Public Key Cryptography in India

P.V. Ananda Mohan
***Fellow* IEEE, FNAE, FIETE**
CDAC, Bangalooru

27th November 2014
Bangalore

Digital World

- **A new way of interaction and communication.**
- **e-commerce:** "consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks." (Wikipedia)
- **e-government:** "the use of information and communication technology to provide and improve government services, transactions and interactions with citizens, businesses, and other arms of government." (Wikipedia)

Old World versus New World

- In the conventional world, a commitment is achieved by getting a player to **sign a** statement on a piece of **paper**.
- In the digital world, the same needs to be created (at least, to simulate the conventional world). This gives rise to **digital signatures**.

Two Basic Tasks

- Encryption.
- Authentication.
- **Two basic notions.**
- Conventional or classical notion: secret or symmetric key cryptosystems.
- Paradigm shift: asymmetric key cryptosystem (Diffie-Hellman, 1976).

Asymmetric key cryptosystem

- Public key agreement.
- Public key encryption.
- Digital signature.
- In practice a combination is actually employed.

Indian IT Act, 2000, 2006

- Provides legal sanctity to digital signatures based upon the
- principle of equivalence to handwritten signatures.
- Provides for the creation and management of PKI in India.

Indian IT Act, 2000, 2006

- Cascaded amendments to several other acts.
- Indian Evidence Act, 1872.
- Banker's Book Evidence Act, 1891.
- Reserve Bank of India Act, 1934.
- Indian Penal Code.
- Covers aspects other than digital signatures.
- Issues related to digital distribution of obscenity.
- Issues related to wire-tapping by governmental agencies.

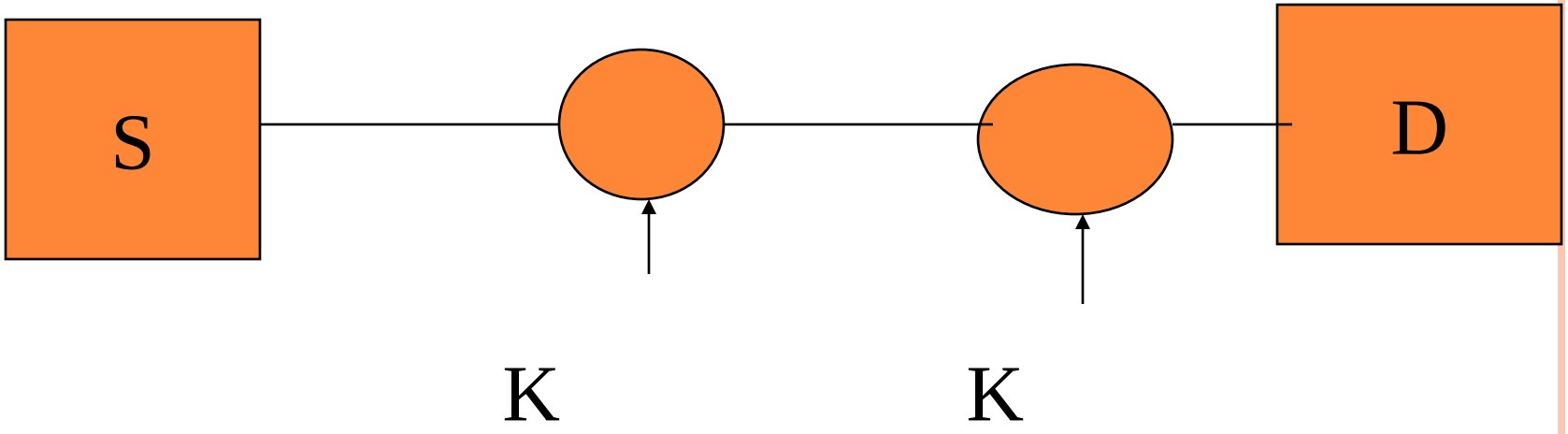
IT Act History

- IT Act 2000
- IT Act Amendment(2008)
- Modifications in Other Act's

Guidelines issued by CCA

- OID (object Identifier)
- Audit Frequency
- Storage of Private key
- India PKI CP Ver 1.1
- DSC (digital Signature Certificate) Interoperability Guidelines
- NRDC (national repository of Digital Signatures) Submission
- Site preparation guidelines

