

Digital Signatures and PKI

Dr. Balaji Rajendran

Centre for Development of Advanced Computing (C-DAC)

Bangalore

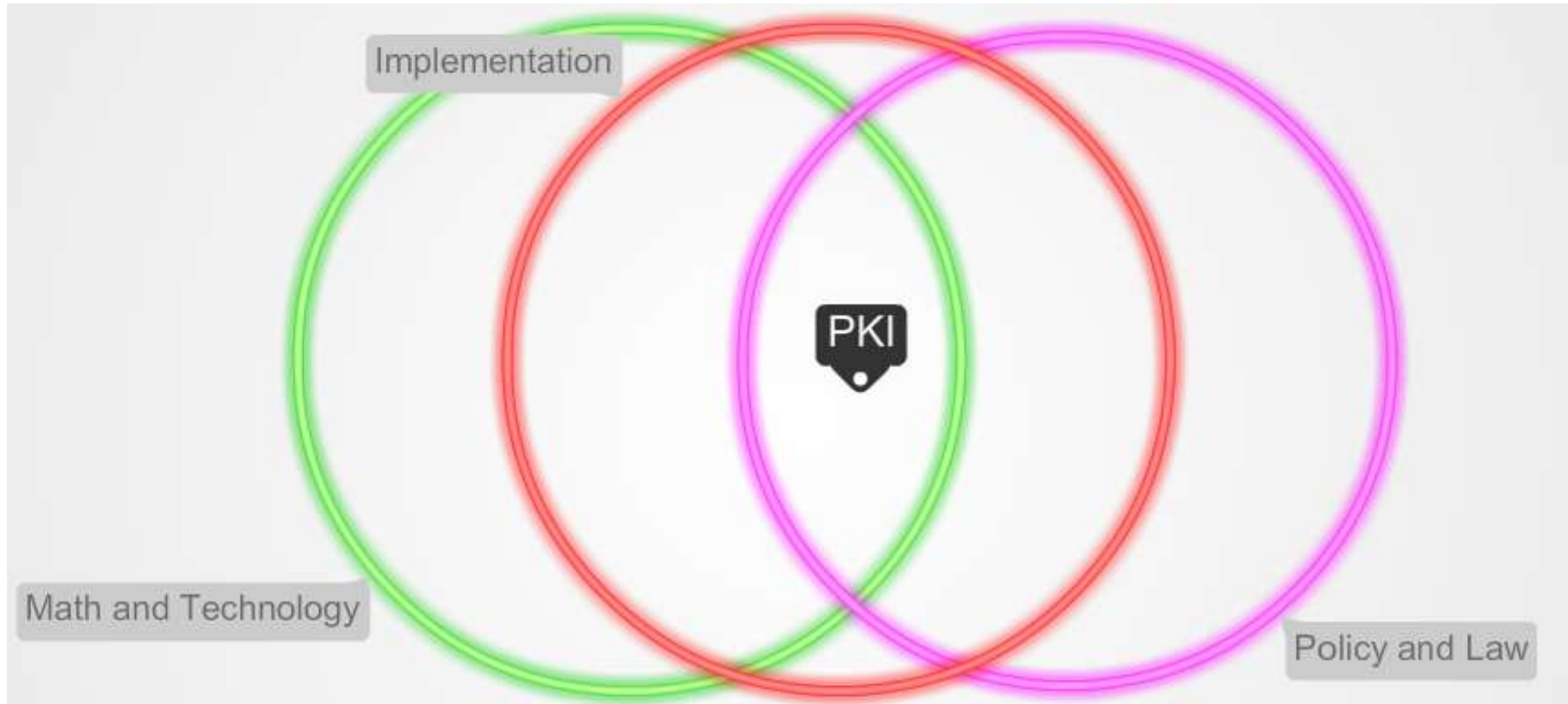
Under the Aegis of

Controller of Certifying Authorities (CCA)

Government of India

15th July 2014

- ✓ Dimensions of PKI
- ✓ Paper World Vs Electronic World
- ✓ Why Digital Signature?
- ✓ What is Digital Certificate?
- ✓ What is Digital Signature?
- ✓ Certificate Classes
- ✓ How to get DSC?
- ✓ Risks and Precautions with DS
- ✓ Legal Aspects of DSC
- ✓ Present Scenario in India

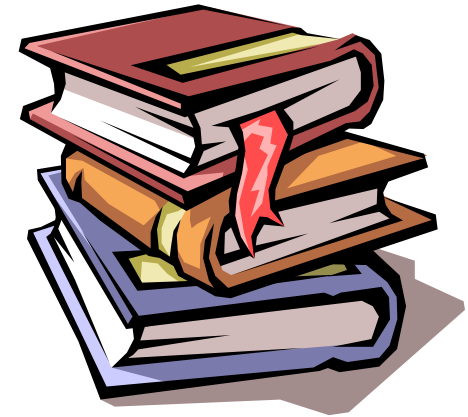


Technology Perspective

Paper Records v/s Electronic Records

Paper Records v/s Electronic Records

	Paper Record	Electronic Record
Document Form	Physical	Digital
Very easy to make copies	No	Yes
Very fast distribution	No	Yes
Archival and Retrieval	Challenging	Easy
Copies are as good as original	No. Copies are easily distinguishable	Yes
Easily modifiable	No	Yes
Environmental Friendly	No	Yes





For trust worthiness in Transactions



The following properties must be assured:

Privacy (Confidentiality): Ensuring that *only Authorized persons* should read the *Data/Message/Document*

Authenticity: Ensuring that *Data/Message/Document* are genuine

Integrity : Ensuring that *Data/Message/Document* are unaltered by unauthorized person during transmission

Non-Repudiation: Ensuring that one party of a transaction cannot deny having sent/received a transaction

