

Strategy and Synergy for Security

Elliptic Curve Cryptography (ECC) based Public Key Infrastructure (PKI)

Kunal Abhishek
Society for Electronic Transactions & Security (SETS), Chennai

14th November, 2017



Strategy and Synergy for Security

Focus of this talk

What should I do for implementing an ECC based PKI?



Strategy and Synergy for Security

Outline

- Part I** Evolution of PKI
- Part II** Some Details on ECC based PKI and Underlying Science
- Part III** Implementation Issues and Solution
- Part IV** RFCs and Standards on ECC based PKI
- Part V** Case Study : Implementation of Customized ECC based PKI
- Part VI** Concluding Remarks



Strategy and Synergy for Security

Part I

Evolution of PKI



Strategy and Synergy for Security

History of PKI in India

- The first CA for facilitating PKI services was licensed in **2002**.
- There are total **08 licensed CAs** in India which are offering **RSA** based CA services. [source : www.cca.gov.in]
- Only **03 CAs** offer **ECC based CA services** at present.



Strategy and Synergy for Security

IT Act for ECC based PKI in India

- Use of ECC became **legally permitted** asymmetric technique for **End Entity Digital Signing** purposes **since August 2015** through Gazette Notification.
- CA can offer ECC based digital certificate for **signing purposes** at present.



Strategy and Synergy for Security

Licensed CAs in India

- Following CAs are licensed to offer services to the users:

	Certification Authority	Licensed by CCA, GoI w.e.f.
1.	Safescrypt	5 th Feb, 2002
2.	IDRBT	6 th August, 2002
3.	National Informatics Centre	23 rd May, 2003
4.	(n)Code Solutions	12 th October, 2004
5.	E-mudhra CA	7 th November, 2008
6.	CDAC CA	29 th June, 2015
7.	Capricorn CA	16 th May, 2016
8.	NSDL e-Gov CA	27 th October, 2016

ECC/RSA based CA

RSA based CA

*Source : http://www.cca.gov.in/cca/?q=licensed_ca.html



Strategy and Synergy for Security

ECC based CAs across Globe

- **Elliptic curve Mathematics** was **used in Cryptography** by Neil Koblitz and Victor Miller **in 1985**, but was implemented formally as a proven **asymmetric technique** only **after the year 2000**.
- Despite **thousands of RSA-based PKIs** being flooded in the market to date, **only few companies** outside India offer ECC-based CA services these days.
- Some of these CAs are
 - GeoTrust
 - Thowte
 - Verisign
 - Global Sign
 - Semantec
 - Comodo etc.
- ECC based PKI is still in the **evolving stage**.



Strategy and Synergy for Security

Reasons for Scarcity of ECC based PKI

- The reason for **scarcity** of ECC based PKI or **delay in implementation** of ECC based PKI is
 - Elliptic Curve Mathematics is **very complex** and,
 - ECC based PKI, does not conform to the **common standards** for facilitating **interoperability** among the systems and within the system components.
- Apart from that **no fixed standard** has been given/finalized as yet for ECC based PKI.



Strategy and Synergy for Security

Part II

Some Details on ECC based PKI and Underlying Science



Strategy and Synergy for Security

Benefits of using ECC in PKI

- **RSA** is based on **Integer Factorization (IF) Problem** which is supposed to have **sub-exponential time solutions** [$\text{Time}_{\text{RSA}} \sim \exp((\log N)^{1/3})$] whereas,

ECC is based on **Elliptic Curve Discrete Logarithm Problem (ECDLP)** having **fully exponential time** [$\text{Time}_{\text{Elliptic Curve}} \sim \exp(c\sqrt{N})$] solutions being a **tougher mathematical problem** to solve.
- Public Key Infrastructure (PKI) based on RSA is successfully deployed and practiced across the globe. But **large RSA key sizes** leads to **slower performance** in different cryptographic operations in PKI activities.
- ECC is **faster, cheaper** and **more secure** with a **given key size** than RSA.



Strategy and Synergy for Security

ECC Vs. RSA : Performance Comparison

- Performance Comparison **ECC-256 & RSA-3072** [[Certicom](#)]

Operations	ECC-256	RSA-3072
Key Generation	166ms	Too Long
Encrypt/Verify	150ms	52ms
Decrypt/Sign	168ms	8s



Strategy and Synergy for Security

ECC Vs. RSA : Performance Comparision

- **Operational Speed-up Comparison** [[Certicom](#) and [RIM](#)]

Operations	Operation Time (in Seconds)	Speedup (ECC:RSA)
RSA 1024	10.99	1
ECC 160	0.81	13.6
RSA 2048	83.26	1
ECC 224	2.19	38

- Elliptic Curve Cryptography (ECC) is a [state-of-the-art asymmetric technique](#) supposed to be a [viable replacement](#) of traditional RSA.



Strategy and Synergy for Security

Public Key Infrastructure (PKI)

- RFC 2822 defines PKI as the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke digital certificates based on asymmetric cryptography.
- The principal objective for developing a PKI is to enable secure, convenient and efficient acquisition of public keys.
- A PKI enables the establishment of a trust hierarchy.
- The implementation of a PKI using a Certification Authority (CA) provides the trust hierarchy.



Strategy and Synergy for Security

Public Key Infrastructure (PKI)

The screenshot shows a Firefox Web Browser window with a single tab titled 'Google'. The address bar displays the URL: https://www.google.co.in/?gfe_rd=cr&dcr=0&ei=psogWu6rLujH8ges-bmIAQ. The browser's interface includes a search bar, navigation buttons (back, forward, home, refresh), and a user profile icon labeled 'U'. A vertical sidebar on the left contains various application icons. The main content area displays a 'Certificate Viewer' window for a certificate from '*.google.com'. The window has two tabs: 'General' and 'Details', with 'Details' selected. The 'Certificate Hierarchy' section is expanded, showing a tree structure: 'GeoTrust Global CA' (highlighted in orange and labeled 'Root CA' with a red arrow), 'Google Internet Authority G2', and '*.google.com'. Below this, the 'Certificate Fields' section is expanded, showing a tree structure: 'GeoTrust Global CA', 'Certificate', 'Version', 'Serial Number', 'Certificate Signature Algorithm', 'Issuer', 'Validity' (with sub-items 'Not Before' and 'Not After'), 'Subject', 'Subject Public Key Info', and 'Subject Public Key Algorithm'. The 'Field Value' section is currently empty. At the bottom of the window, there are 'Export...' and 'Close' buttons.