Encryption and authentication

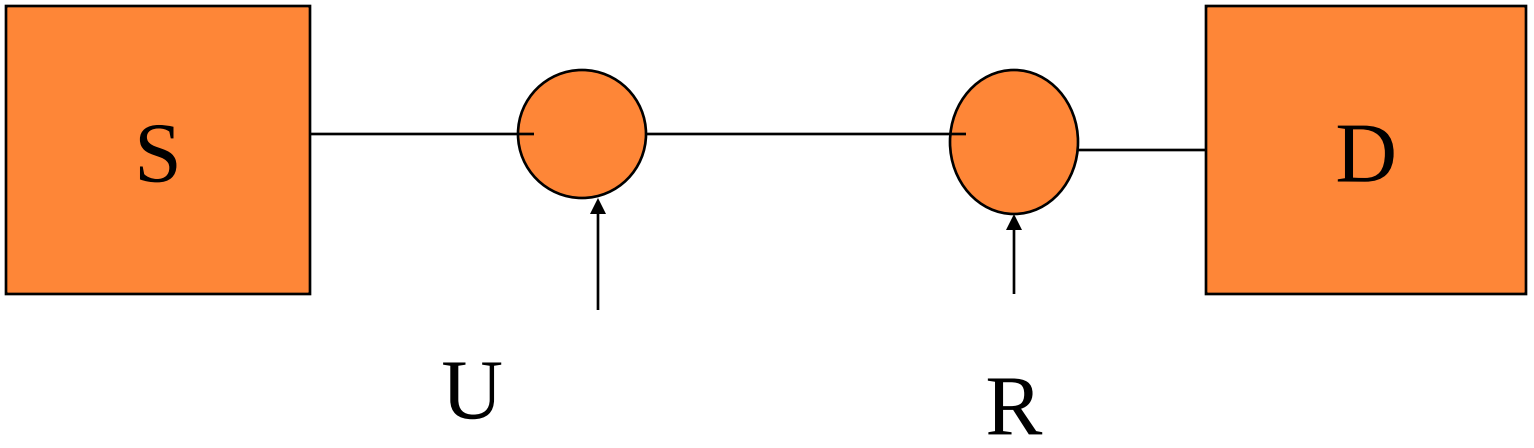


CONVENTIONAL ENCRYPTION

Encryption and authentication

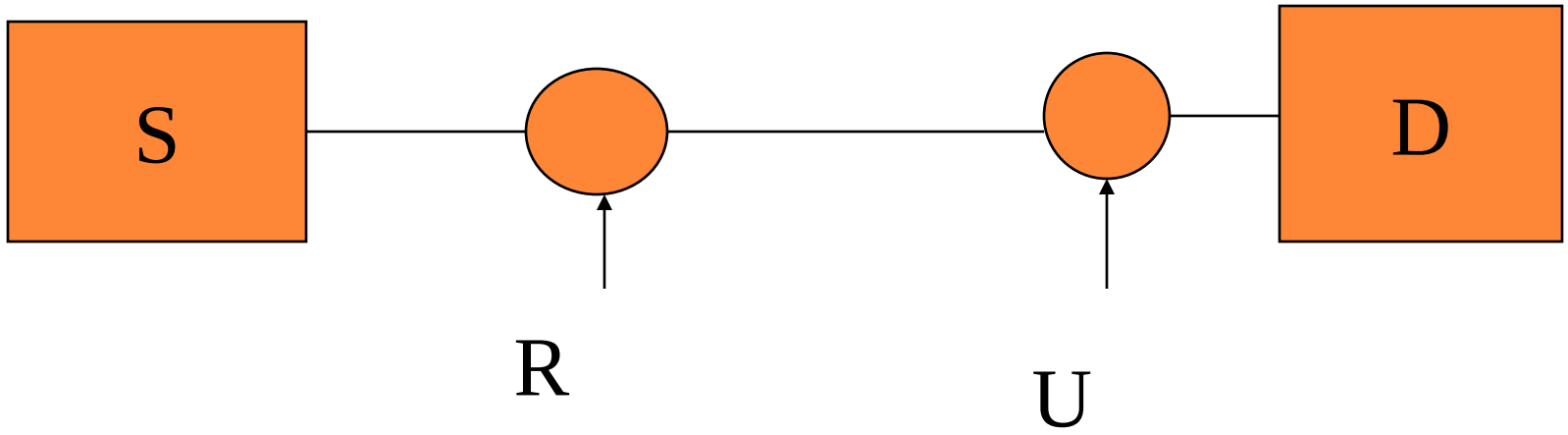
U stands for Public

R stands for Private



