PAYMENT SECURITY USING PKI

By Mitesh Radia

Sr. Manager NPCI

Mitesh.radia@npci.org.in

OVERVIEW

- ✓ Introduction
  - ✓ Symmetric vs Asymmetric Encryption
  - ✓ Secure communication
- ✓ Key Exchange
- ✓ Applications
  - ✓ Secure Session
  - ✓ Message Level Security
- ✓ Certificate format
- ✓ Digital Signatures
- ✓ EMV offline data authentication
- ✓ RFID – Electronic Toll Transactions

INTRODUCTION

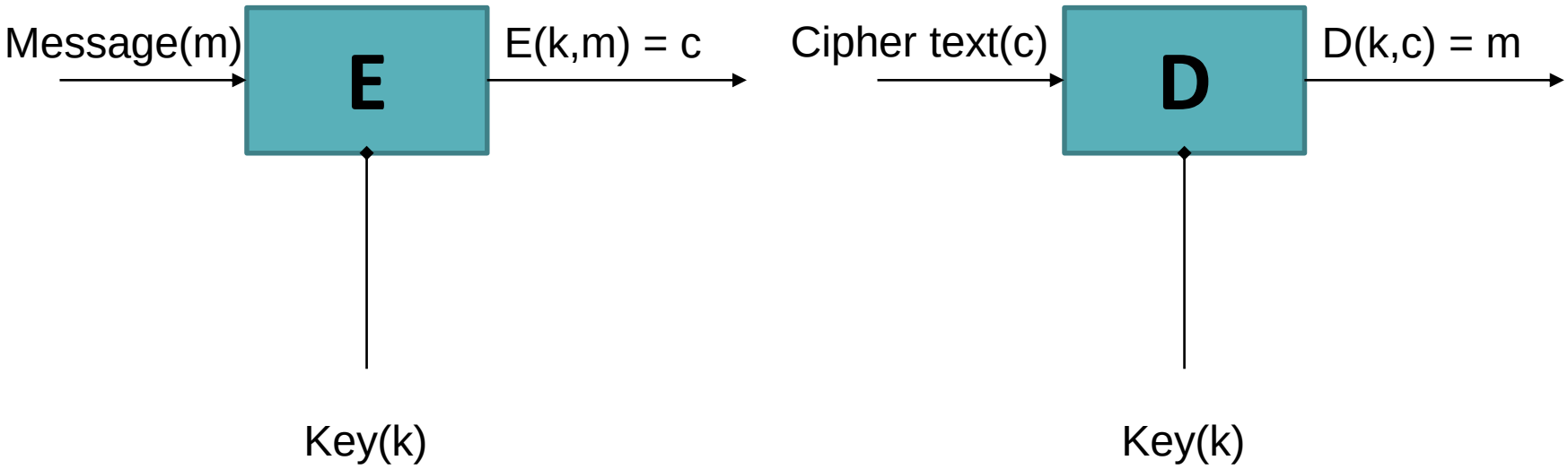
Assumptions

1. Security is required for all electronic transactions [processing of transactions, communications etc.]

Public Key Infrastructure (PKI) is _not_

1. Solution to all security problems
2. Reliable unless it is implemented as it should be
3. Something we should try and invent ad-hoc