Strategy and Synergy for Security

Why Implement a PKI?

- The implementation of a PKI is intended to provide mechanisms to ensure **trusted relationships are established and maintained.**
- The specific security functions in which a PKI can provide foundation are
 - Confidentiality
 - Integrity
 - Authentication
 - Non-repudiation



Strategy and Synergy for Security

Why Implement a PKI?

- PKI prevents :
 - ✓ **Eavesdropping** (obtain information that is being transmitted) by providing **Confidentiality** to data through **Encryption**
 - ✓ **Modification (Tempering) of Data** by providing **Integrity** through **Hash Algorithms, Message Digest, Digital Signature**
 - ✓ **Spoofing** (one entity pretends to be a different entity) by providing **Authenticity** through **Digital Signature, Certificates**
 - ✓ **Flooding**
Availability through **Redundant Systems, Automatic Fail over**
 - ✓ **Phishing**
Source Authentication



Strategy and Synergy for Security

PKI Applications

- Some examples of PKI applications are:
 1. SSL, IPsec and HTTPS for communication and transactional security
 2. S/MIME and PGP for E-mail security
 3. SET for value exchange



Strategy and Synergy for Security

PKI : Underlying Crypto Mechanisms

- **Cryptographic Mechanisms** need to be used to provide a **complete suite of security services** including **confidentiality, authenticity, integrity** and **non-repudiation**.
- These mechanisms include,
 1. Symmetric Key
 2. Secure Hash
 3. Asymmetric Cryptography



Strategy and Synergy for Security

PKI : Underlying Crypto Mechanisms

1. Symmetric Key

Normally [AES-128](#) is used in PKI to achieve confidentiality.

2. Secure Hash

The secure hash algorithm is used for data integrity in PKI. [SHA256](#), [SHA384](#) and [SHA512](#) are suggested for use.

3. Asymmetric Cryptography

[ECC](#) is used as an [alternative](#) to [RSA](#) to achieve authentication, integrity, non-repudiation and key distribution purposes in the PKI.

[ECC](#) is used for [digital signatures](#) (ECDSA), [key transport](#) (Encrypting symmetric key) and [key agreement](#) (ECDHE).



Strategy and Synergy for Security

PKI : Underlying Crypto Mechanisms

Screenshot : ECDSA and ECDHE

The screenshot shows a web browser window with the address bar displaying <https://setzca.com/setzca/>. A 'Page Info' dialog box is open, showing the following information:

- Website Identity:**
 - Website: **setzca.com**
 - Owner: **This website does not supply ownership information.**
 - Verified by: **SETS**
 - Expires on: **October 19, 2022**
- Privacy & History:**
 - Have I visited this website prior to today? **Yes, 301 times**
 - Is this website storing information (cookies) on my computer? **Yes**
 - Have I saved any passwords for this website? **No**
- Technical Details:**
 - Connection Encrypted (TLS **ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**, 128 bit keys, TLS 1.2)
 - The page you are viewing was encrypted before being transmitted over the Internet.
 - Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Buttons for 'View Certificate', 'View Cookies', 'View Saved Passwords', and 'Help' are visible in the dialog. The background shows a blue header with the Indian flag and a 'SIGN IN' button. At the bottom, there are buttons for 'Renew Certificate', 'Revoke Certificate', and 'Track Certificate'. A footer at the bottom of the browser window reads 'COPYRIGHT © SETS 2017. ALL RIGHTS RESERVED.'



Strategy and Synergy for Security

Digital Signatures

- An **authentication** mechanism that enables the creator of a message to **attach a code that acts as a signature**.

```
To: user1.sets@gmail.com
From: user2 <user2.sets@gmail.com>
Subject: digital signed email
Message-ID: <33e1022d-0d35-18eb-0bb0-b00de13cc36c@gmail.com>
Date: Fri, 3 Feb 2017 12:38:04 +0530
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Thunderbird/45.5.1
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha-512; boundary="-----ms080800030504010205040602"
```

This is a cryptographically signed message in MIME format.

```
-----ms080800030504010205040602
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: quoted-printable
```

hi,

get it!!

Message Contents





Strategy and Synergy for Security

Digital Signatures

- The signature is formed by taking the **hash** of the message and **encrypting** the message with the **creator's private key**.
- The signature guarantees the **source** and **integrity** of the message.
- The Digital Signature Standard (DSS) is a **NIST standard** that uses the Secure Hash Algorithm (SHA).
- Applications include **Authenticity**, **Data Integrity** and **Non-repudiation**.



Strategy and Synergy for Security

Digital Signatures

Summarizing,

- It is a **mathematical** process
- **Contents** are signed
- **Authentication** and **tamper** evident
- Non-repudiation through **law**
- Signature is a **private** operation
- **Owner** is responsible for **private key security**
- **Multiple signers** can sign the **same doc**
- **Time stamping** provides additional assurance

Time Stamping :

- It adds the **Time element**, making a stronger case of evidence
- Protects from **signature stripping**
- **CA** provides time stamping services



Strategy and Synergy for Security

Digital Signatures

Signing and Verification :

▪ To sign

- hash the data
- encrypt the hash with the sender's private key
- send data signer's name and signature

▪ To verify

- hash the data
- find the sender's public key
- decrypt the signature with the sender's public key
- the result of which should match the hash



Strategy and Synergy for Security

Digital Signatures

Elliptic Curve Digital Signature Algorithm (ECDSA) :

- m : Message (hash of the data)
 F_q : Finite field defined over prime q
 E : Elliptic Curve defined over F_q
 r : a large prime such that $f * r = \#E$ where $f = 1,2,4$
 G : Base Point
 Q : $a * G$ where a is a secret integer drawn
Public Info : (F_q, E, r, G, Q)

To Sign:

1. Choose random integer k provided $1 < k < r$
2. Compute $R = k * G$
3. Compute $s = k^{-1}(m + ax) \pmod{r}$

Signed document is (m, R, s) .