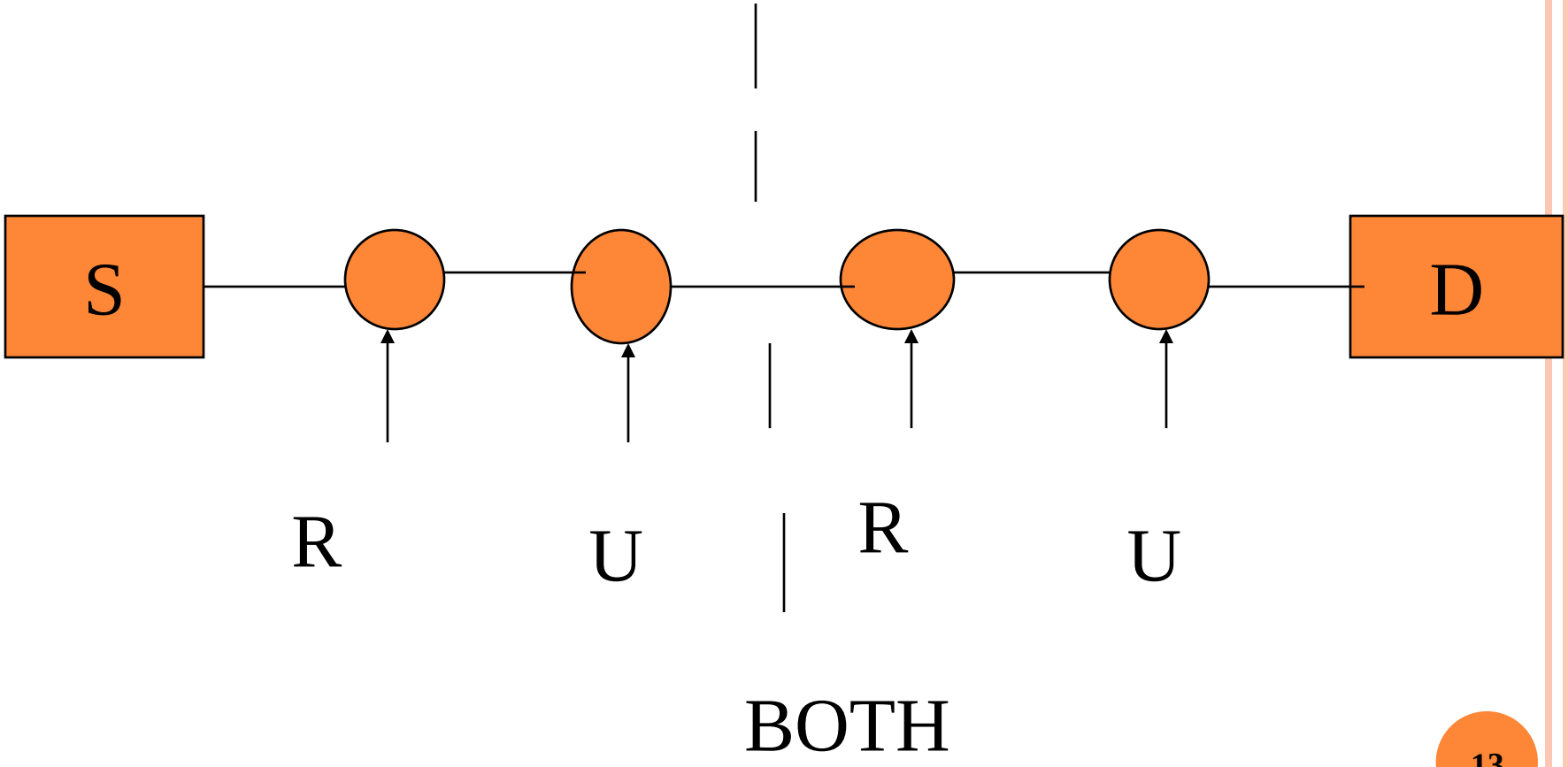
CONFIDENTIALITY

Encryption and authentication

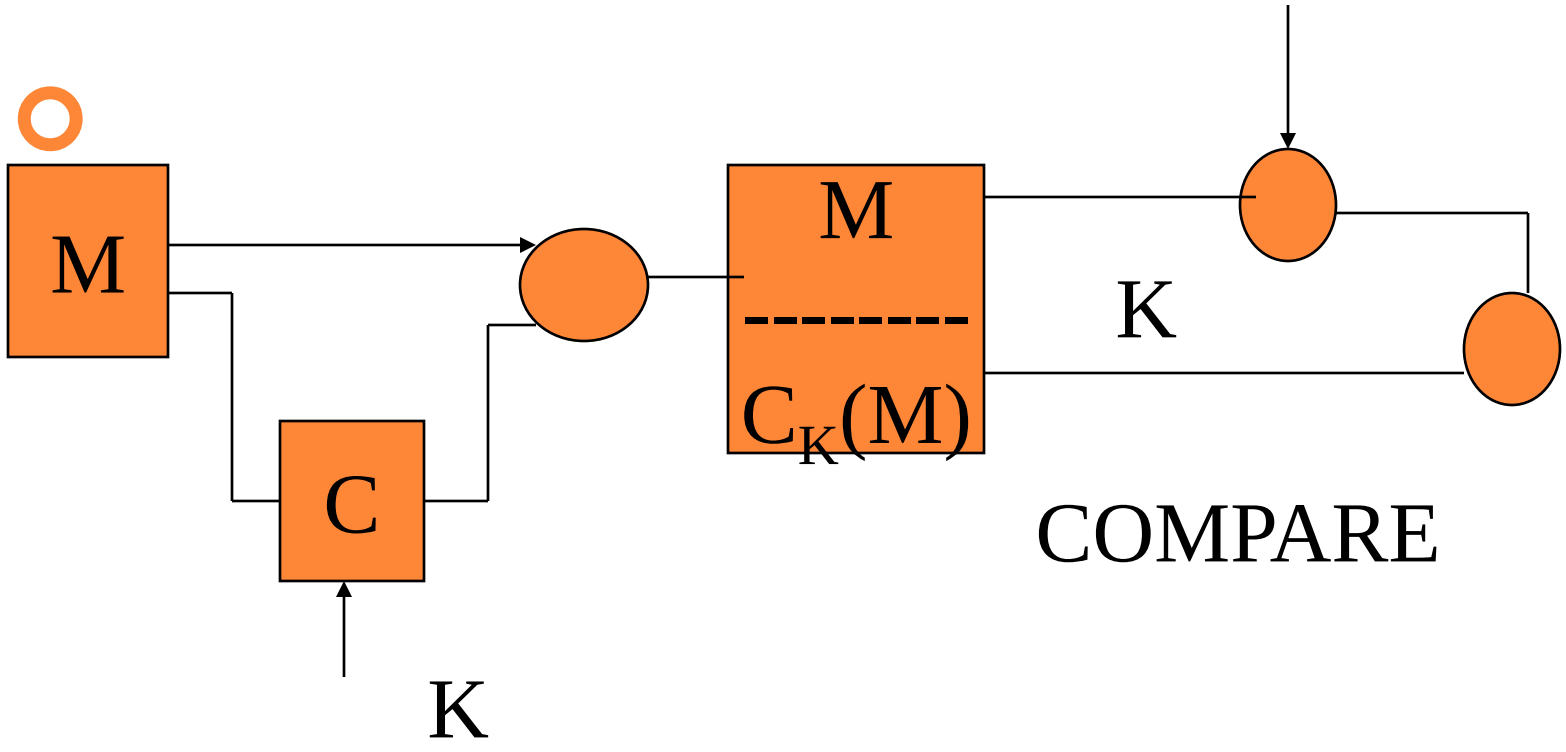


AUTHENTICATION

Encryption and authentication



Authentication by digital signatures

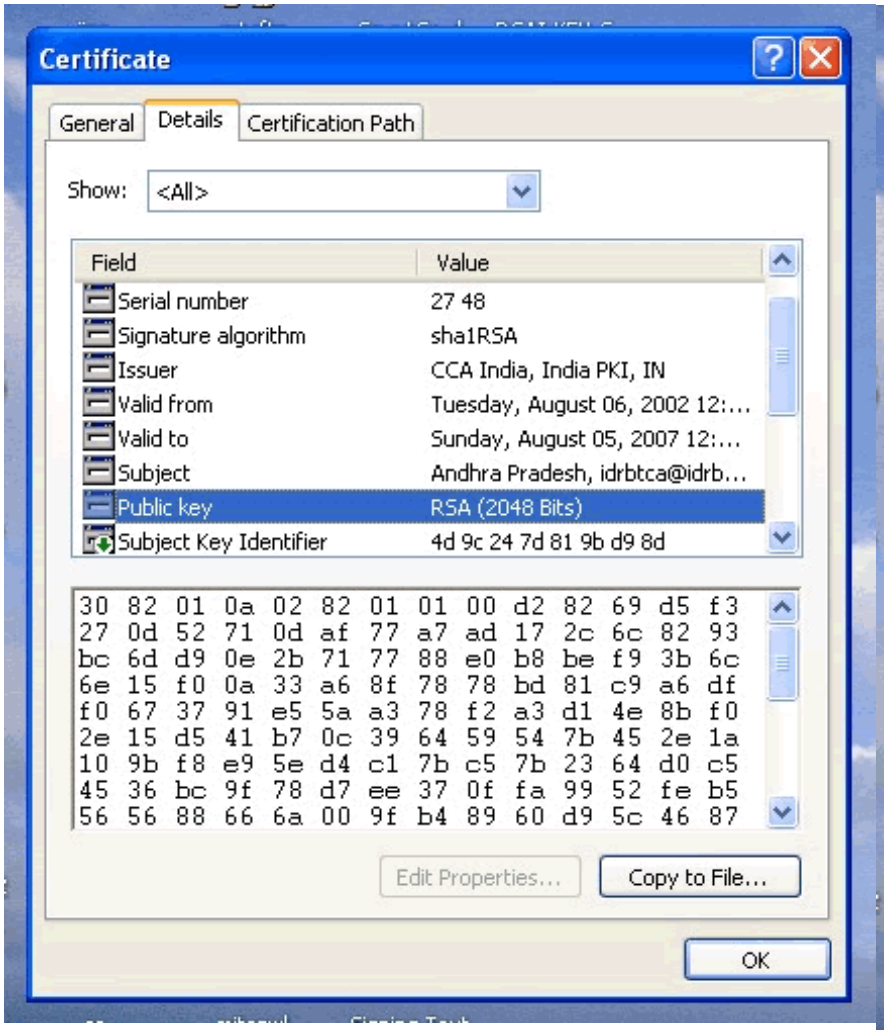