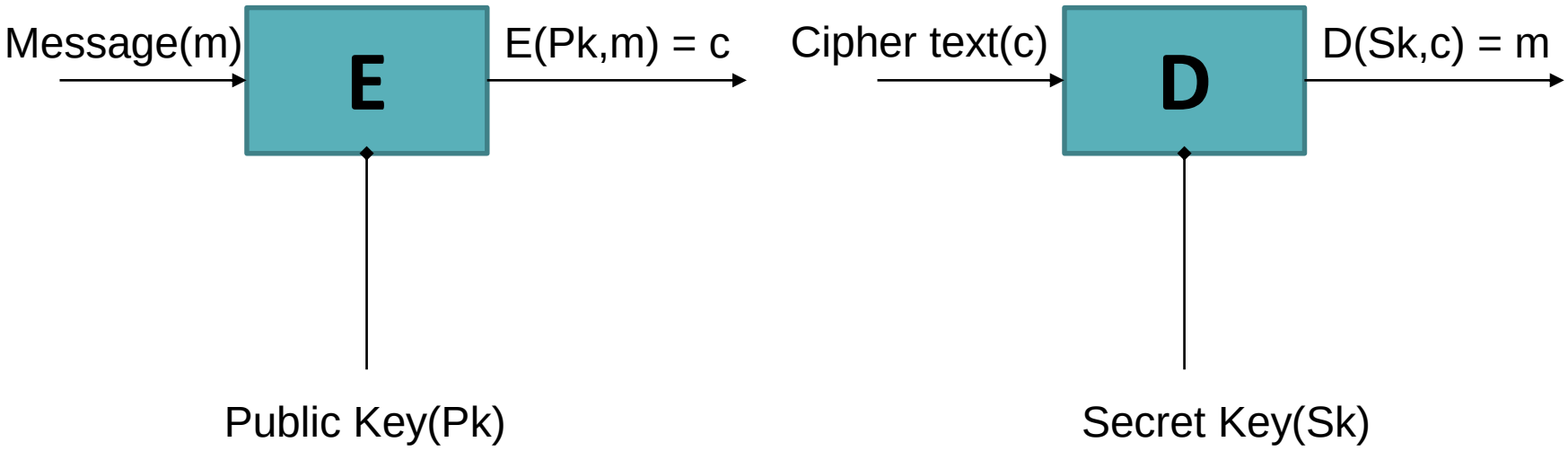
Introduction – Building blocks



Encryption/Decryption algorithm is publicly known

- Never use a proprietary algorithms

Introduction – Building blocks

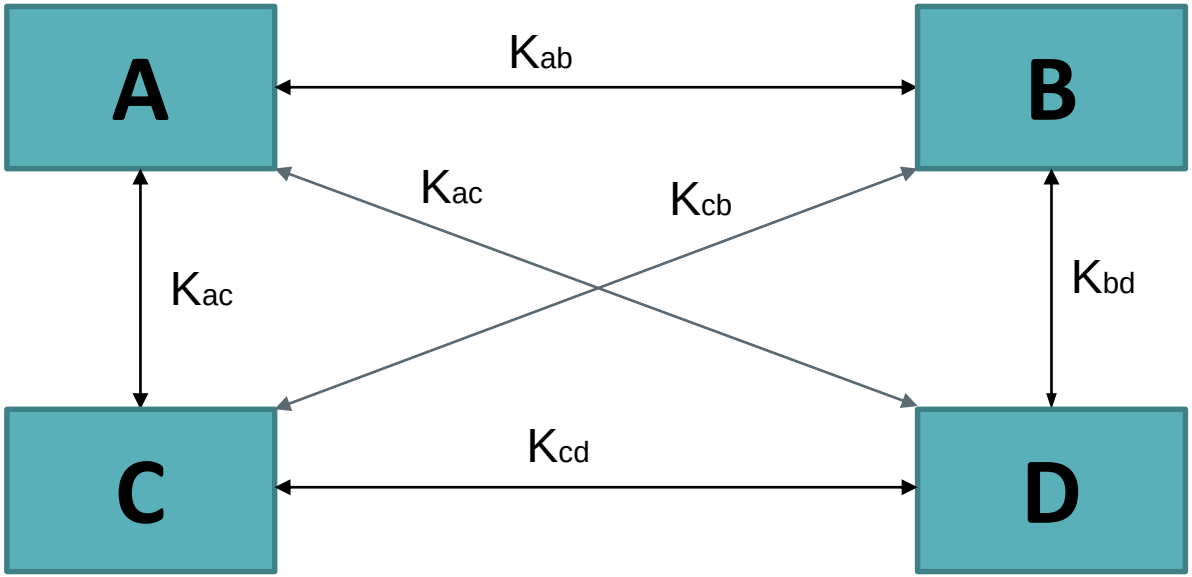


Public Key Encryption has _three_ parts

1) Key Pairs Generation
2) Encryption algorithm using public key
3) Decryption algorithm using secret key

Q: How is this possible?
Example: Trapdoor functions (RSA)

