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

Focus of this talk

Strategy and Synergy for Security

What should I do for implementing an ECC based PKI?

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.

IT Act for ECC based PKI in India

- Use of ECC became legally permitted asymmetric technique for End Entity Digial 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	5th Feb, 2002
2.	IDRBT	6th August, 2002
3.	National Informatics Centre	23rd May, 2003
4.	(n)Code Solutions	12th October, 2004
5.	E-mudhra CA	7th November, 2008
6.	CDAC CA	29th June, 2015
7.	Capricorn CA	16th May, 2016
8.	NSDL e-Gov CA	27th October, 2016

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

ECC/RSA based CA

RSA based CA

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.

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

Benefits of using ECC in PKI

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

  ECC is based on Elliptic Curve Discrete Logarithm Problem (ECDLP) having fully exponential time [$Time_{Elliptic\ Curve} \sim \exp(c\sqrt{N})$] 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 Comparision

- 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

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.

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.

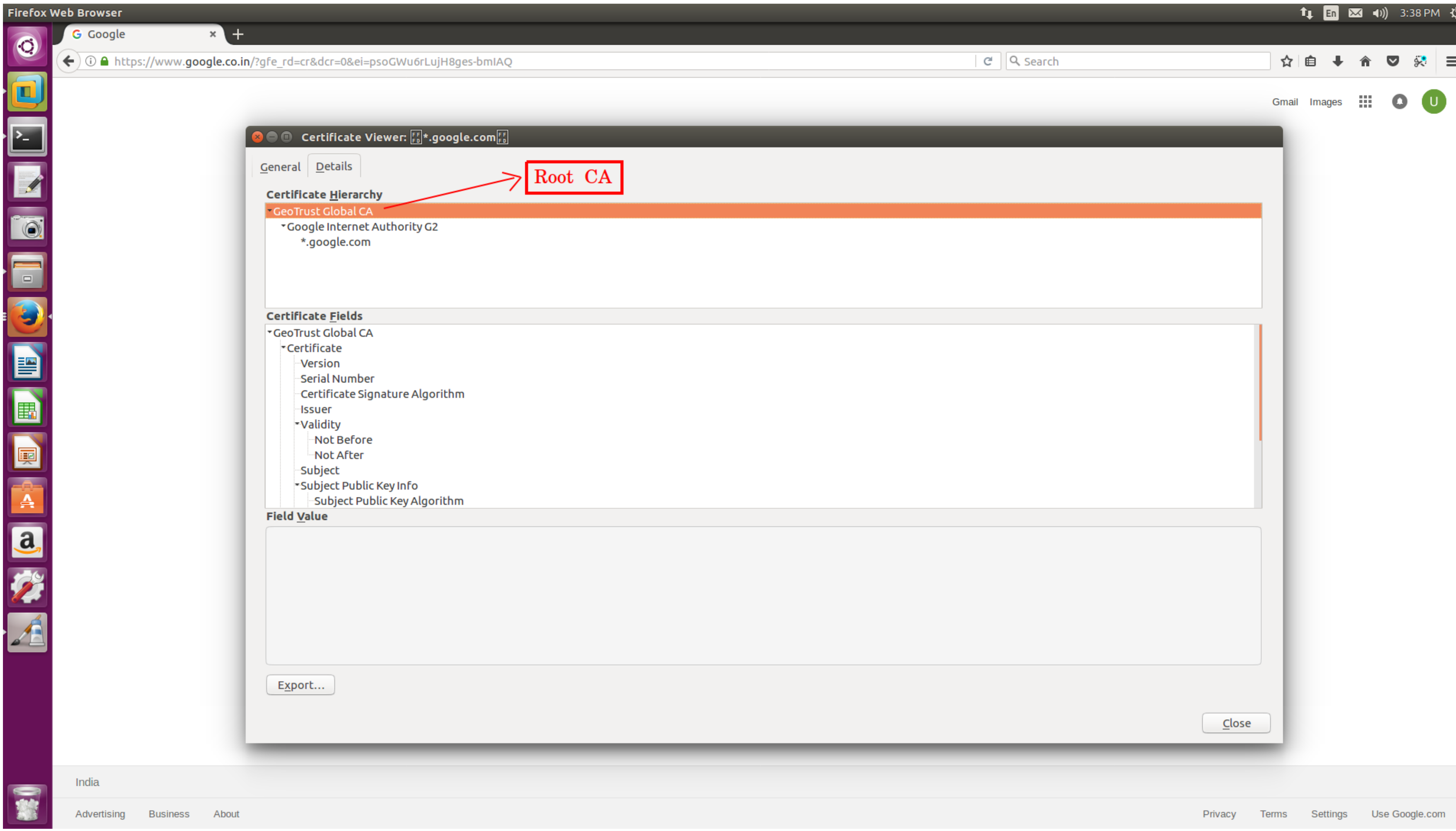
- The principal objective for developing a PKI is to enable secure, convenient and efficient acquisition of public keys.