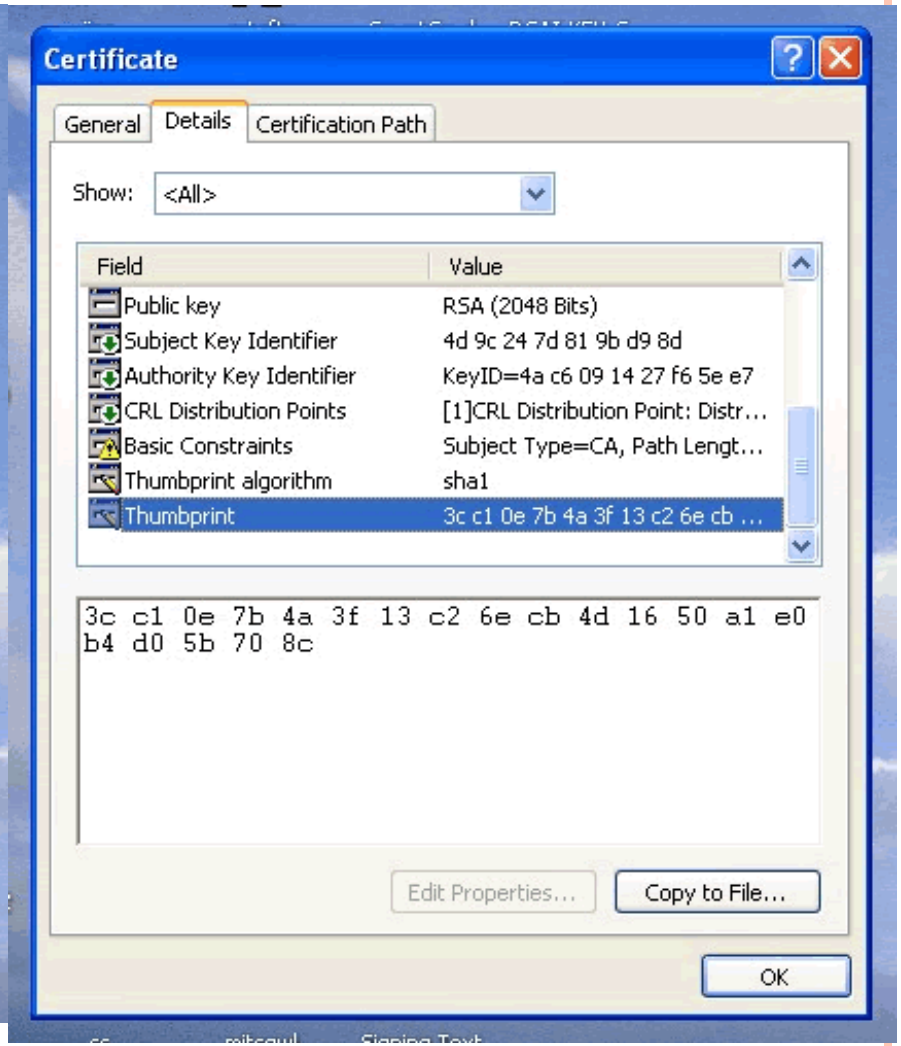
Certifying Authority

- A CA has a key pair (*pkC*, *skC*).
- Bob obtains certificate.
- Bob generates (*pkB*, *skB*); sends *pkB* to CA.
- CA signs (Bob, *pkB*) using *skC* to obtain *B*;
- Bob's certificate: (Bob, *pkB*, *B*).
- Alice verifies (*M*,) signed by Bob.
- Verifies (Bob, *pkB*, *B*) using *pkC*.
- Verifies (*M*,) using *pkB*.
- **Trust:**
- Alice trusts *pkC*;
- hence, Alice trusts *pkB*.