To Verify:

1. Compute $u_1 = s^{-1} m \pmod{r}$ and $u_2 = s^{-1} x \pmod{r}$
2. Compute $V = u_1 G + u_2 Q$
3. Declares Signature valid if $V = R$

If message is signed correctly, the verification equation holds:

$$\begin{aligned} V &= u_1 G + u_2 Q \\ &= s^{-1} m * G + s^{-1} x Q \\ &= s^{-1} (mG + xQ) \\ &= s^{-1} (mG + xaG) = s^{-1} G (m + ax) \\ &= s^{-1} * G * s * k = kG = R \end{aligned}$$

So, $V = R$



Strategy and Synergy for Security

Digital Signatures

Screenshot for E-mail Signing :

The screenshot displays the Thunderbird Mail interface. The left sidebar shows the folder structure, including 'Inbox (13911)', 'Junk E-mail', 'Drafts', 'Sent Mail', 'All Mail (1391)', 'Spam', 'Trash (534)', 'Important (67)', 'Starred', 'Personal (v1)', 'Receipts', 'Travel', 'Work', and 'Local Folders' (Trash, Outbox). The main pane shows an email from 'bugslife.1492@gmail.com' with the subject 'Your Amazon.in order of Sparx Men's Navy Blue and Mindtree MEGA Off Campus Drive Hiring Freshers'. A 'Message Security' notification is overlaid on the email, stating: 'Message Is Signed. This message includes a valid digital signature. The message has not been altered since it was sent.' Below this, it lists 'Signed by: Kunal', 'Email address: kunal.sets@gmail.com', and 'Certificate issued by: CAcert', with a 'View Signature Certificate' button. A 'Certificate Viewer: "Kunal"' window is open, showing the following details:

General Details

This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate
- Email Signer Certificate
- Email Recipient Certificate
- Object Signer

Issued To

Common Name (CN)	Kunal
Organization (O)	PSA
Organizational Unit (OU)	SETS
Serial Number	00:F6:1F:C7:8A:43:25:FF:23

Issued By

Common Name (CN)	CAcert
Organization (O)	SETS
Organizational Unit (OU)	ACG

Period of Validity

Begins On	11/11/2017
Expires On	11/11/2019

Fingerprints

SHA-256 Fingerprint	33:1F:27:B0:BA:69:A0:04:8E:5F:BE:2E:23:BB:56:D0: 2D:BB:BF:52:DA:60:DE:5B:78:1C:66:E1:85:D4:F6:3F
SHA1 Fingerprint	EA:AF:7C:0D:48:82:74:9C:F0:EF:DE:33:9C:DE:33:DD:EF:03:B5:AA

The interface also shows a 'Delete' button and a 'More' dropdown menu in the bottom right corner of the email pane.



Strategy and Synergy for Security

Digital Certificates

- CAs provide digital certificates as **proof of the ownership** of **public keys**.
- A digital certificate **binds the owner's public key, name, E-mail** and other necessary information together.
- Some Standards of Digital Certificate
 - X.509 (v1, v2, v3)
 - Simple Public Key Infrastructure (SPKI)
 - PGP Certificates
 - Attribute Certificates

Among these types of Certificates, ITU recommended **X.509** format is most accepted Certificate format.



Strategy and Synergy for Security

Digital Certificates

- X.509 Certificate (Elliptic Curve based)

```
Terminal
┌───┴───┐
│ < > Home Desktop certificate |
├───┬───┤
│ Recent |
│ Home |
│ Desktop |
│ Documents |
│ Downloads |
│ Music |
│ Pictures |
│ Videos |
│ Trash |
│ Network |
│ Computer |
│ Connect to Server |
├───┬───┤
│ Amazon |
│ Settings |
│ System |
│ Search |
│ Terminal |
└───┬───┘
    >

Name
┌───┴───┐
│ kunal.sets_cert.pem |
├───┬───┤
│ Size | Type | Modific |
│      |      |         |
│      |      |         |
├───┬───┤
│      |      |         |
└───┬───┘
    Nov 9

root@setsca: ~/Desktop/certificate
root@setsca:~/Desktop/certificate# openssl x509 -in kunal.sets_cert.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 17735113254254280481 (0xf61fc78a4325ff21)
    Signature Algorithm: ecdsa-with-SHA512
    Issuer: C=IN, ST=TN, L=Chennai, O=SETS, OU=ACG, CN=CACert
  Validity
    Not Before: Nov  9 16:46:44 2017 GMT
    Not After : Nov  9 16:46:44 2019 GMT
  Subject: C=IN, ST=TN, O=PSA, OU=SETS, CN=Kunal/emailAddress=kunal.sets@gmail.com
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (521 bit)
    pub:
        04:01:24:9b:f8:e5:48:f3:39:d4:16:de:19:ef:0a:
        8b:c9:83:14:bb:c5:44:70:9e:22:b2:d0:71:e7:09:
        a5:02:bb:60:51:70:46:96:75:fd:04:c7:a0:e5:cf:
        98:82:7d:32:81:57:34:45:e1:35:4c:3c:57:5c:45:
        b9:87:2d:ce:4c:4f:06:00:bb:e5:85:91:3c:e3:f4:
        44:7c:34:d6:af:72:34:4e:85:14:08:00:d5:a7:b9:
        e6:38:da:e9:83:30:9f:6e:ca:de:ef:f4:a3:c4:fa:
        6f:2a:46:3a:1e:63:c6:cd:37:e5:96:88:ca:f8:d6:
        e0:90:ab:73:b1:4d:a1:38:33:ac:a8:3a:83
    ASN1 OID: secp521r1
    NIST CURVE: P-521
  X509v3 extensions:
    X509v3 Subject Key Identifier:
        D3:B0:BE:20:21:C3:FD:8C:5A:9E:93:5D:65:D3:3C:D4:3E:C2:D0:A7
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 key usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign
    X509v3 CRL Distribution Points:

  Full Name:
    URI:https://setsca.com/setsca/CRL/crl_list.crl

  Authority Information Access:
    OCSP - URI:http://ocsp.setsca.com:8888
    CA Issuers - URI:http://setsca.com/setsca/cacert/ca_cert.crt

  Netscape CA Revocation Url:
    http://setsca.com/setsca/CRL/crl_list.crl
  Signature Algorithm: ecdsa-with-SHA512
    30:81:87:02:42:01:8c:49:be:9b:24:ef:1e:e0:8a:2c:a3:df:
    2c:3f:58:82:d9:47:c9:85:e3:b7:5b:33:00:60:b2:c3:b2:90:
    6f:c4:8b:c2:45:4b:e1:05:3f:b5:b8:f6:c7:30:15:10:02:77:
    0e:a4:80:47:5a:cb:25:76:aa:91:38:c2:5d:e6:8b:b4:77:02:
    41:3f:94:eb:28:92:58:88:ba:af:fe:f8:de:be:53:b7:c4:2c:
    fc:61:41:83:32:08:d0:46:e5:59:79:9c:03:e4:aa:11:18:6f:
    7c:07:4a:4d:2e:89:c1:90:62:60:29:a7:e0:53:f9:0e:f7:67:
    79:9c:8c:9d:b0:fc:6e:ec:36:b9:da:bb
root@setsca:~/Desktop/certificate#
```