- A PKI enables the establishment of a trust hierarchy.

- The implementation of a PKI using a Certification Authority (CA) provides the trust hierarchy.

Public Key Infrastructure (PKI)

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

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

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

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

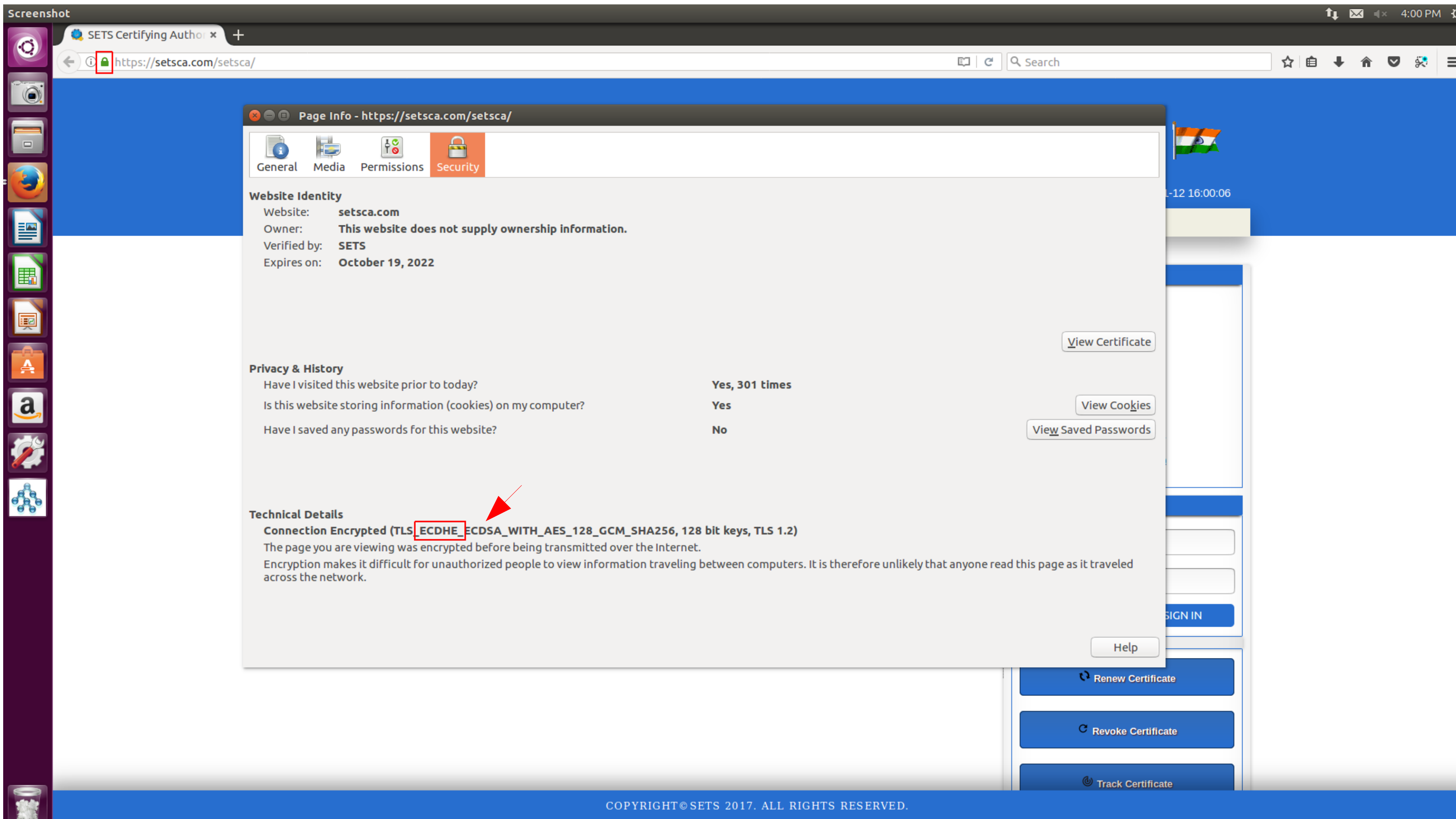
ECC is used as an alternative to RSA to achieve authentication, integrity, non-repudiation and key distribution purposes in the PKI.

