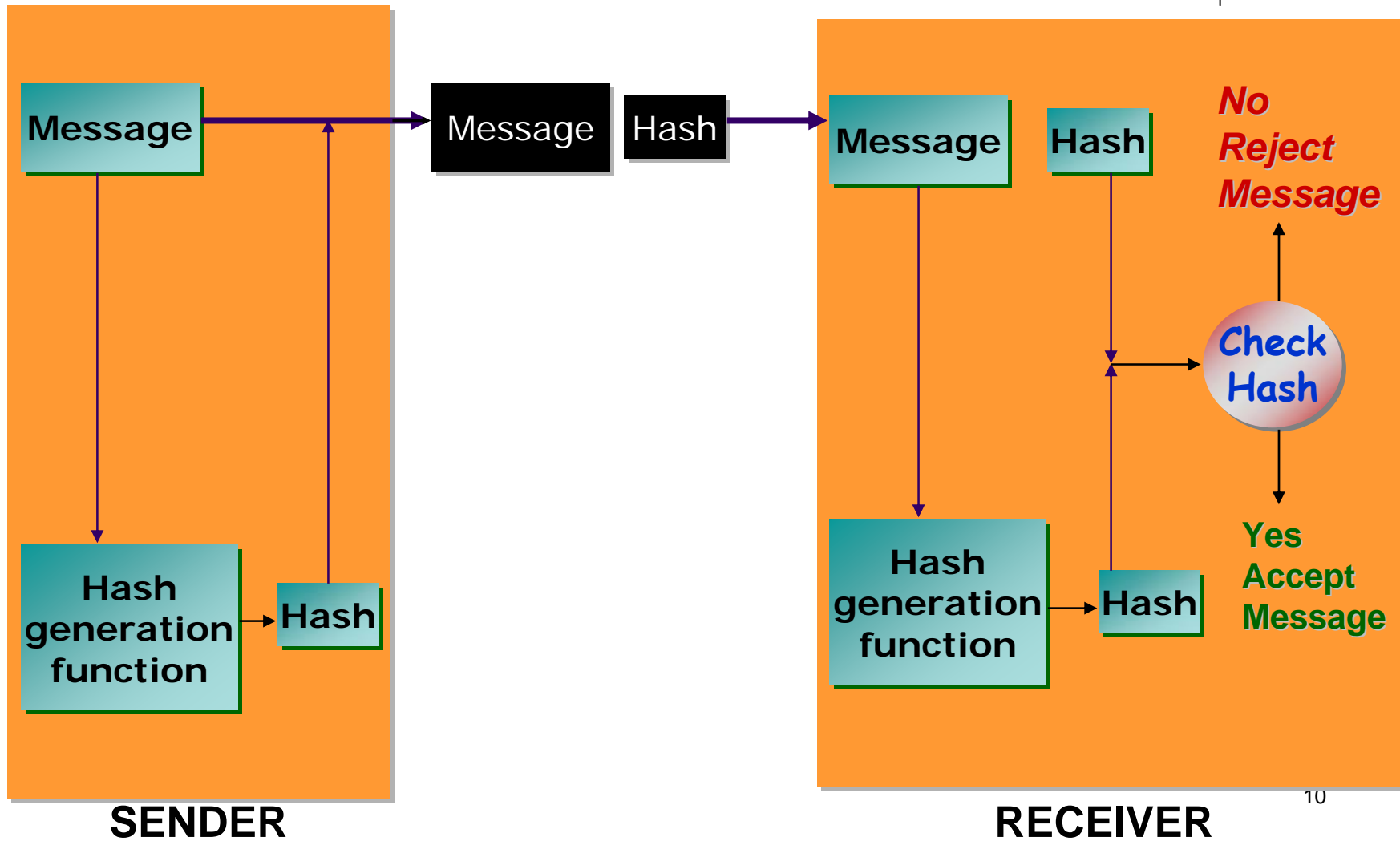


Message Integrity

1. Generating the “Digest” or “Hash” of a message through well-known hash algorithms
 - one-way hash functions
 - original data cannot be generated from hash output
 - No two messages will generate the same hash.
2. Any change in message results in a changed “Hash”
4. SIGN the HASH *NOT* the entire Message