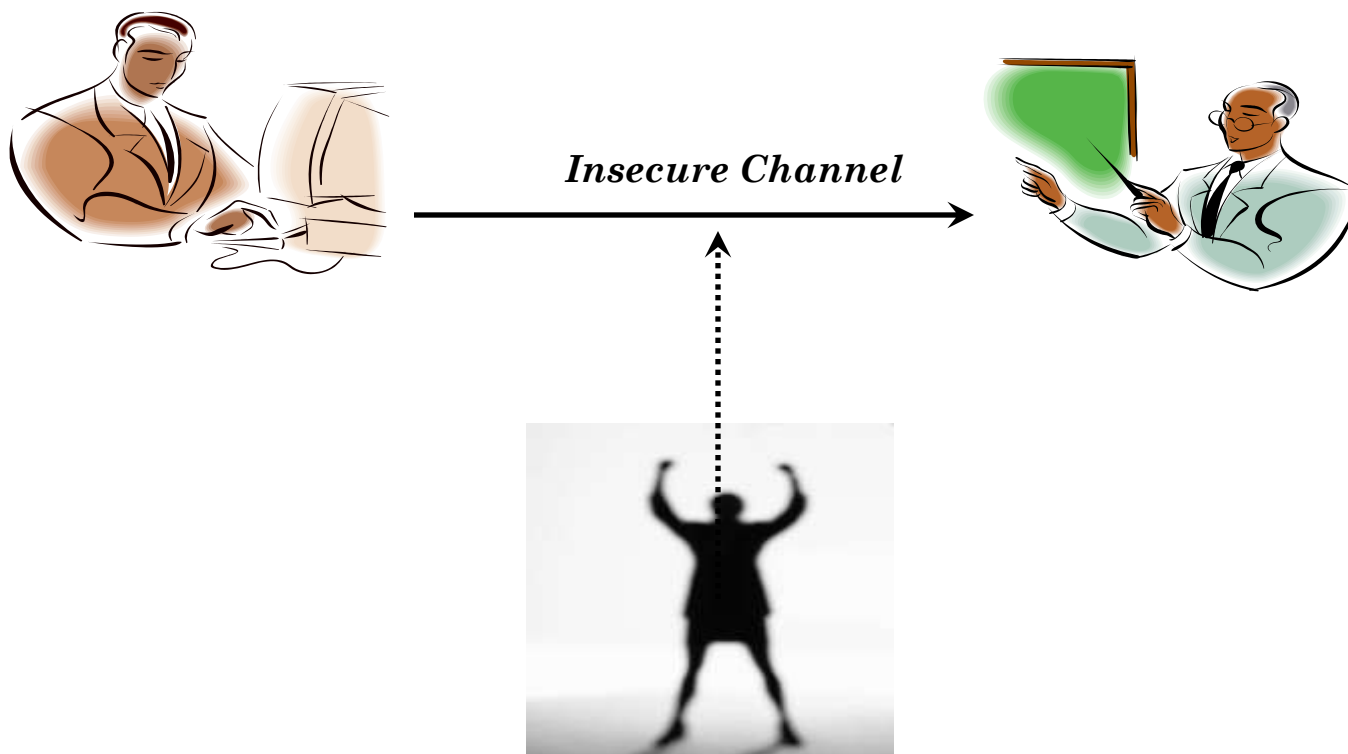


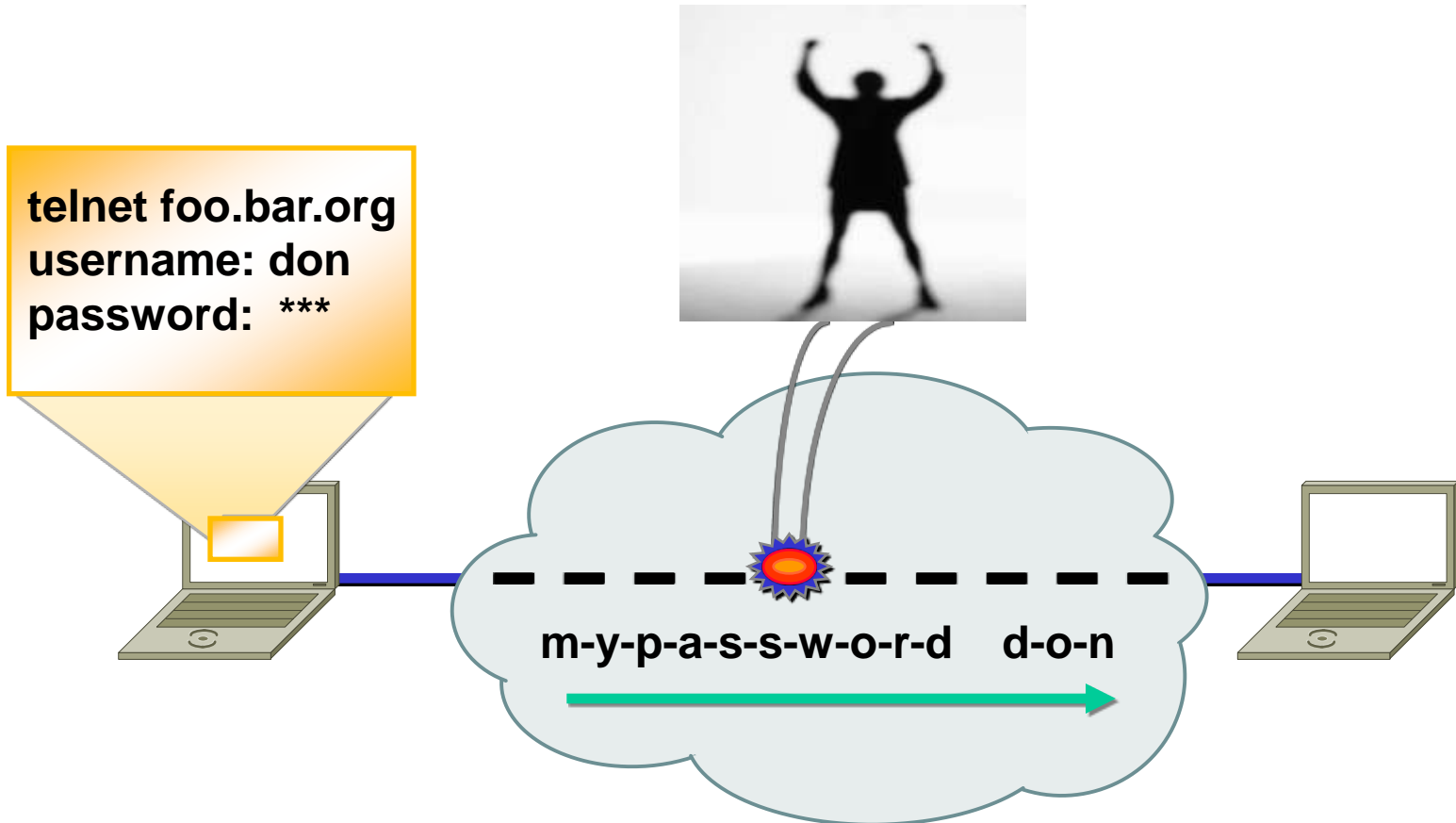
Paper Records v/s Electronic Records



	Paper Record	Electronic Record
Privacy (Confidentiality)	Sealed Envelope	Digital Envelope
Authenticity	Hand Signature	Digital Signature
Integrity	Hand Signature	Digital Signature
Non-Repudiation	Hand Signature but it is Challenging	Digital Signature