Strategy and Synergy for Security

Digital Certificates

- Popular **formats** of a digital certificate are **.pem**, **.crt**, **.p12**, **.cer**, **.der**
- Digital certificate with **.crt** extension is generally installed in the **Trusted Root directory** of the machine.
- Digital Certificate with **.p12** extension only carries **encrypted private key** among all other extensions.



Digital Certificates

- Example : Screenshot of .p12 certificate structure

```
root@setsca: ~/Documents
root@setsca:~/Documents# openssl pkcs12 -info -in Kunal.sets_cert.p12
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: EA AF 7C 0D 48 82 74 9C F0 EF DE 33 9C DE 33 DD EF 03 B5 AA
subject=/C=IN/ST=TN/O=PSA/OU=SETS/CN=Kunal/emailAddress=kunal.sets@gmail.com
issuer=/C=IN/ST=TN/L=Chennai/O=SETS/OU=ACG/CN=CAcert
-----BEGIN CERTIFICATE-----
MIIDazCCAsygAwIBAgIJAPYfx4pDJf8jMAoGCCqGSM49BAMEMFoxCzAJBgNVBAYT
Ak1OMQswCQYDVQQLDAJUTjEQA4GA1UEBwwHQ2h1bm5haTENMA5GA1UECgwEU0VU
UzEMMAoGA1UECwwDQUNHM08wDQYDVQDDAZDQWlnQWwHhcnMTcxMTEwMTYxODE0
HhcnMTcxMTEwMTYxODE0HjBsMQswCQYDVQQLGwEwJjJjELMAkGA1UECAwV4xDDAK
BgnVBAOMA1BTQENMASGA1UECwwEU0VUUEZEMAwGA1UEAwwFS3VvYXVwIzAhBgkq
hkiG9w0BCQEFgt1bmFslNlDHNAZ21haWwUY29tMIGbMBAGByqGSM49AgEGSUB
BAAjA4GGAQAQNOPJLvjkuI7jFXN3Qx9tE/NTuLIS9SFJDNwRjaLeZnoL0ZcM4LI
zrh7bk3RjcrH+LATLB+ehSILHcquJ01xE4AbmaX0b5X3ZTYK8uiGxjIj62zmN0x
kP0VvYefKhCFXZCsJd6CL/EZytoLyfKlR04ICo1bL2Z/8Mx9Q40vtTYKhGjggEk
MIIBIDAdBgNVHQ4EFgQUzLsqFY/dNInMUmydBeEIjgK/nkwCQYDVRR0TBAIwADAL
BgNVHQ8EBAMCAFYwOwYDVRR0FBDQWmJAwOC6gLIYgaHR0cHM6Lj9zZXRzY2EuY29t
L3NldHNjYS9DUkwvY3J5X2xpc3QvY3J5SjMhAGCCsGAQUFBwEBBGGQwYjAnBggrBgE
BQcwAYYbaHR0cDovL29jc3Auc2V0c2NhLmNvbTo40Dg4MDCGCCsGAQUFBzAChito
dHRwOi8vc2V0c2NhLmNvbS9zZXRzY2EuY29tY2FjZjZ0L2NhX2NlcnQuY3J0MDgGCWCG
SAGG+EIBBAQRFlodHRwOi8vc2V0c2NhLmNvbS9zZXRzY2EuY29tY2FjZjZ0L2NhY29t
LmNybDAKBggqhkjOPQDBA0BjAAwGyGCGAZy6xYHhXscG+Z2aDaciCob5UBCz
xhZf4C7KXMPRRexdnUjVg0s2KxBEBa29Ac7PSi13XaTm17wlThbyHwaAJCAJIX
c1k4U4uzv3tncJN779lhX8Ly47LORBa8Cj2Cwi4gdDeeNG4shf11d28dxy6cK/G
FPLo6i03Z37hsRC5bgwD
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: EA AF 7C 0D 48 82 74 9C F0 EF DE 33 9C DE 33 DD EF 03 B5 AA
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBPTBAbGqhkIG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIoH7r5VJPRWRCAGGA
MBQGCCqGSIb3DQMHBAJL2d4JfxPjVQSB+Anb8vYXlye6+/EhTnyAiyVlhuoP4TZ
rnmPphf9/vV1vwCLu+hUtB6FonIRmxNBIInXYQNRcIk2N+RQD29MrzjXStnXX
ET0L9mzFhXbhjoobbPdoNkozFVQ0b5TV+VZjs0bx+cPxrBDTKndnmbpTq1oAd
Q7hBVRpwMEg6+KDNuED087XErwY1Cm4nRHK3bWhHQ0+FI7nJx+Rx0q+LkBUHhM
QLT1jqQ12HSQEv3r3i2eprup6PBhzo1Dg/kmsGQPzDK3wAFH+/B3HTNEpbnWNTF
FTC6uQ2d9ZCcSyox7B8bcqaS24cYzNhdTU9KMEKmlax0
-----END ENCRYPTED PRIVATE KEY-----
root@setsca:~/Documents#
```