Maintaining Message Integrity

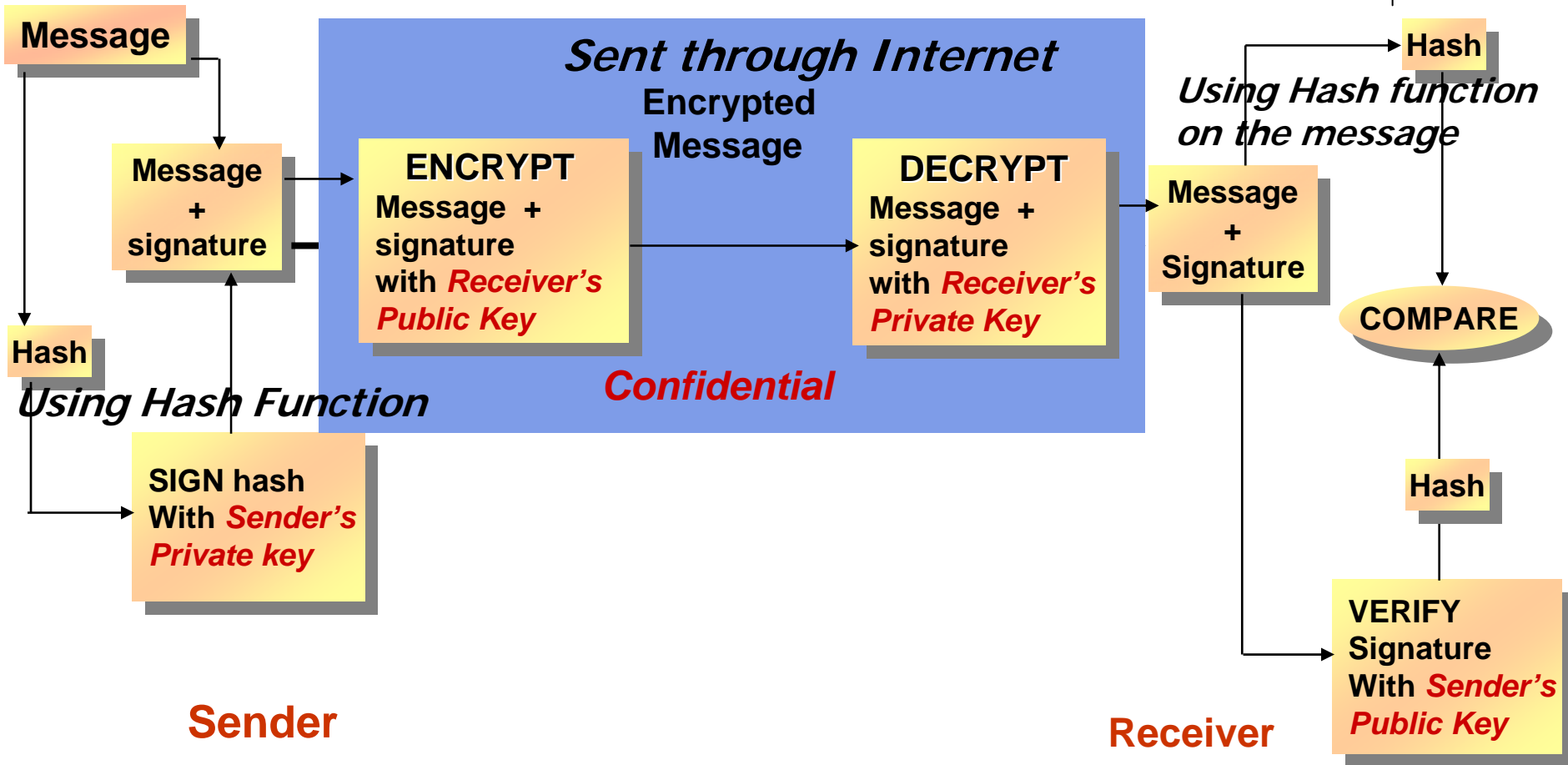


Digital Signature



- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document
 - **Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.**
 - As the public key of the signer is known, anybody can verify the message and the digital signature

Signed *Confidential* Messages





Authenticity and Confidentiality



- A signs message with his own private key
- A then encodes the resulting message with B's Public key
- B decodes the message with his own Private key
- B applies A's Public key on the digital signature



Authenticity and Confidentiality



- When A uses his own private key, it demonstrates that
 - he wants to sign the document
 - he wants to reveal his identity
 - he shows his will to conclude that agreement
- The encoded message travels on the Net, but nobody can read it :
confidentiality



Authenticity and Integrity



- B needs to know that A and only A sent the message
 - B uses A's public key on the signature
 - Only A's public key can decode the message
 - A cannot repudiate his signature
- Digital signature cannot be reproduced from the message
- No one can alter a ciphered message : **INTEGRITY**