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



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

Digital Signature as PKCS#7 attachment

```
--------------ms080800030504010205040602
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature
```


MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglghkgBZQMEAgMFADCABgkqhkiG9w0BBwEAAKCC
BkgwggLRMIICMqADAgECAgkA+ojwJkXzcIgwCgYIKoZIzj0EAwQwWjELMAkGA1UEBhMCSU4x
CzAJBgNVBAgMAlROMRAwDgYDVQQHDAdDaGVubmFpMQ0wCwYDVQQKDARTRVRTMQwwCgYDVQQL
DANBQ0cxDzANBgNVBAMMBkNBY2VydDAeFw0xNzAyMDMwNjUwMTFaFw0xODAyMDMwNjUwMTFa
MIGAMQswCQYDVQQGEwJJTjELMAkGA1UECAwCVE4xEDAOBgNVBAcMB0NoZW5uYWkxDTALBgNV
BAoMBFNFVFMxDDAKBgNVBAsMA0FDRzEQMA4GA1UEAwwHdXNlclR3bzEjMCEGCSqGSIb3DQEJ
ARYUdXNlcjIuc2V0c0BnbWFpbC5jb20wgZswEAYHKoZIzj0CAQYFK4EEACMDgYYABACYXNDT
SEP1ogWKrhXWQXHOvEkmLOPH0eWDEmboy7G7x211GBbglM4fzBCnkHHpCqBTw8HM9Eo8ZTAF
YinBQsZMwABAyeudzn/55E/MNe4PgV8m6yMSBMKOCi78W/NQNOQ2SdsKk6adqut7CR4TQqEw
pqX8pJ/jeNCtLyiut7LNghwmKKN3MHUwHQYDVR0OBBYEFGnL4edlToJtD2DyW8Oa5WdJ6Gam
MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgH2MDwGA1UdHwQ1MDMwMaAvoC2GK2h0dHBzOi8vc2V0
c2NhLmNvbS9zZXRzY2ExL0NSTC9jcmxfbGlzdC5jcmwwCgYIKoZIzj0EAwQDgYwAMIGIAkIA
pXUD9Jtb39CyWMhtylKeAUdZehG6DZyEwCTghHsg2QfUKt5xzhvE5jmG2XGIjJnZTJQh6RR8
j+ifnSDJswV+2PgCQgEa9TWb992dRwADKGmnCRACaSn/XZ7HdhNxWxot6QQmfhQ4dEJfAmmR
GAqihqW2PuBUKqW6WvaceGBRC3qGl4qGtDCCA28wggLQoAMCAQICCQC5bUOnHsDAWzAKBggq
hkjOPQQDBDB/MQswCQYDVQQGEwJJTjELMAkGA1UECAwCVE4xEDAOBgNVBAcMB0NoZW5uYWkx
DTALBgNVBAoMBFNFVFMxDDAKBgNVBAsMA0FDRzEPMA0GA1UEAwwGQ0FjZXJ0MSMwIQYJKoZI
hvcNAQkBFhRzZXRzY2FtYWlsQGdtYWlsLmNvbTAeFw0xNzAxMTkxMjIwNTdaFw0xODAxMTkx
MjIwNTdaMFoxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJUTjEQMA4GA1UEBwwHQ2hlbm5haTEN
MAsGA1UECgwEU0VUUzEMMAoGA1UECwwDQUNHMQ8wDQYDVQQDDAZDQWNlcnQwgZswEAYHKoZI
zj0CAQYFK4EEACMDgYYABAGg3o+zWwh0tfrswSjnvVis1ncrENxjwsrNn2m/2rubOsTY/+bs
oJQjwHCfI+b60b5dGPR+KIvhJQfzl4TilMdS3AFfhmeeOrm/9sJlmhieuhUplT6IlH7gE694
iSmEOyEksnfskusjSEvoWUyX5M6YY3K8BfBZ+RKI1u+1YVnVjeSauKOCARUwggERMB0GA1Ud