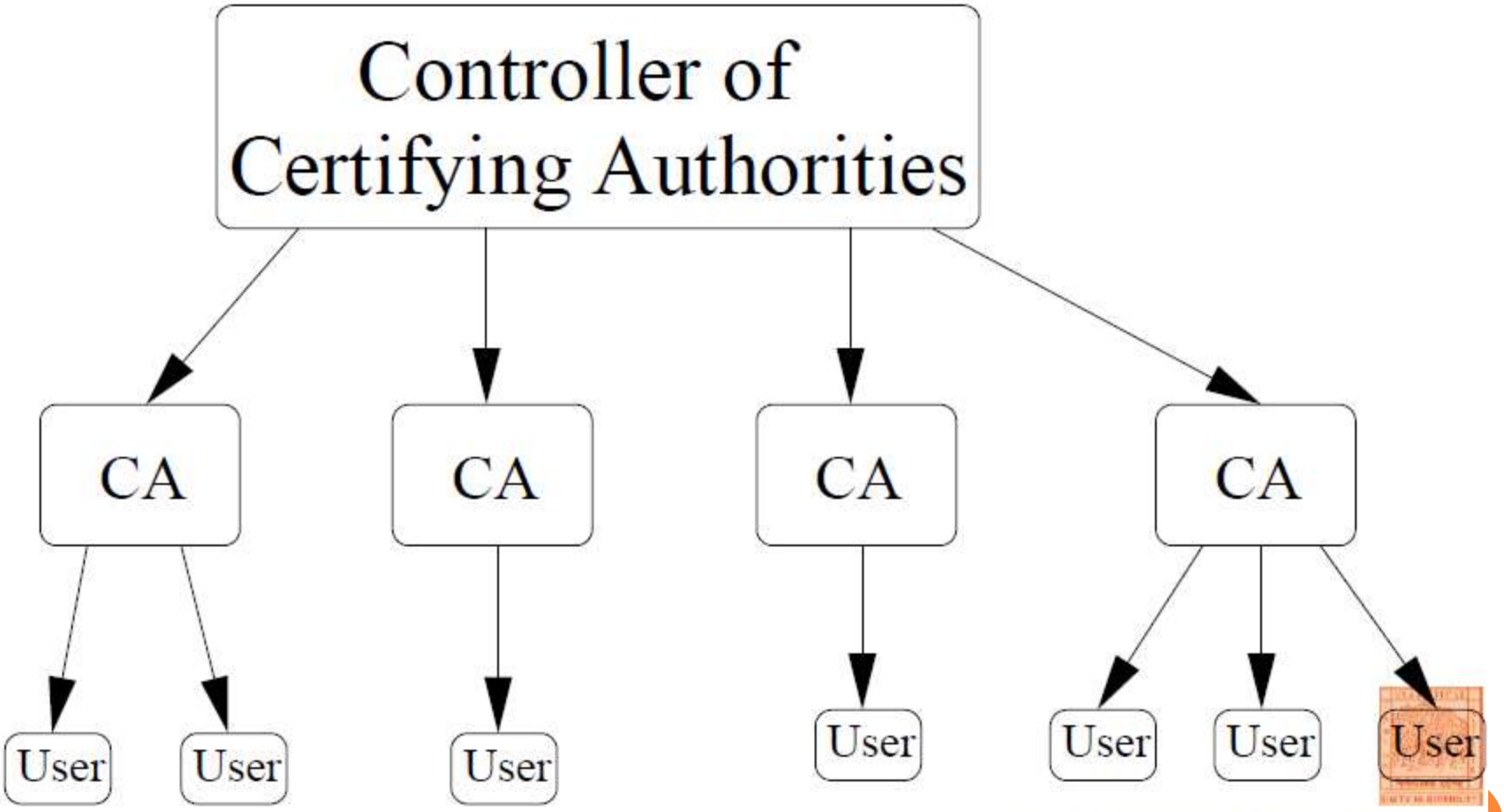
X.509 Certificate Format

- version number
- serial number
- signature algorithm ID
- issuer name
- validity period
- subject name (i.e., certificate owner)
- certificate owner's public key
- optional fields
- the CA's signature on all previous fields


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Serial number
27 48
Signature algorithm
sha1RSA
Issuer
CCA India, India PKI, IN
Valid from
Tuesday, August 06, 2002 12:...
Valid to
Sunday, August 05, 2007 12:...
Subject
Andhra Pradesh, idrbtca@idrb...
Public key
RSA (2048 Bits)
Subject Key Identifier
4d 9c 24 7d 81 9b d9 8d
30 82 01 0a 02 82 01 01 00 d2 82 69 d5 f3
27 0d 52 71 0d af 77 a7 ad 17 2c 6c 82 93
bc 6d d9 0e 2b 71 77 88 e0 b8 be f9 3b 6c
6e 15 f0 0a 33 a6 8f 78 78 bd 81 c9 a6 df
f0 67 37 91 e5 5a a3 78 f2 a3 d1 4e 8b f0
2e 15 d5 41 b7 0c 39 64 59 54 7b 45 2e 1a
10 9b f8 e9 5e d4 c1 7b c5 7b 23 64 d0 c5
45 36 bc 9f 78 d7 ee 37 0f fa 99 52 fe b5
56 56 88 66 6a 00 9f b4 89 60 d9 5c 46 87
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Public key
RSA (2048 Bits)
Subject Key Identifier
4d 9c 24 7d 81 9b d9 8d
Authority Key Identifier
KeyID=4a c6 09 14 27 f6 5e e7
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Basic Constraints
Subject Type=CA, Path Lengt...
Thumbprint algorithm
sha1
Thumbprint
3c c1 0e 7b 4a 3f 13 c2 6e cb ...
3c c1 0e 7b 4a 3f 13 c2 6e cb 4d 16 50 a1 e0
b4 d0 5b 70 8c
Edit Properties...
Copy to File...
OK

A Three–Level Hierarchy



Functions of the CCA

- Creation and maintenance of the Root CA of India (RCAI).
  - Root CA certificate is a self-signed certificate. It is based on the ITU-T X.509 standard.
  - Protection of private key of CCA (using tamper proof hardware and 3-out-of-3 access control).
- Issue certificates to individual CAs.
- Maintain the national repository of digital certificates (NRDC) (mandated under Section 20 of the IT Act): copies of all certificates and certificate revocation lists.
- Empanel auditors for auditing infrastructure of CAs.
- Generally act as the controlling authority of all PKI-related issues in India.