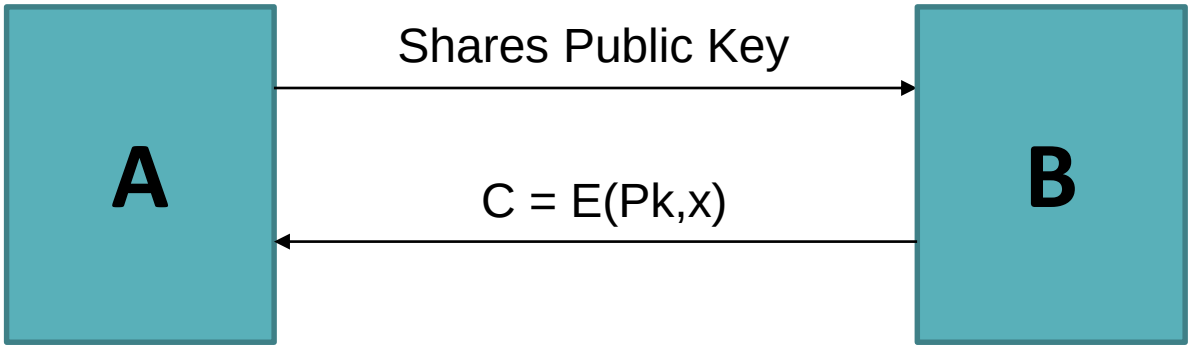
KEY MANAGEMENT



Problem: Storing mutual secret key is difficult
Solution: Trusted third party

Q: Can we share keys without trusted third parties
A: Yes!!! [Merkel, Diffie Hellman, RSA]

APPLICATIONS – SESSION SETUP [SSL/TLS]



1. A shares the public key
2. B generates the a random secret ‘x’
3. B encrypts the random secret x using A’s public key
4. A decrypts the random secret using the A’s secret key

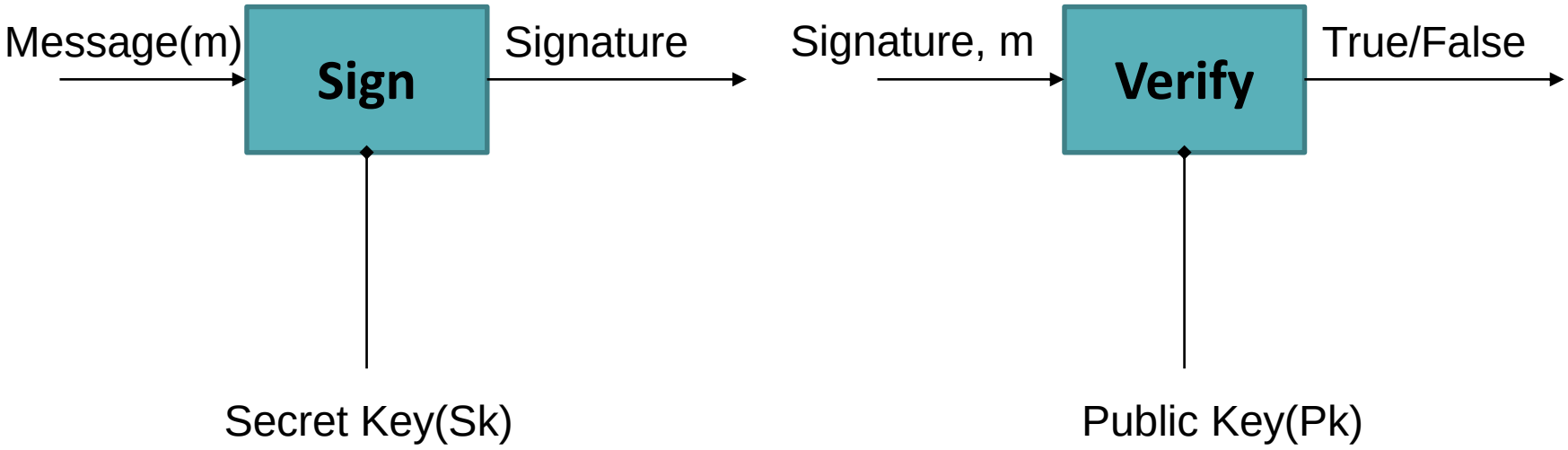
Note: Above example is vulnerable to man in middle attack

APPLICATION - MESSAGE LEVEL SECURITY

```
<Envelope>
        <OrgContent>
                .
                .
                .
        </OrgContent>
        <Signature>
                Y7z1Y+c+u80a9vhUSi
                        .
                        .
                        .
                u80a9vhUSi==
        </Signature>
</Envelope>
```

The digital signature on the files/messages ensures the integrity and source authentication of the files and non-repudiation and accountability of the sender of the message. The digital signatures on the files will be verified with the sender's certificate. The files will be verified by the application and the digital certificates using for affixing the signature will be validated.