The Scenario



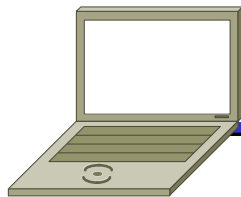


Breach of Confidentiality

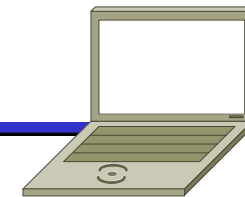
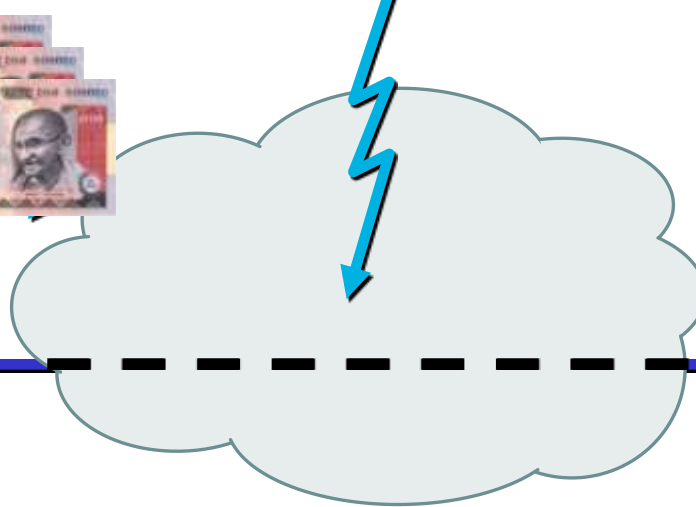
Deposit 1,00,000
in Veeru's Account



Deposit 99,990 in Gabbar's
Account and 10 in Veeru's
Account



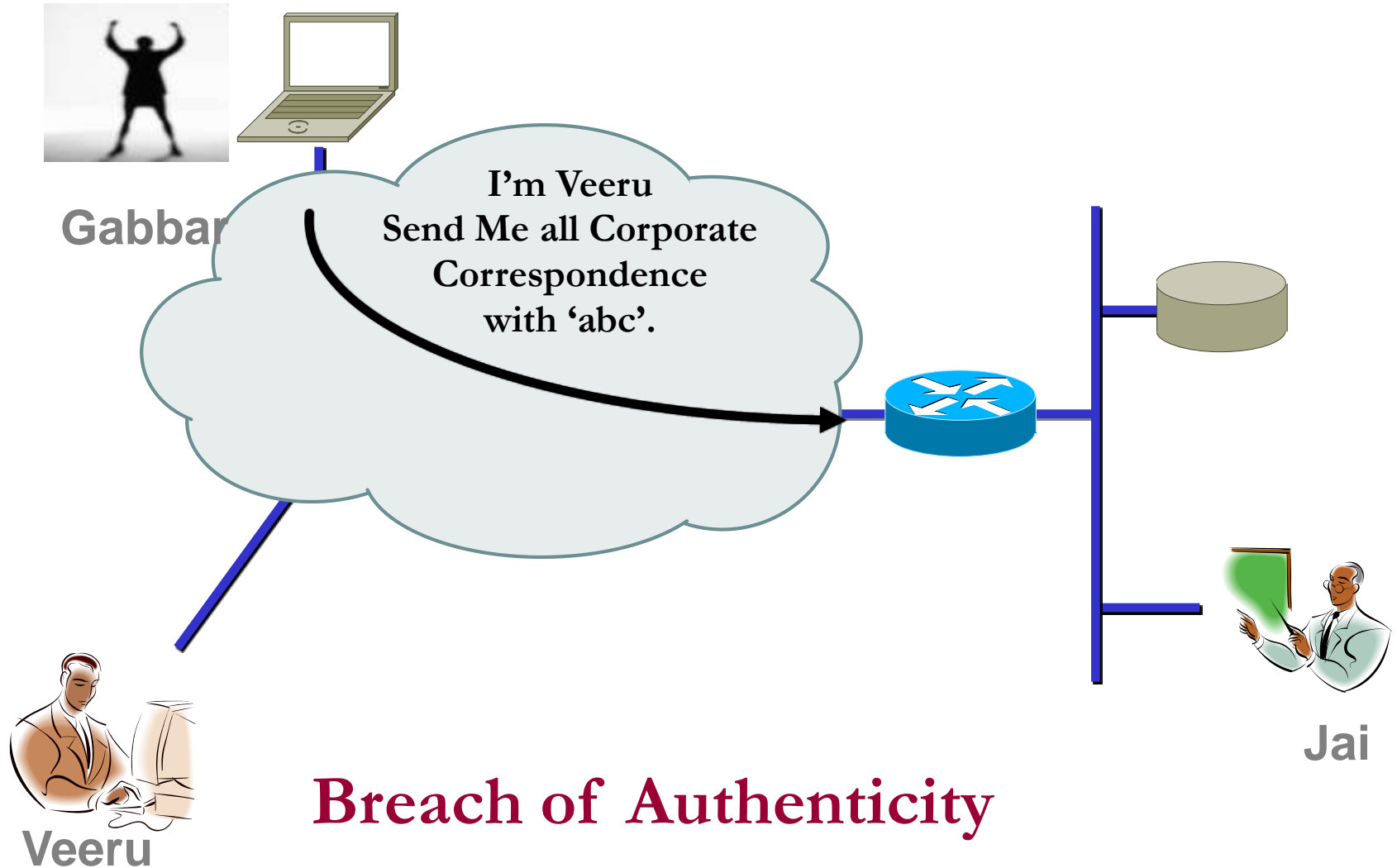
Customer



Bank

Breach of Integrity

Threats: Spoofing



Why Digital Signature?

Why Digital Signatures?