Strategy and Synergy for Security

Digital Certificates

Screenshot : User certificate in P12 format having encrypted private key

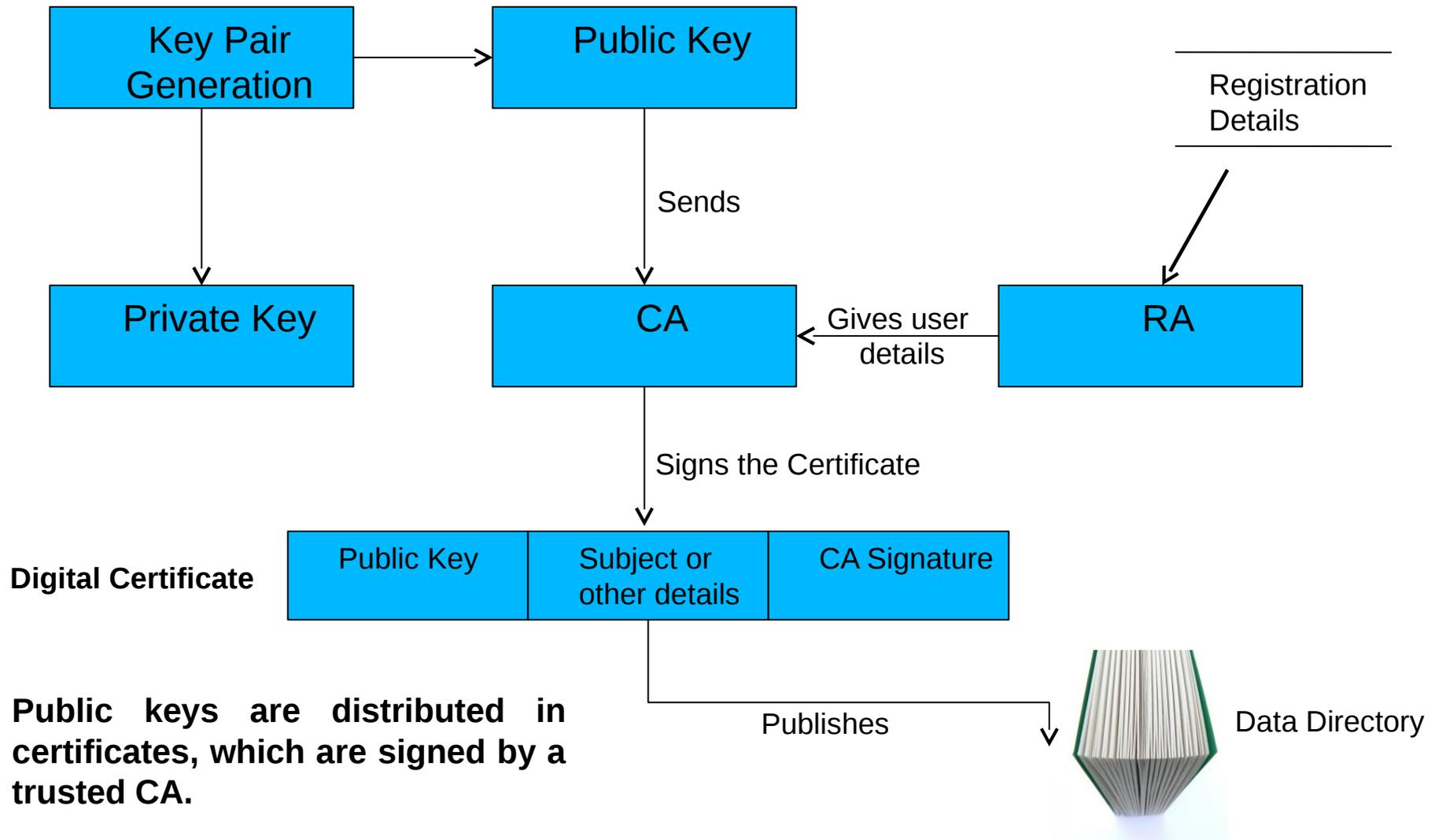
The screenshot displays the Thunderbird Mail interface for the account **kunal.sets@gmail.com**. The **Certificate Manager** dialog box is open, showing the **Your Certificates** tab. The dialog contains a table with the following columns: **Certificate Name**, **Security Device**, **Serial Number**, and **Expires On**. Below the table, there are buttons for **View...**, **Backup...**, **Backup All...**, **Import...**, and **Delete...**. An **Alert** dialog box is overlaid on top of the Certificate Manager, displaying the message: **Successfully restored your security certificate(s) and private key(s).** with an **OK** button.