Digital Signatures



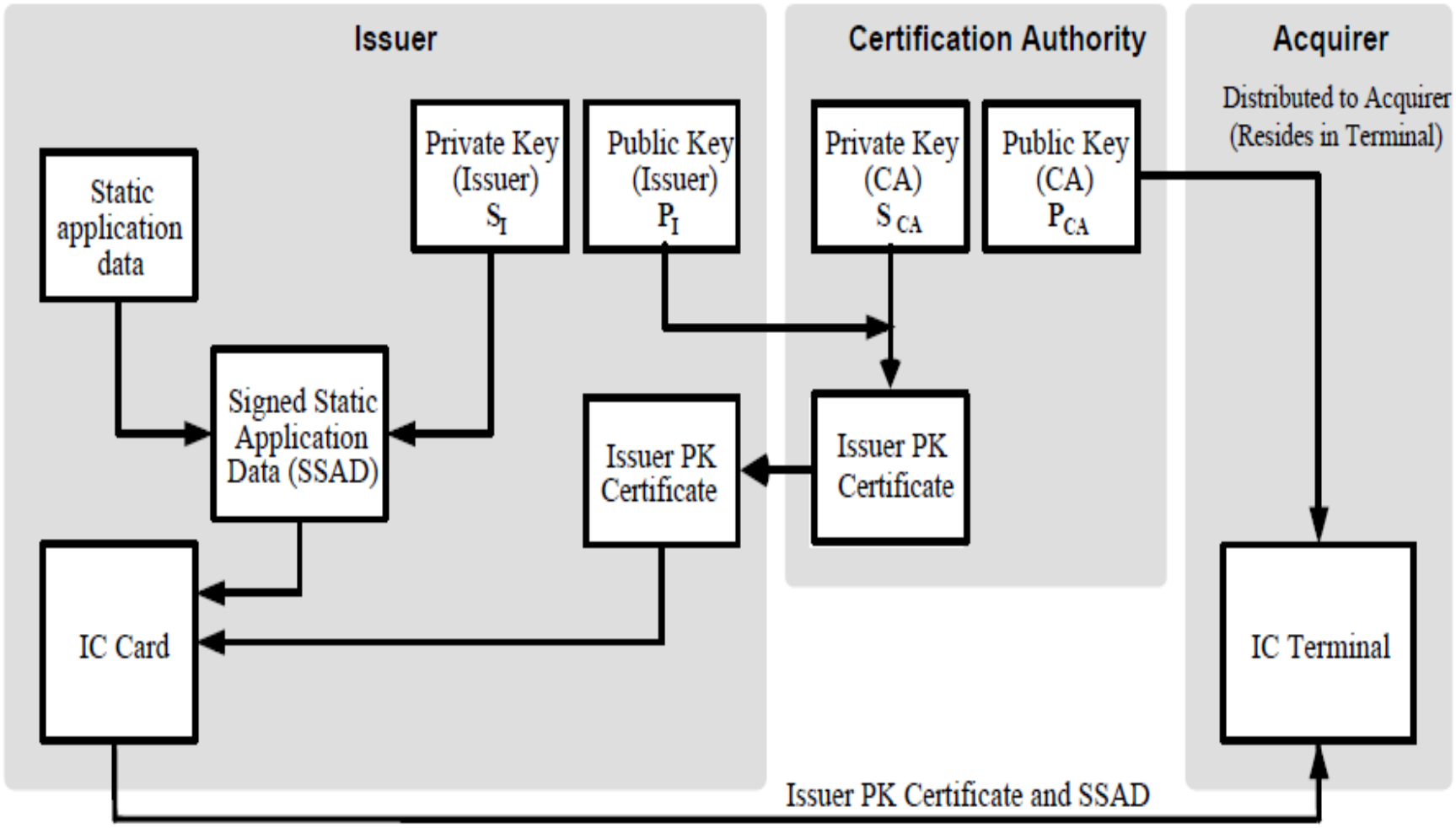
In smartcard applications the signing operations are performed in the computationally modest environment of the smart card while the verification process is implemented in a more computationally rich environment such as a personal computer, a hardware cryptographic module, or a mainframe computer