- To provide **Authenticity, Integrity and Non-repudiation** to electronic documents
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance



Mathematical Perspective

- Major cryptographic components for creating Digital Signature are:
 - Hash Functions
 - Asymmetric Key Cryptography
-

- A hash function is a cryptographic mechanism that operates as one-way function
 - Creates a digital representation or "fingerprint" (Message Digest)
 - Fixed size output
 - Change to a message produces different digest

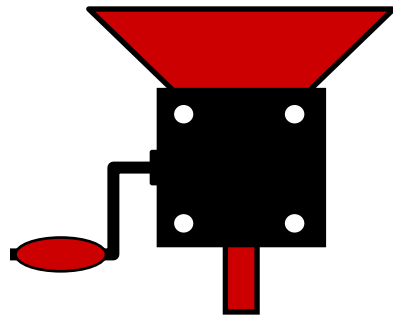
Examples : MD5 , Secure Hashing Algorithm (SHA)

Hash - Example

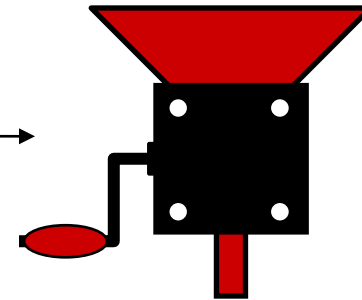
Hi Jai,
I will be in the park at
3 pm
Veeru

Message

Hi Jai,
I will be in the park at
8 pm
Veeru



← Hash Algorithm →



Message Digest

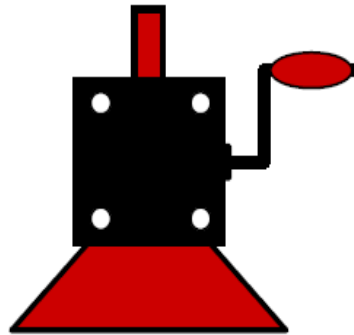
cfa2ce53017030315fde705b9382d9f4

d4216ytf6b9385fe502b165dfe8cec17

Digests are Different

Hash – One-way

cfa2ce53017030315fde705b9382d9f4



Hi Jai
I will be in the park at
3 pm
Veeru

MD5 and SHA

Message

Hi Jai,
I will be in the
park at 3 pm
Veeru

MD5

Message Digest

cfa2ce53017030315f
de705b9382d9f4

128 Bits

Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-1

1f695127f210144329ef
98e6da4f4adb92c5f18
2

160 Bits

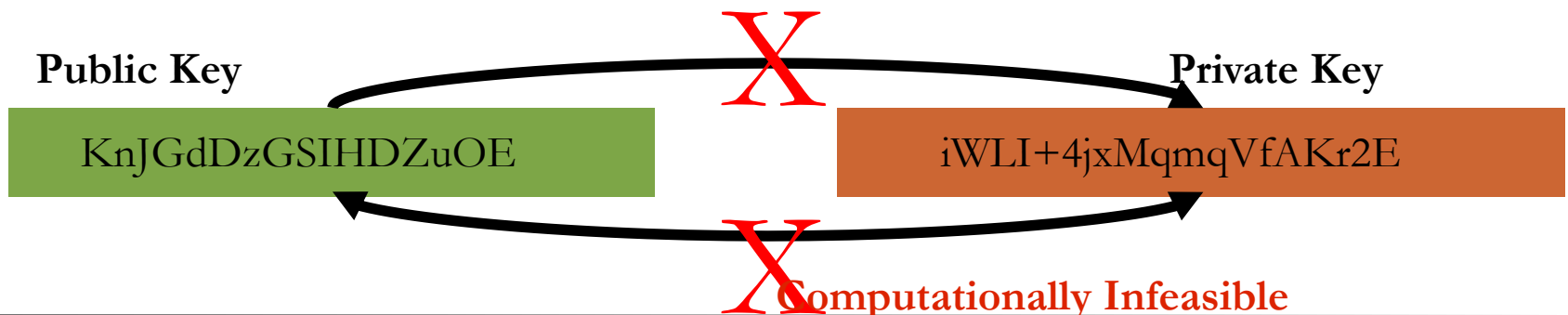
Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-2

2g5487f56r4etert654tr
c5d5e8d5ex5gttahy55e

224/256/384/512

- Also called as Public Key Cryptography
- Uses a related key pair wherein one is Private key and another is Public key
 - One for encryption, another for decryption
- Knowledge of the *encryption* key doesn't give you knowledge of the *decryption* key
- A tool generates a related key pair (public & private key)
 - Publish the public key in a directory






RSA Key pair

(including Algorithm identifier) [2048 bit]



Private Key

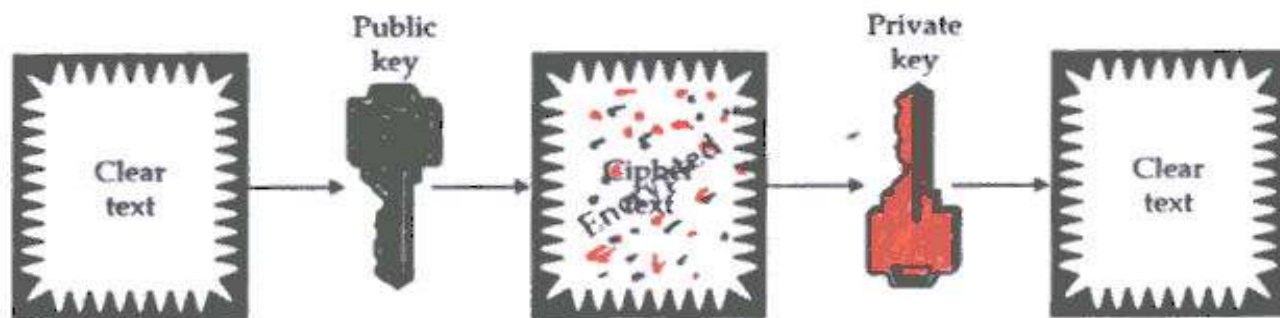


```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83
463d e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc
b055 9653 8466 0500 da44 4980 d854 0aa5 2586 94ed 6356 ff70 6ca3
a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1 463d 1ef0 b92c 345f
8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f
5a22 97ec 199b c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95
9c39 0a8a cf42 b2f0 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93 a9d3
7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced 9cbb f2cb
5b10 f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742
859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04e3 459e
a146 2840 8102 0301 0001
```