Standards Notified in India

- **Internet Engineering Task Force (IETF):** Internet X.509 Public Key Infrastructure.
- **IEEE standard P1363 for three families:** Discrete Logarithm (DL) systems; Elliptic Curve Discrete Logarithm (EC) systems; Integer Factorization (IF) systems.
- **Public-key Cryptography Standards (PKCS):** numbers 1,3,5,6,7,8,9,10,11,12,13 and 15.
- **Federal Information Processing Standards (FIPS):** FIPS 180-1, Secure Hash Standard; FIPS 186-1, Digital Signature Standard (DSS). FIPS 140-1 level 3, Security Requirement for Cryptographic Modules.
- **Discrete Logarithm (DL) systems:** Diffie-Hellman, MQV key agreement; DSA, Nyberg-Rueppel signatures.

- **Elliptic Curve (EC) systems:** elliptic curve analogs of DL systems.
- **Integer Factorization (IF) systems:** RSA encryption; RSA, Rabin-Williams signatures.
- **Key agreement schemes.**
- **Signature schemes:** DL/EC scheme with message recovery; PSS, FDH, PKCS #1 encoding methods for IF family; PSS-R for message recovery in IF family.
- **Encryption schemes:** Abdalla-Bellare-Rogaway DHAES for DL/EC family.

Rules Governing Key Pairs

- **CA:** at least 2048-bit RSA keys;
- **users:** at least 1024-bit RSA keys.
- CA has to change key pair every 3 to 5 years as per certificate
- practice statement (CPS) guidelines.
- Subscriber's key pair should be changed every 1 to 2 years.

ECC Guidelines Issued In November 2013 for public Scrutiny

Security Strength (symmetric key)	RSA key size	Equivalent ECC Key Size
112	2048	224
128	3072	256
192	7680	384
256	15360	512

RFC 5753

Curves	EC Key Size	Message digest Algorithms
P-224	224	SHA-256
P-256	256	SHA-256
P-384	384	SHA-384
P-521	512	SHA-512

CAs in India

- **Safescrypt:** private sector.
- **IDRBT:** issues certificates to the banking sector.
- **National Informatics Centre:** issues certificates to the
- government sector.
- **TCS:** private sector.
- **Customs and Central Excise:** government department.
- **MTNL:** telecom sector.
- **GNFC, (n)Code:** private sector.
- **e-Mudhra:** private sector.

Applications where already used.

- E-Procurement.
- Financial Services.
- Stock exchanges.
- Banking Services.
- Government.
- e-Payment System: Government of India
- e-Governance in India

Applications in Judiciary

1. Instant posting of judgment on the web.
2. Secured electronic communications within judiciary
3. Authentic archiving of Judicial records
4. Submission of affidavits
5. Giving certified copies of the Judgment

Applications in Telecommunications

- Subscriber's services management
  - STD/ISD, Opening, Closing, Initializing Password
- Shifting of telephones, Accessories (Clip, Cordless)
- Small Payments through telephones bills
  - Books, gifts, Internet purchases
- Mobile Authentication of SMS
  - Share market trading, Intra/Inter office instructions
- Mobile Phones as Credit cards
  - Mobile operator can venture into credit card business

Applications in Telecommunications *(contd.)*

B. Internal
   - Intra/Inter offices authentic communications
     - OBs, approvals, Instructions, requests
   - Procurement of material
     - Calling/Receiving bids, Purchase orders, Payment instructions
   - Network Management functions
     - Change of configuration, Blocking/unblocking routes

E-Governance

- Empowering Citizens
  a) Transparency
  b) Accountability
  c) Elimination of Intermediatory
  d) Encouraging Citizens to exercise their Rights

GOVERNMENT ONLINE

1. Issuing forms and licences
2. Filing tax returns online
3. Online Government orders/treasury orders
4. Registration
5. Online file movement system
6. Public information records
7. E-voting
8. Railway reservations & ticketing
9. E-education
10. Online money orders

Thank You