CERTIFICATES – X509

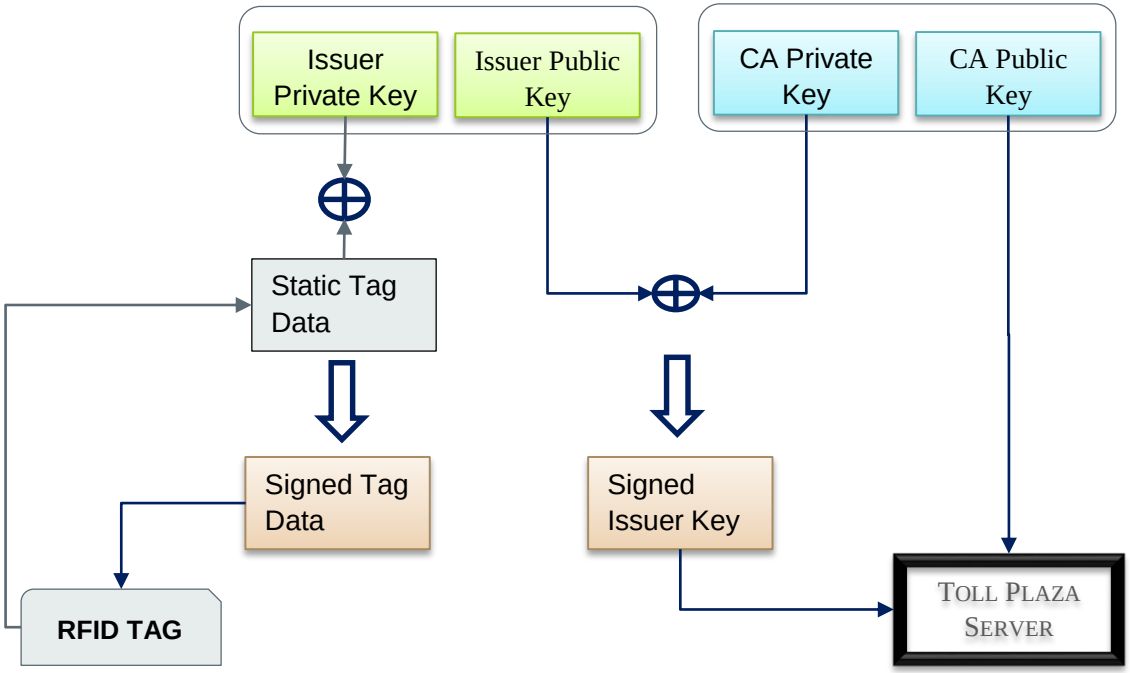
- ✓ **Version – certificate format**
- ✓ **Serial Number – unique within CA**
- ✓ **Algorithm Identifier – algo used to sign the certificate**
- ✓ **Issuer – name of CA**
- ✓ **Validity – pair of dates**
- ✓ **Subject – name of the user**
- ✓ **Public Key details – algorithm name, necessary parameters, public key**
- ✓ **Signature - CA**

Certificates can also be revoked, either because the user's key has been compromised, the CA's key has been compromised, or because the CA no longer wants to certify the user. Each CA must maintain a list of all revoked but not expired certificates.

EMV – STATIC DATA AUTHENTICATION



TAG/READER SECURITY – TOLL PLAZA VALIDATION



1. Toll Plaza Server/Lane Controller will read the signed data
2. As toll plaza server has CA Public keys, it can validate the issuer key
3. Using validated issuer key, toll plaza server can validate the signed tag data
4. Tag is not performing any crypto operations, its only toll plaza server which will perform required crypto operation.

ATTACKS - RSA

Timing Attack

The time it takes to compute decryption can expose private key

Power Attack

The power consumption of smart card during decryption can expose private key

Faults Attack

Computation error during decryption can expose private key. [Good to check output before giving out the results]

Caution:

To speed RSA decryption never use small private keys.

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

THANK YOU!