Public Key

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d
e493 bab6 0673 0d59 bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653
8466 0500 da44 4980 d8b4 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68
2a44 5e2f cfcc 185e 47bc 3ab1 463d 1df0 b92c 345f 8c7c 4c08 299d 4055
eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd
e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca
da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559
b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90
bcff 9634 04de 45de af46 2240 8410 02f1 0001
```

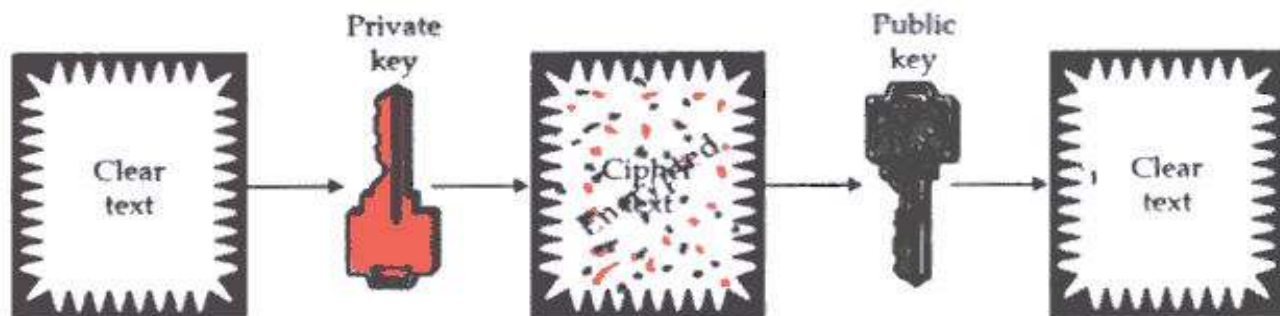




Works!



सी डैक
CDAC



Fails!



Matrix of Knowledge of Keys

Key details	<i>A</i> should know	<i>B</i> should know
A's private key	Yes	No
A's public key	Yes	Yes
B's private key	No	Yes
B's public key	Yes	Yes

Implementation Perspective

Digital Signature



Hand Signature vs Digital Signature



- A *Hand Signature* on a document is
 - a unique pattern dependant on some secret known only to the signer and
 - **Independent of the content** of the message being signed
 - A *Digital signature* of a message is
 - **a number** dependent on some secret known only to the signer and
 - **Dependent on the content** of the message being signed
 - Signatures must be verifiable
 - Applications
 - Authentication,
 - Data Integrity
 - Non-repudiation
-

What is 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





Creating Digital Signature



- Key pairs of every individual
 - *Public key*: known to everyone
 - *Private key*: known only to the owner
 - To *digitally sign* an electronic document the signer uses his/her *Private key*
 - To *verify* a digital signature the verifier uses the signer's *Public key*
-

Digital Signing – Step 1

This is an example of
how to create a
message digest and
how to digitally sign a
document using
Public Key
cryptography

Hash

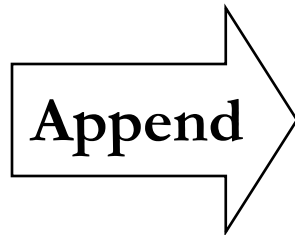
Message
Digest

Digital Signing – Step 2



Digital Signing – Step 3

Digital
Signature



This is an example of
how to create a
message digest and
how to digitally sign a
document using
Public Key
cryptography

Digital
Signature

This is an example of how to create a message digest and how to digitally sign a document using Public Key cryptography

Digital
Signature

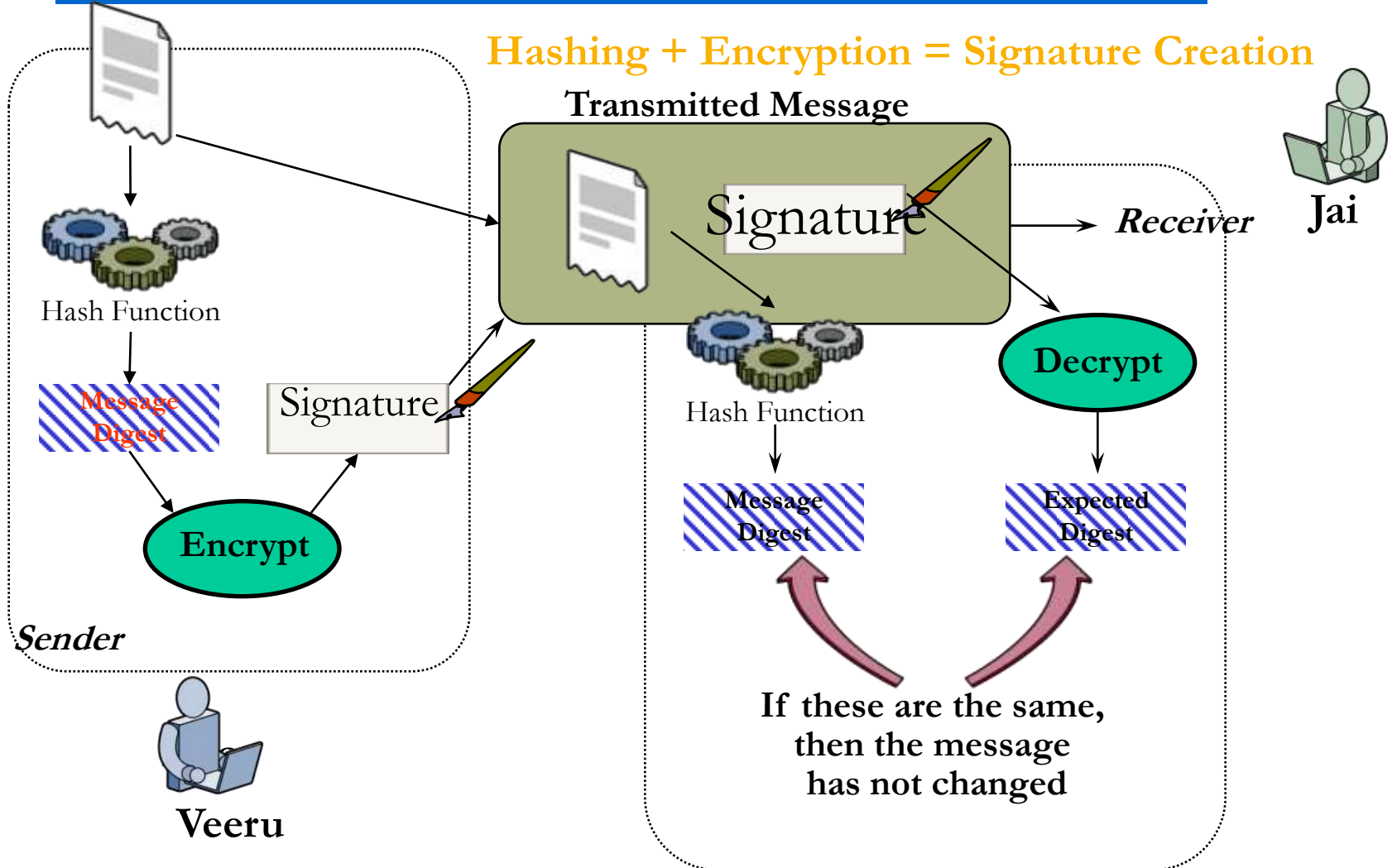
Hash

Message
Digest

Decrypt with
public key

Message
Digest

Signature Creation & Verification



Hashing + Decryption = Signature Verification



Digital Signatures (Examples)



I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is at Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

0e6d7d56c4520756f59235b6ae981cdb5f9820a0

I am an Engineer.

ea0ae29b3b2c20fc018aaca45c3746a057b893e7

I am a Engineer.

01f1d8abd9c2e6130870842055d97d315dff1ea3

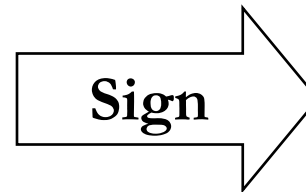
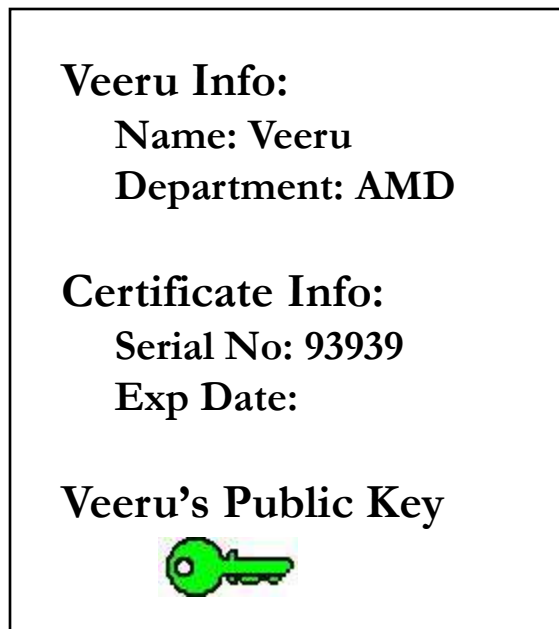
- These are digital signatures of same person on different documents

-
- Digital Signatures are numbers
 - They are content and signer dependent
-

Digital Signature Certificate (DSC)

What is Digital Certificate?

- A digital certificate binds the owners public key, name email and other necessary information together



?


✕

Certificate

General

Details

Certification Path



Certificate Information

This certificate is intended for the following purpose(s):


- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

* Refer to the certification authority's statement for details.

Issued to: Rajendran Balaji

Issued by: NIC sub-CA for NIC 2011

Valid from 2/24/2014 **to** 2/23/2016

 You have a private key that corresponds to this certificate.

Issuer Statement

OK

?

✕

Certificate

General

Details

Certification Path

Show: <All>

Field	Value
Serial number	31 11 99 e6 b8 a3 74 47 9e ab
Signature algorithm	sha256RSA
Issuer	NIC sub-CA for NIC 2011, Sub...
Valid from	Monday, February 24, 2014 6...
Valid to	Tuesday, February 23, 2016 6...
Subject	Rajendran Balaji, Karnataka, 5...
Public key	RSA (2048 Bits)
Subject Key Identifier	0c 34 5a 29 d9 86 03 5a 35 19...