Certificate Name	Security Device	Serial Number	Expires On
------------------	-----------------	---------------	------------



Digital Certificates

- Public Key Distribution through digital Certificate :





Strategy and Synergy for Security

PKI Components

- Certification Authority
- Registration Authority
- End User
- Repository
- Archives



Strategy and Synergy for Security

PKI Functions

- Key Generation and Management
- Certificate Management and Distribution
- Certificate Revocation List
- Online Certificate Status Protocol (OCSP)
- Access Control

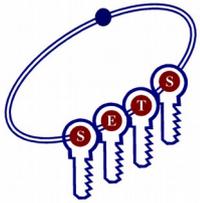


Strategy and Synergy for Security

PKI Functions

- Certificate Revocation List (CRL)

CA generates CRL and make it available at the location pointed to be the primary CRL distribution point extension that the CA populates in all end-user certificates.



Strategy and Synergy for Security

PKI Functions

```
Terminal
root@setsca: ~/Desktop/certificate
root@setsca:~/Desktop/certificate# openssl x509 -in kunal.sets_cert.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 17735113254254280481 (0xf61fc78a4325ff21)
    Signature Algorithm: ecdsa-with-SHA512
    Issuer: C=IN, ST=TN, L=Chennai, O=SETS, OU=ACG, CN=CACert
    Validity
      Not Before: Nov  9 16:46:44 2017 GMT
      Not After : Nov  9 16:46:44 2019 GMT
    Subject: C=IN, ST=TN, O=PSA, OU=SETS, CN=Kunal/emailAddress=kunal.sets@gmail.com
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (521 bit)
      pub:
        04:01:24:9b:f8:e5:48:f3:39:d4:16:de:19:ef:0a:
        8b:c9:83:14:bb:c5:44:70:9e:22:b2:d0:71:e7:09:
        a5:02:bb:60:51:70:46:96:75:fd:04:c7:a0:e5:cf:
        98:82:7d:32:81:57:34:45:e1:35:4c:3c:57:5c:45:
        b9:87:2d:ce:4c:4f:06:00:bb:e5:85:91:3c:e3:f4:
        44:7c:34:d6:af:72:34:4e:85:14:08:00:d5:a7:b9:
        e6:38:da:e9:83:30:9f:6e:ca:de:ef:f4:a3:c4:fa:
        6f:2a:46:3a:1e:63:c6:cd:37:e5:96:88:ca:f8:d6:
        e0:90:ab:73:b1:4d:a1:38:33:ac:a8:3a:83
      ASN1 OID: secp521r1
      NIST CURVE: P-521
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        D3:B0:BE:20:21:C3:FD:8C:5A:9E:93:5D:65:D3:3C:D4:3E:C2:D0:AF
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign
      X509v3 CRL Distribution Points:
        Full Name:
          URI:https://setsca.com/setsca/CRL/crl_list.crl

    Authority Information Access:
      OCSP - URI:http://ocsp.setsca.com:8888
      CA Issuers - URI:http://setsca.com/setsca/cacert/ca_cert.crt

    Netscape CA Revocation Url:
      http://setsca.com/setsca/CRL/crl_list.crl
    Signature Algorithm: ecdsa-with-SHA512
    30:81:87:02:42:01:8c:49:be:9b:24:ef:1e:e0:8a:2c:a3:df:
    2c:3f:58:82:d9:47:c9:85:e3:b7:5b:33:00:60:b2:c3:b2:90:
    6f:c4:8b:c2:45:4b:e1:05:3f:b5:b8:f6:c7:30:15:10:02:77:
    0e:a4:80:47:5a:cb:25:76:aa:91:38:c2:5d:e6:8b:b4:77:02:
    41:3f:94:eb:28:92:58:88:ba:af:fe:f8:de:be:53:b7:c4:2c:
    fc:61:41:83:32:08:d0:46:e5:59:79:9c:03:e4:aa:11:18:6f:
    7c:07:4a:4d:2e:89:c1:90:62:60:29:a7:e0:53:f9:0e:f7:67:
    79:9c:8c:9d:b0:fc:6e:ec:36:b9:da:bb
root@setsca:~/Desktop/certificate#
```