Putting it all together



- Digital signatures provide a means of identification that can not be *repudiated*.
- If I encrypt with your public key, only you with your private key can read it
encryption = confidentiality
- If I encrypt with my private key, anyone with my public key can tell it was only me that could have sent it and it has not changed.
digital signature = identity and integrity



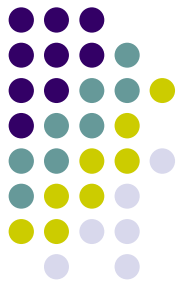
Issues in Public key Cryptosystems

- How will recipient get senders public key?
- How will recipient authenticate sender's public key ?
- How will the sender be prevented from repudiating his/her public key?

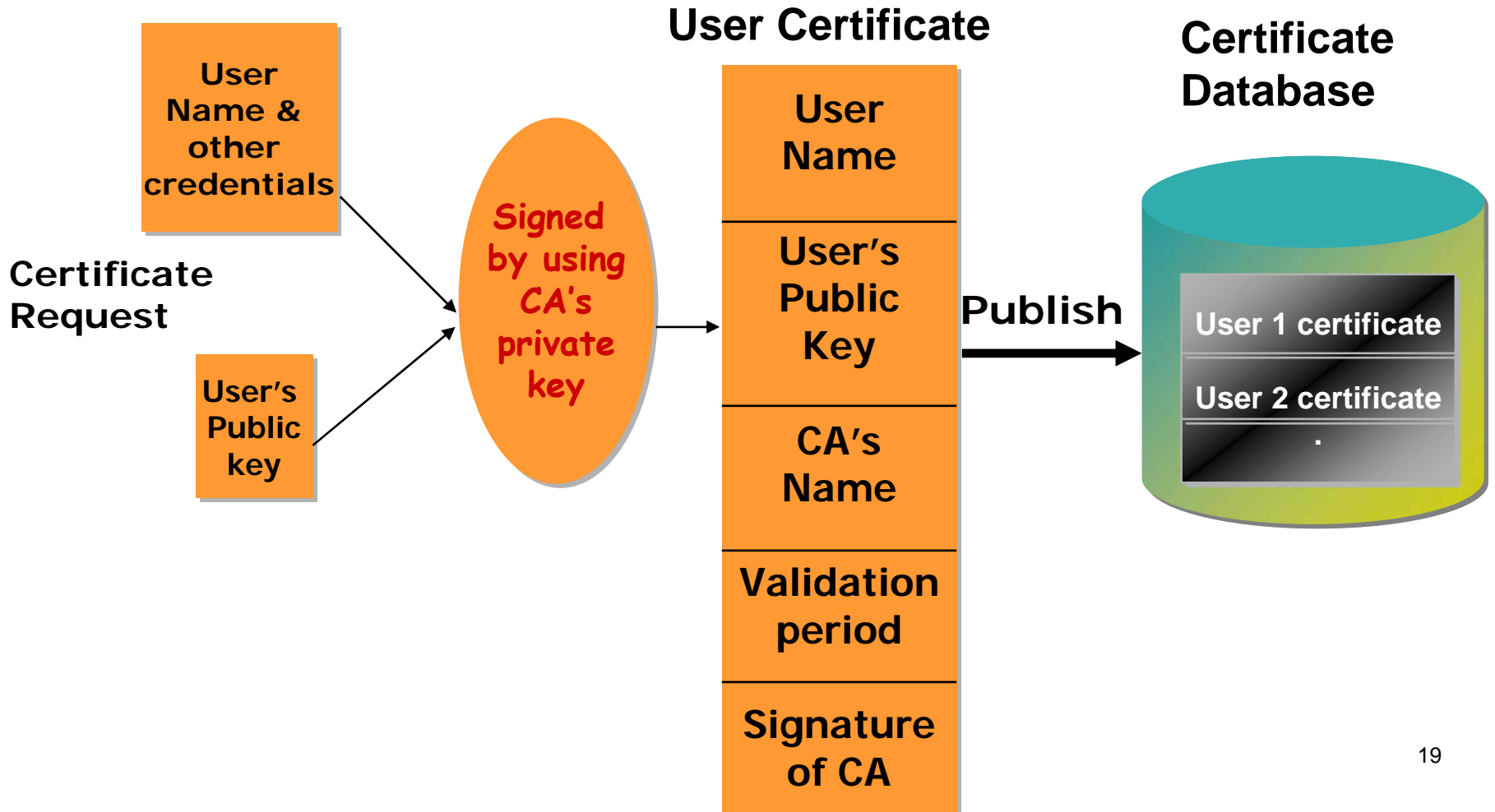


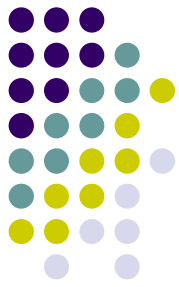
Certifying Authority

- An organization which issues public key certificates.
- Must be widely known and trusted
- Must have well defined methods of assuring the identity of the parties to whom it issues certificates.
- Must confirm the attribution of a public key to an identified physical person by means of a public key certificate.
- Always maintains online access to the public key certificates issued.



Public-Key Certification





Contents of a Public Key Certificate

- Issued by a CA as a data message and always available online
 - **S.No of the Certificate**
 - **Applicant's name, Place and Date of Birth, Company Name**
 - **Applicant's legal domicile and virtual domicile**
 - **Validity period of the certificate and the signature**
 - **CA's name, legal domicile and virtual domicile**
 - **User's public key**
 - **Information indicating how the recipient of a digitally signed document can verify the sender's public key**
 - **CA's digital signature**

Example



Certificate[1]:

Owner: CN=hitechvalley.com, OU=D&AI, O=Hi-tech Valley iNet Pvt. Ltd., ST=Kathmandu, C=NP

Issuer: OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, OU=VeriSign International Server CA - Class 3, OU="VeriSign, Inc.", O=VeriSign Trust Network