```

30 82 01 0a 02 82 01 01 00 94 af f2 4f ca
61 28 fb 13 b2 cb 82 07 c1 37 c1 9a 5e a2
49 6f a2 69 19 78 61 8e 41 c1 e0 48 da 1c
48 af 6a 43 4f c9 36 8b 61 82 e8 e8 61 d2
b3 08 b1 59 38 06 ed af 37 ec 9d 6f a0 50
ec ae 29 38 d8 5c 21 07 40 38 80 a3 e7 bb
ea de 0a 8f f8 55 8f 0a b2 ea 52 b8 c4 d0
1a bb 81 29 82 33 69 77 cf cb 23 e0 f9 8b
1a 7e ff 63 92 8d 6d f3 2d 33 d8 51 0f 39
                
```

Edit Properties...

Copy to File...

OK

Certificate Classes

- 4 Classes of Certificates
 - Class 0 Certificate
 - Used only for testing and demo purposes
 - Class – 1 Certificate
 - Issued to Individuals
 - Assurance Level: Certificate will confirm User's name and Email address
 - Suggested Usage: **Signing certificate** primarily be used for signing personal emails and **encryption certificate** is to be used for encrypting digital emails and **SSL certificate** to establish secure communication through SSL
-

– Class – 2 Certificate

- Issued for both business personnel and private individuals use
 - Assurance Level: Conforms the details submitted in the form including photograph and documentary proof
 - Suggested Usage: **Signing certificate** may also be used for digital signing, code signing, authentication for VPN client, Web form signing, user authentication, Smart Card Logon, Single sign-on and signing involved in e-procurement / e-governance applications, in addition to Class-I usage
-

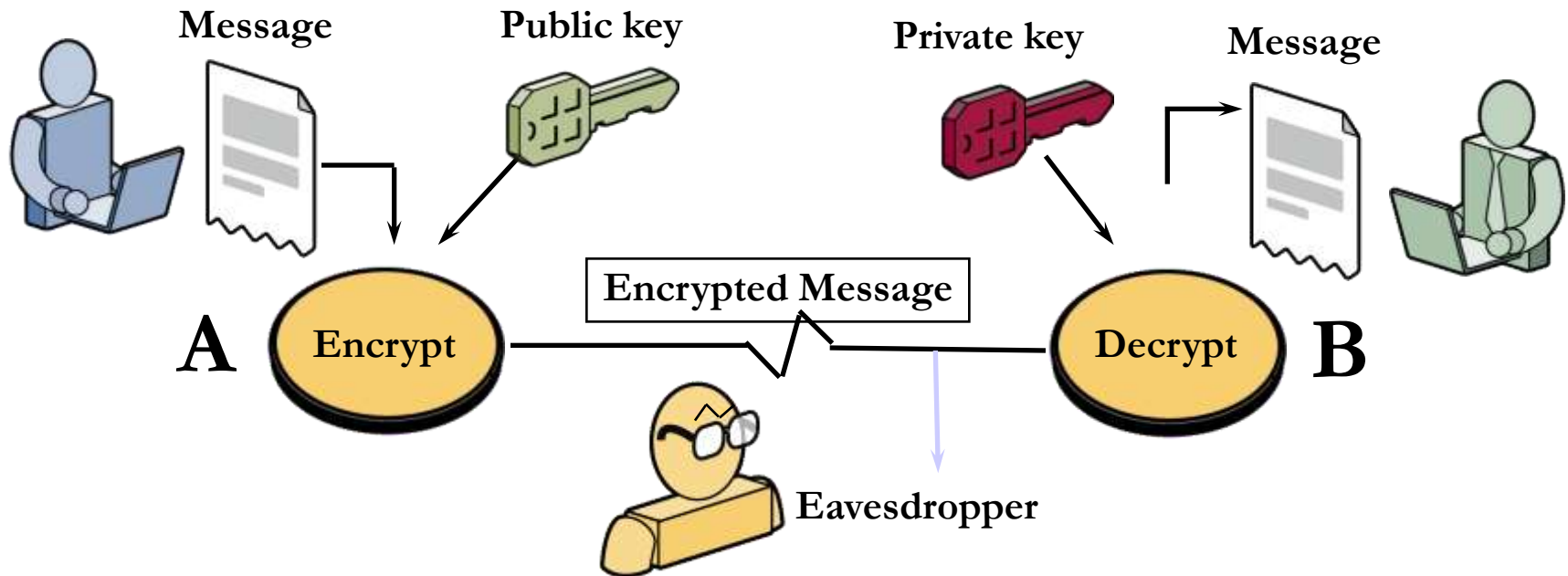
– Class – 3 Certificate

- Issued to Individuals and Organizations
 - Assurance Level: Highest level of Assurance; Proves existence of name of the organization, and assures applicant's identity authorized to act on behalf of the organization.
 - Suggested Usage: **Signing certificate** may also be used for digital signing for discharging his/her duties as per official designation and also **encryption certificate** may also be used for encryption requirement as per his/her official capacity
-

Certificate Extension	Description
.CER	Contains only Public Key
.CRT	Contains only Public Key
.DER	Contains only Public Key
.P12	Contains Public and Private Key
.PFX	Contains Public and Private Key
.PEM, .KEY, .JKS	Contains Public and Private Key
.CSR	Certificate Signing Request
.CRL	Certificate Revocation List

Achieving Confidentiality

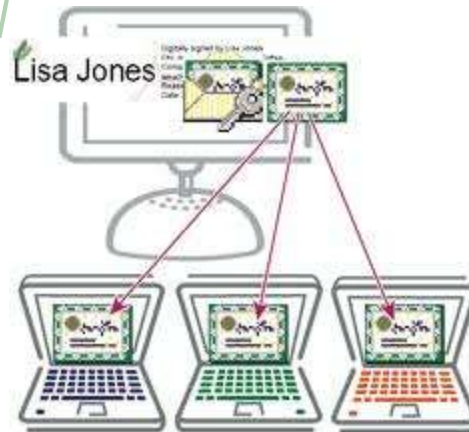
Asymmetric Key Encryption - Confidentiality



Risks & Precautions in PKI Security

- The Private key generated is to be protected and kept secret. **The responsibility of the secrecy of the key lies with the owner.**
- The key is secured using
 - PIN Protected soft token
 - Smart Cards
 - Hardware USB Tokens





- The Private key is encrypted and kept on the Hard Disk in a file, this file is password protected.
- This forms the lowest level of security in protecting the key, as
 - The key is highly reachable.
 - PIN can be easily known or cracked.
- **Soft tokens are not preferred because**
 - The key becomes static and machine dependent.
 - The key is in a known file format.

- The Private key is generated in the crypto module residing in the smart card.
- **The key is kept in the memory of the smart card.**
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (**Having smart card reader**)





- They are similar to smart cards in functionality as
 - Key is generated inside the token.
 - Key is highly secured as it doesn't leave the token.
 - Highly portable.
 - Machine Independent.
- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.



General Security Lessons



- Risks are inherent in any cryptographic system
 - PKI is not a one-stop solution for all your security needs
 - Any security system is only as safe as the weakest link in a security chain!
-

Policy Perspective

- UN Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996.
 - India is a signatory to this and therefore had to revise its laws accordingly
 - Indian IT Act follows the above model.
 - To facilitate e-commerce and e-governance the IT Bill, 1999 was introduced in the Indian Parliament