Strategy and Synergy for Security

PKI Functions

■ Online Certificate Status Protocol (OCSP)

```
Terminal
root@setsca: ~/Desktop/certificate
root@setsca:~/Desktop/certificate# openssl x509 -in kunal.sets_cert.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 17735113254254280481 (0xf61fc78a4325ff21)
    Signature Algorithm: ecdsa-with-SHA512
    Issuer: C=IN, ST=TN, L=Chennai, O=SETS, OU=ACG, CN=CAcert
    Validity
      Not Before: Nov  9 16:46:44 2017 GMT
      Not After : Nov  9 16:46:44 2019 GMT
    Subject: C=IN, ST=TN, O=PSA, OU=SETS, CN=Kunal/emailAddress=kunal.sets@gmail.com
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (521 bit)
      pub:
        04:01:24:9b:f8:e5:48:f3:39:d4:16:de:19:ef:0a:
        8b:c9:83:14:bb:c5:44:70:9e:22:b2:d0:71:e7:09:
        a5:02:bb:60:51:70:46:96:75:fd:04:c7:a0:e5:cf:
        98:82:7d:32:81:57:34:45:e1:35:4c:3c:57:5c:45:
        b9:87:2d:ce:4c:4f:06:00:bb:e5:85:91:3c:e3:f4:
        44:7c:34:d6:af:72:34:4e:85:14:08:00:d5:a7:b9:
        e6:38:da:e9:83:30:9f:6e:ca:de:ef:f4:a3:c4:fa:
        6f:2a:46:3a:1e:63:c6:cd:37:e5:96:88:ca:f8:d6:
        e0:90:ab:73:b1:4d:a1:38:33:ac:a8:3a:83
      ASN1 OID: secp521r1
      NIST CURVE: P-521
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        D3:B0:BE:20:21:C3:FD:8C:5A:9E:93:5D:65:D3:3C:D4:3E:C2:D0:AF
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign
      X509v3 CRL Distribution Points:

      Full Name:
        URI:https://setsca.com/setsca/CRL/crl_list.crl

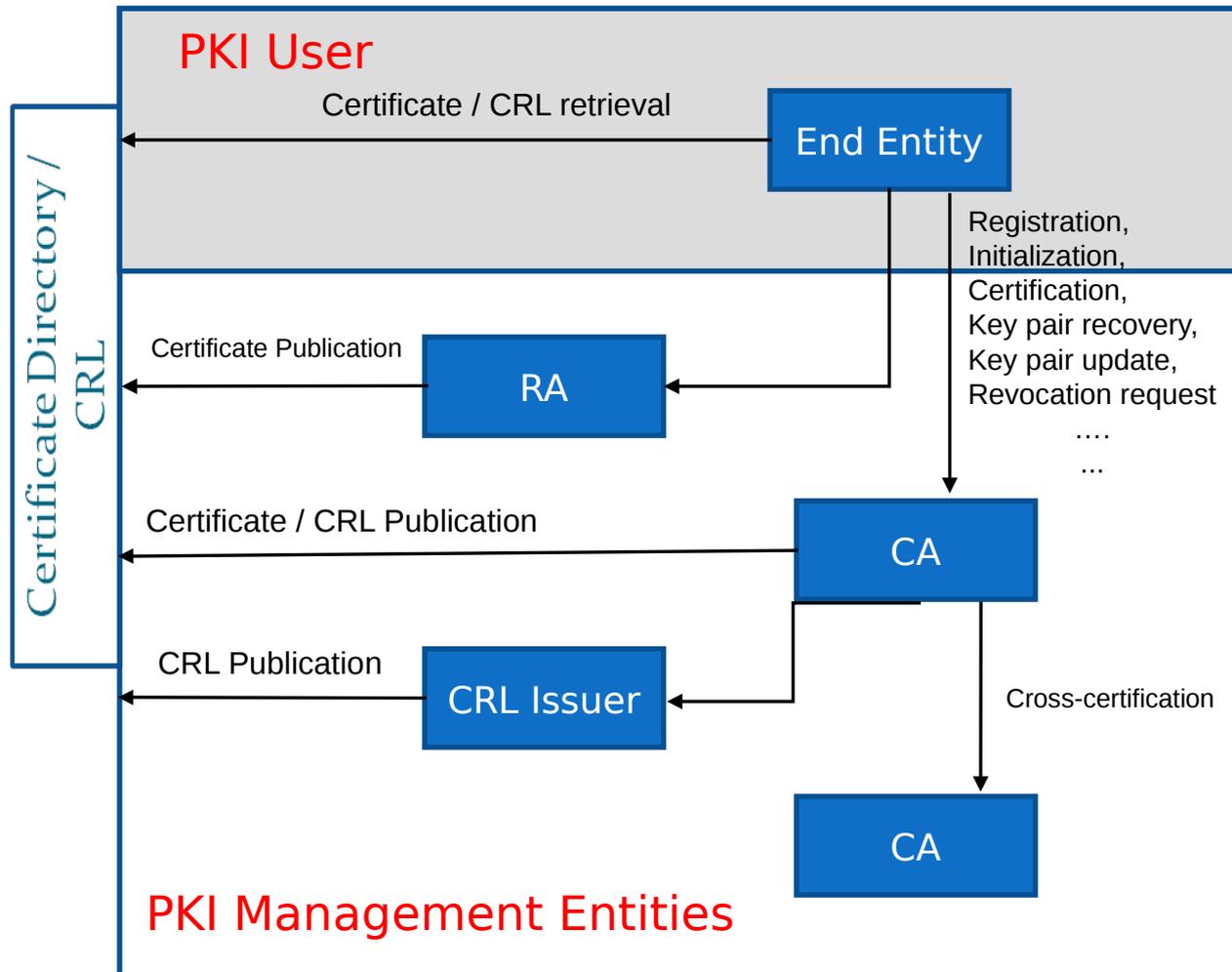
      Authority Information Access:
        OCSP - URI:http://ocsp.setsca.com:8888
        CA Issuers - URI:http://setsca.com/setsca/cacert/ca_cert.crt

      Netscape CA Revocation Url:
        http://setsca.com/setsca/CRL/crl_list.crl
    Signature Algorithm: ecdsa-with-SHA512
    30:81:87:02:42:01:8c:49:be:9b:24:ef:1e:e0:8a:2c:a3:df:
    2c:3f:58:82:d9:47:c9:85:e3:b7:5b:33:00:60:b2:c3:b2:90:
    6f:c4:8b:c2:45:4b:e1:05:3f:b5:b8:f6:c7:30:15:10:02:77:
    0e:a4:80:47:5a:cb:25:76:aa:91:38:c2:5d:e6:8b:b4:77:02:
    41:3f:94:eb:28:92:58:88:ba:af:fe:f8:de:be:53:b7:c4:2c:
    fc:61:41:83:32:08:d0:46:e5:59:79:9c:03:e4:aa:11:18:6f:
    7c:07:4a:4d:2e:89:c1:90:62:60:29:a7:e0:53:f9:0e:f7:67:
    79:9c:8c:9d:b0:fc:6e:ec:36:b9:da:bb
root@setsca:~/Desktop/certificate#
```



PKI Architecture

PKIX Architectural Model





Strategy and Synergy for Security

Part III

Implementation Issues and Solution



Strategy and Synergy for Security

Implementation Issues

- PKI needs **complex design** (63+ RFCs)
- **Major issues** with implementation of ECC based PKI are
 - Non-interoperability
 - Security considerations
 - Patent problem
- Lack of **common standards**



Strategy and Synergy for Security

Solution to Interoperability Issues

- One way to achieve interoperability among different entities or modules in a system is to *specify the cryptographic schemes well before starting any communication.*

For example, SSL/TLS.

- Other way to achieve interoperability among different entities or modules in a system is *to follow the same set of established standards and schemes/protocols so that there should not be any compatibility issues.*
- Careful selection of **stable standards** would encourage interoperability.



Strategy and Synergy for Security

Solution to Interoperability Issues

- *List out most suitable standards and protocols for designing ECC-based PKI to avoid implementation issues keeping cryptographic security and patent issues in mind.*
- Example:
IEEE P1363 standard is defined for Public Key Cryptography but it doesn't mandate **minimum security requirements** which is our one of the major concern. This standard also gives **plenty of options** that definitely leads to interoperability problems.