Serial number: 50daa4e88174ea478f4cfa312d51887a

Valid from: Fri Feb 13 19:00:00 EST 2004 until: Tue Feb 12 18:59:59 EST 2005

Certificate fingerprints:

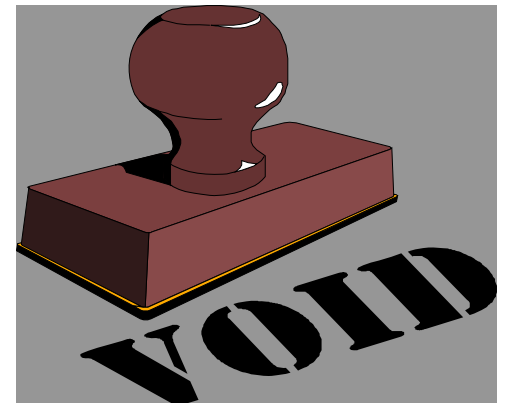
MD5: 38:37:ED:EF:41:2C:DD:12:A6:AB:9B:F9:90:B0:82:37

SHA1: 0:F8:70:7A:8D:66:71:D1:BC:11:D2:41:82:5C:8A:84:91:BE:87:96



Certificate Revocation List

◆ A list of all known Certificates that have been revoked and declared invalid





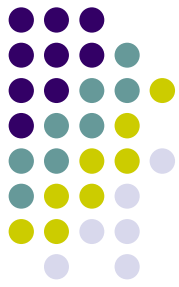
Public Key Infrastructure & the Electronic Transaction Act 2063

Controller of Certifying Authorities as the “Root” Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates

CCA has to regulate the functioning of CAs in the country by-



- Licensing Certifying Authorities (CAs) and exercising supervision over their activities.
- Certifying the public keys of the CAs, i.e. their Digital Signature Certificates more commonly known as Public Key Certificates (PKCs).
- Laying down the standards to be maintained by the CAs,
- Addressing the issues related to the licensing process



The licensing process

- Examining the application and accompanying documents as provided in The Act, and all the Rules and Regulations there- under;
- Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.

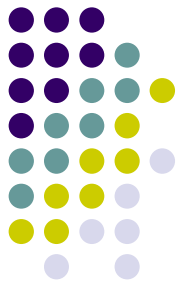


Audit Process

- **Adequacy of security policies and implementation thereof;**
- **Existence of adequate physical security;**
- **Evaluation of functionalities in technology as it supports CA operations;**
- **CA's services administration processes and procedures;**
- **Compliance to relevant process as approved and provided by the Controller;**
- **Adequacy to contracts/agreements for all outsourced CA operations;**
- **Adherence to Electronic Transaction Act 2063, the rules and regulations thereunder, and guidelines issued by the Controller from time-to-time.**

Auditors Panel

- To be nominated by CCA



Thank you

rajesh.shakya@gmail.com