 - India enacted the Information Technology Act, 2000 that made changes to facilitate e-commerce and e-governance
 - India is one of the very few countries in the world besides Singapore to enact cyber laws as early as in 2000
-

- UNCITRAL Model law on e-commerce focuses on two basic functions of a signature
 - To identify the author of a document and
 - To confirm that the author approved the content of that document
 - Functions of Article 7 of UNCITRAL Model Law
 - Identify a person
 - Associate that person with the content of a document
 - Provide certainty as to the personal involvement of that person in the act of signing
 - Attest to the intent of a person to endorse authorship of a text;
 - Attest to the intent of a person to associate itself with the content of a document written by someone else;
 - Attest to the fact that, and the time when a person had been at a given place
-

Legal aspects of Digital Signature as per Indian IT Act



Objective of the Indian IT Act 2000



- To grant legal recognition to records maintained in electronic form
 - To prescribe methods for authenticating electronic records
 - To establish a hierarchical trust model with a root CA at the top - CCA to regulate the CAs
 - To define computer system and computer network misuse and make it legally actionable
-

- IT Act 2000 made changes in the Law of Evidence, and provides
 - Legal recognition for electronic records and electronic signatures, which paves the way for
 - Legal recognition for transactions carried out by electronic communication
 - Acceptance of electronic filing of documents with the government agencies
 - Changes in the IPC and the Indian Evidence Act 1872 were made accordingly
 - IT Act 2000 has extra-territorial jurisdiction to cover any offense or contravention committed outside India
-



Authentication Method Prescribed by the Indian IT Act 2000



- The Act specifies that authentication must be by Digital Signatures based upon *Asymmetric Key Cryptography* and *Hash Functions*.
 - The National Root CA uses a 2048 bit RSA key pair
 - Other CA and end entities use 2048 bit RSA key pairs
-

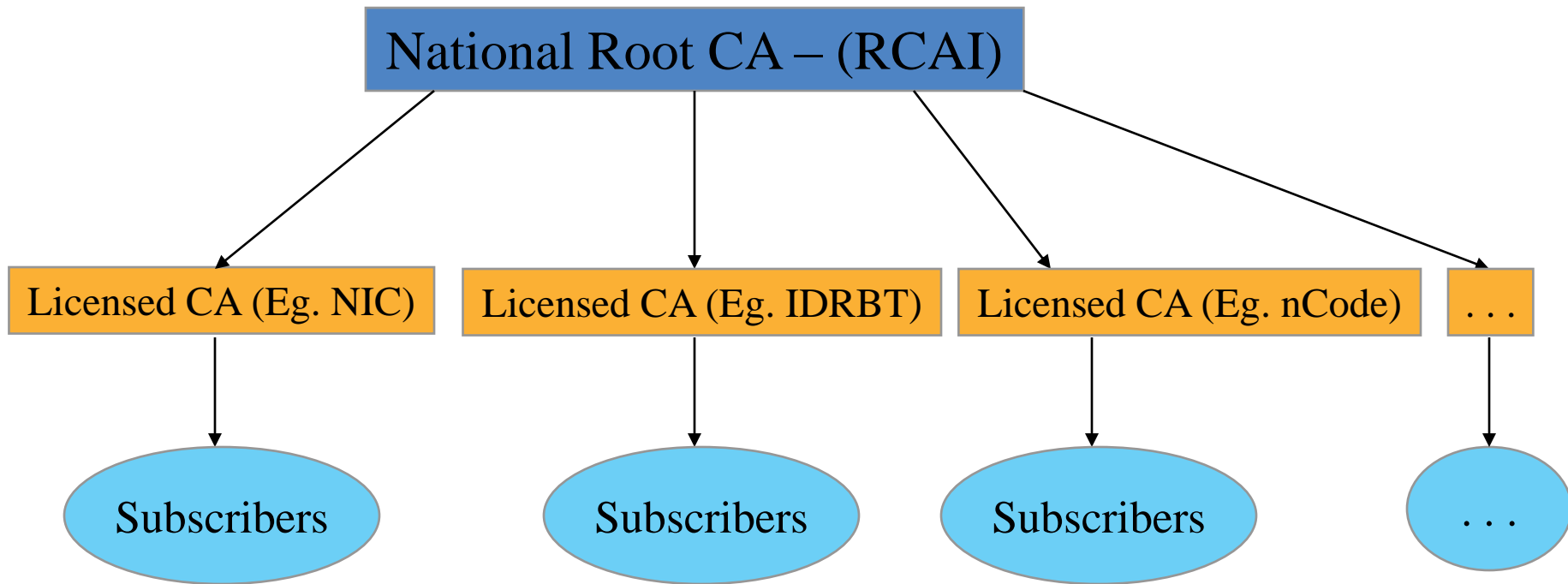


Regulation of Certifying Authorities



- The IT act mandates a hierarchical Trust Model
 - The IT Act provides the Controller for Certifying Authorities (CCA) to license and regulate the working of CA.
 - The CCA operates RCAI for certifying (signing) the public keys of CA's using its private key
-

- For a Digital Signature to have legal validity, it must derive its trust from the Root CA certificate





Licensed CA's in India



- National Root CA (RCAI) – operated by CCA
 - Only issues CA certificates for licensed CAs
 - 6 CAs licensed under the National Root CA
 - National Informatics Centre (<https://nicca.nic.in>)
 - eMudhra (www.e-mudhra.com)
 - TCS (www.tcs-ca.tcs.co.in)
 - nCode Solutions CA(www.ncodesolutions.com)
 - SafeScript (www.safescript.com)
 - IDRBT CA (www.idbrtca.org.in)
 - As of Jan 2014, approx. 70,85,000 (7.08 Million) certificates have been issued
-



Certifying Authority (CA)



- Certifying authority is an entity which issues Digital Certificate
- It is a Trusted third party
- CA's are the important characteristics of Public Key Infrastructure (PKI)

Responsibilities of CA

- Verify the credentials of the person requesting for the certificate (RA's responsibility)
 - Issue certificates
 - Revoke certificate
 - Generate and upload CRL
-



IT Act 2000 on CCA and CAs



- Under the Indian Law, section 35 of the IT (Amendment) Act, 2008 deals with certification and certifying authorities
 - IT Act 2000 recognizes even foreign CAs and gives the power to the CCA to decide on the same
 - CCA can also revoke the certificate for violation in any restriction or condition on which it was recognized by giving reasons in writing.
-

- The term 'Digital Signature' is now superseded by a term 'Electronic Signature'