Strategy and Synergy for Security

Solution to Interoperability Issues

- **Interoperability between CA and CSR:**

Same point compression technique must be used by the public key residing in the certificates or certificate signing request (CSR).

- **No point compression** is a better option to achieve interoperability.



Strategy and Synergy for Security

Implementaion Issues due to Patents

- Most of the patents are owned by Certicom in ECC. [Certicom](#) holds around [130 patents in ECC](#).
- It leads to [high cost](#) in PKI design.
- Point Compression on an elliptic curve is under U.S. patent 6,141,420 therefore, point compression is not suggested in PKI implementation [to avoid huge license cost](#).
- Essentially we need [well-established royalty-free standards and protocols](#) that can [ensure security](#) at one hand and [legal clarity](#) at the other side.



Strategy and Synergy for Security

Solution to Security Issues

- **Cryptographic security must be ensured in a PKI.** We need to consider those **elliptic curves** whose **discrete logarithm problem is very tough** and can not be feasible to solve in a reasonable amount of time.
- For achieving such goal **FIPS** guidelines are suggested for selection of cryptographically suitable elliptic curves.
- **Other cryptographic aspects of PKI should must be ensured as well.**



Strategy and Synergy for Security

Part IV

RFCs and Standards on ECC based PKI



Strategy and Synergy for Security

RFCs in PKI

- RFCs for PKI : Total **63 RFCs** (may be more) that the **IETF's PKIX Working Group** has published to date :

2459, 2510, 2511, 2527, 2528, 2559, 2560, 2585, 2587, 2797,
2822, 2875, 3029, 3039, 3161, 3279, 3280, 3281, 3379, 3628,
3647, 3709, 3739, 3770, 3779, 3820, 3874, 4043, 4055, 4059,
4158, 4210, 4211, 4325, 4334, 4386, 4387, 4476, 4491, 4630,
4683, 4985, 5019, 5055, 5272, 5273, 5274, 5280, 5480, 5636,
5697, 5755, 5756, 5758, 5816, 5877, 5912, 5913, 5914, 5934,
6024, 6025, 6170



Strategy and Synergy for Security

Standards in PKI

- The **purpose of well-established standards** consists of two things: first, to facilitate **well-proven** and **well-specified techniques** and second, to **promote interoperability** among various systems and system components.
- Careful **selection of stable standards** would encourage **interoperability**. For example, the standard given by RSA Laboratory for Elliptic Curve Cryptography is **PKCS#13 which is not stable as yet**. Therefore we would prefer **minimal usage** of this standard.
- Another **IEEE P1363 standard** is defined for Public Key Cryptography but it doesn't mandate **minimum security requirements** which is our one of the major concern. This standard also gives **plenty of options** that definitely leads to interoperability problems.



Strategy and Synergy for Security

Standards in PKI

Standard Body and Working Group	Standard	Abbreviated Title
ANSI	ANSI X9.62	ECDSA
	ANSI X9.63	Key Agreement and Key Transport. Covers ECDH, ECMQV and ECIES
IEEE	P1363	In particular, it covers ECDSA, ECDH, ECIES and ECMQV
ISO	ISO/IEC 15946-1	Techniques based on elliptic curves – Part 1 : General
	ISO/IEC 15946-2	Part 2 – Digital Signatures
	ISO/IEC 15946-3	Part 3 – Key Establishment
	ISO/IEC 15946-4 (draft)	Part 4 – Digital Signature giving Message Recovery
	ISO/IEC 18033-2 (draft)	Encryption Algorithm – Part 2 : Asymmetric Ciphers



Strategy and Synergy for Security

Standards in PKI

Standard Body and Working Group	Standard	Abbreviated Title
NIST	FIPS 186-2	DSA, ECDSA
	FIPS 186-3	Allows generation of alternative curves using methods specified in ANSI X9.62
SECG	SEC1	ECDSA, ECDH, ECIES and ECMQV
	SEC2	Elliptic Curves listed
NESSIE	-	ECDSA, PSEC-KEM, ACE-KEM
IPA	-	ECDSA, ECDH, ECIES and PSEC-KEM
RSA LAB	PKCS#13	Public Key Cryptography

For a fully interoperable ECC based PKI implementation, we need to limit down the options of standards and protocols listed in the above tables.



Strategy and Synergy for Security

Part V

Case Study : Implementation of Customized ECC based PKI



Strategy and Synergy for Security

Implementation of Customized ECC based PKI

- Research on computation of cryptographically suitable elliptic curves is desirable for their use in the implementation of a PKI.
- The curve parameters are supposed to be well validated and tested against modern attacks. Security of a PKI highly relies upon the security of ECDLP offered by the chosen curve parameters.
- Huge mismatch of Standards is expected leading to interoperability and compatibility issues.
- All the applications taking part in the communication needs to be loaded with the same customized curves replacing standard curve parameters which is a very intricate task.
- Almost no supporting hardware is available commercially.
- Ultra sensitive applications needs requires proprietary curve parameters for implementation purposes.



Strategy and Synergy for Security

Part VI

Concluding Remarks



Strategy and Synergy for Security

Remarks

- PKI is a **complex** subject and **still evolving** in terms of its utilization in the commercial and e-commerce sectors.
- Although the underlying technology is quite sound, **issues** exist in areas such as **interoperability** and **performance**.
- A PKI hugely rely on **individual policies of usage**. To set up a PKI, a careful **planning is critical**.
- **First pilot PKI implemetation is suggested** to gain an understanding of the issues and the operational, security, and practical aspects particular to organizational environment.
- Its **pilot implementation will enable people with a clear understanding of focused goals and objectives**. **More comprehensive implementation and field deployment of PKI would be easier and comfortable afterwards**.



Strategy and Synergy for Security

Thank You!