 - Electronic signature is a generalized term; while Digital signature is application of cryptographic techniques to avail a reliable electronic signature.
 - A subscriber may authenticate any electronic record by **such electronic signature** or electronic authentication technique which is considered **reliable**
-

- The signature creation data or the authentication data are within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;
 - The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
 - Any alteration to the electronic signature made after affixing such signature is detectable;
 - Any alteration to the information made after its authentication by electronic signature is detectable;
-

- A ‘Digital Signature’ means an electronic signature created by transforming a data message using a message digest function and encrypting the resulting transformation with an asymmetric cryptosystem using the signer’s private key, such that any person having the initial untransformed data message, the encrypted transformation, and the signer’s corresponding public key can accurately determine:
 - (i) transformation was created using the private key that corresponds to the signer’s public key; and
 - (ii) whether the initial data message has been altered since the transformation was made.
-

Present Scenario in India



PKI enabled Applications



1	E-Invoice	(B2C)
2	E-Tax Filing	(G2C)
3	E-Customs	(G2B)
4	E-Passport	(G2C) - Presently in India, the Ministry of External Affairs has started issuing e-Passports in Karnataka state with the fingerprints and the digital photo of applicant
5	E-Governance	Bhoomi (G2C) a PKI enabled registration and Land Records Services offered by Govt. of Karnataka to the people. All the land records and certificates issued are digitally signed by the respective officer
6	E-Payment	(B2B) - In India, currently between banks fund transfers are done using PKI enabled applications whereas between customers and vendors such as online shopping vendor the payment is done through SSL thereby requiring the vendor to hold DSC)

7	E-Billing	(B2C) -The electronic delivery and presentation of financial statement, bills, invoices, and related information sent by a company to its customers)
8	E-Procurement	G2B , B2B
9	E-insurance service	(B2C) - Presently the users are getting the E-Premium Receipts etc. which is digitally signed by the provider

- DGFT - Clearance of goods are now initiated by exporters through push of a button and in their offices;
 - Previously it used to take days; and requests are cleared within 6 hours
 - Indian Patent office has implemented e-filing of patents and allows only use of Class-3 Certificates
 - Around 30% of e-filing of patents is happening now, among the total filings.
-



C-DAC Activities in PKI Domain



- PKI Outreach Programme
- PKI based Secure Messaging System

- Cryptography and Network security – principles and practice William Stallings
- Applied Cryptography, Second Edition: Bruce Schneier
- http://campustechnology.com/articles/39190_2
- <http://csrc.nist.gov/>
- Handbook of Applied Cryptography, by Menezes
- Cryptographic Techniques for N/w Security
- <http://www.productivity501.com/digital-signatures-encryption/4710/>
- <http://www.arx.com/digital-signatures-faq>
- http://www.asclonline.com/images/d/d4/Simple_Guide_to_Digital_Signatures.pdf
- <http://www.digitalsignatureindia.com/faq.php#3a>
- <http://www.asianlaws.org/library/infosec/obtaining-digital-signature-certificate.pdf>
- <http://nicca.nic.in/pdf/EncrBack.pdf>
- <http://nicca.nic.in/pdf/DSC-Request-Form.pdf>
- <http://cca.gov.in/>
- www.seekha.in/events/pki - for slides and resources
- ~~Ryder, Rodney D, Guide to Cyber Laws, 3rd Edition, Wadhwa & Company, New Delhi 2007~~

- Digital Signatures has been and continue to transform the way traditional transactions happen
 - Digital Signatures when implemented fully in an ecosystem, can bring in transparency, accountability, cost-savings, and speed of execution
 - Digital Signatures can become integral part of our digital identity
-

Thank You