DgQWBBTYKEWfiNqbafEuup8+iro4TxJfPDAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIB9jCB
swYDVR0jBIGrMIGogBTYKEWfiNqbafEuup8+iro4TxJfPKGBhKSBgTB/MQswCQYDVQQGEwJJ
TjELMAkGA1UECAwCVE4xEDAOBgNVBAcMB0NoZW5uYWkxDTALBgNVBAoMBFNFVFMxDDAKBgNV
BAsMA0FDRzEPMA0GA1UEAwwGQ0FjZXJ0MSMwIQYJKoZIhvcNAQkBFhRzZXRzY2FtYWlsQGdt
YWlsLmNvbYIJALltQ6cewMBbMB8GA1UdEQQYMBaBFHNldHNjYW1haWxAZ21haWwuY29tMAoG
CCqGSM49BAMEA4GMADCBiAJCAKYxVtJ04UG66qTie5Nzm7tM+FBXpPdSTFaDxexJdamt4vSI
oHgA5XuAmEMtp8Om4wrNOu91eFmPO43KKaNU+8vvAkIBwiBfLw/iADZL2zZgJvGK/qqCcUci
wmwqivu/3QxaOcy7va6hK/e+wOzVE3uoKN7bzfxtOHAd6zxfol/HkQhxJR4xggMFMIIDAQIB
ATBnMFoxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJUTjEQMA4GA1UEBwwHQ2hlbm5haTENMAsG
A1UECgwEU0VUUzEMMAoGA1UECwwDQUNHMQ8wDQYDVQQDDAZDQWNlcnQCCQD6iPAmRfNwiDAN
BglghkgBZQMEAgMFAKCCAekwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0B
CQUxDxcNMTcwMjAzMDcwODA1WjBPBgkqhkiG9w0BCQQxQgRA44M6mmO7V4KKFLWGFpmnDeny
YaSQFcv9neGqhFDQGyYQHEd1kgVBvk01eYCcEM8gXmXNlskHiusd9kiLO/PYqDBsBgkqhkiG
9w0BCQ8xXzBdMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAQIwCgYIKoZIhvcNAwcwDgYIKoZI
hvcNAwICAgCAMA0GCCqGSIb3DQMCAgFAMAcGBSsOAwIHMA0GCCqGSIb3DQMCAgEoMHYGCSsG
AQQBgjcQBDFpMGcwWjELMAkGA1UEBhMCSU4xCzAJBgNVBAgMAlROMRAwDgYDVQQHDAdDaGVu
bmFpMQ0wCwYDVQQKDARTRVRTMQwwCgYDVQQLDANBQ0cxDzANBgNVBAMMBkNBY2VydAIJAPqI
8CZF83CIMHgGCyqGSIb3DQEJEAILMWmgZzBaMQswCQYDVQQGEwJJTjELMAkGA1UECAwCVE4x
EDAOBgNVBAcMB0NoZW5uYWkxDTALBgNVBAoMBFNFVFMxDDAKBgNVBAsMA0FDRzEPMA0GA1UE
AwwGQ0FjZXJ0AgkA+ojwJkXzcIgwCQYHKoZIzj0CAQSBizCBiAJCATDYu+e1WZWrZhe0MDki
U9awORj8ScCiigeHwYPsKFL46Unixs7BxZmDV6Gxnk4hI/CQfJ5dp7Ls0+qGdKo6WFFYAkIB
lSI+o0/VIlk6p9CjXpcyfLDVJ+rcVXDYjbUpdToAlMiRAO6avst64eILW2u1Xqwk984P1ZNc
Kx+FbCOljcXHW/cAAAAAAAA=


```
--------------ms080800030504010205040602--
```

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.

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

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

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 $V= u_1 G + u_2Q$
3. Declares Signature valid if **V = R**

If message is signed correctly, the verification equation holds:

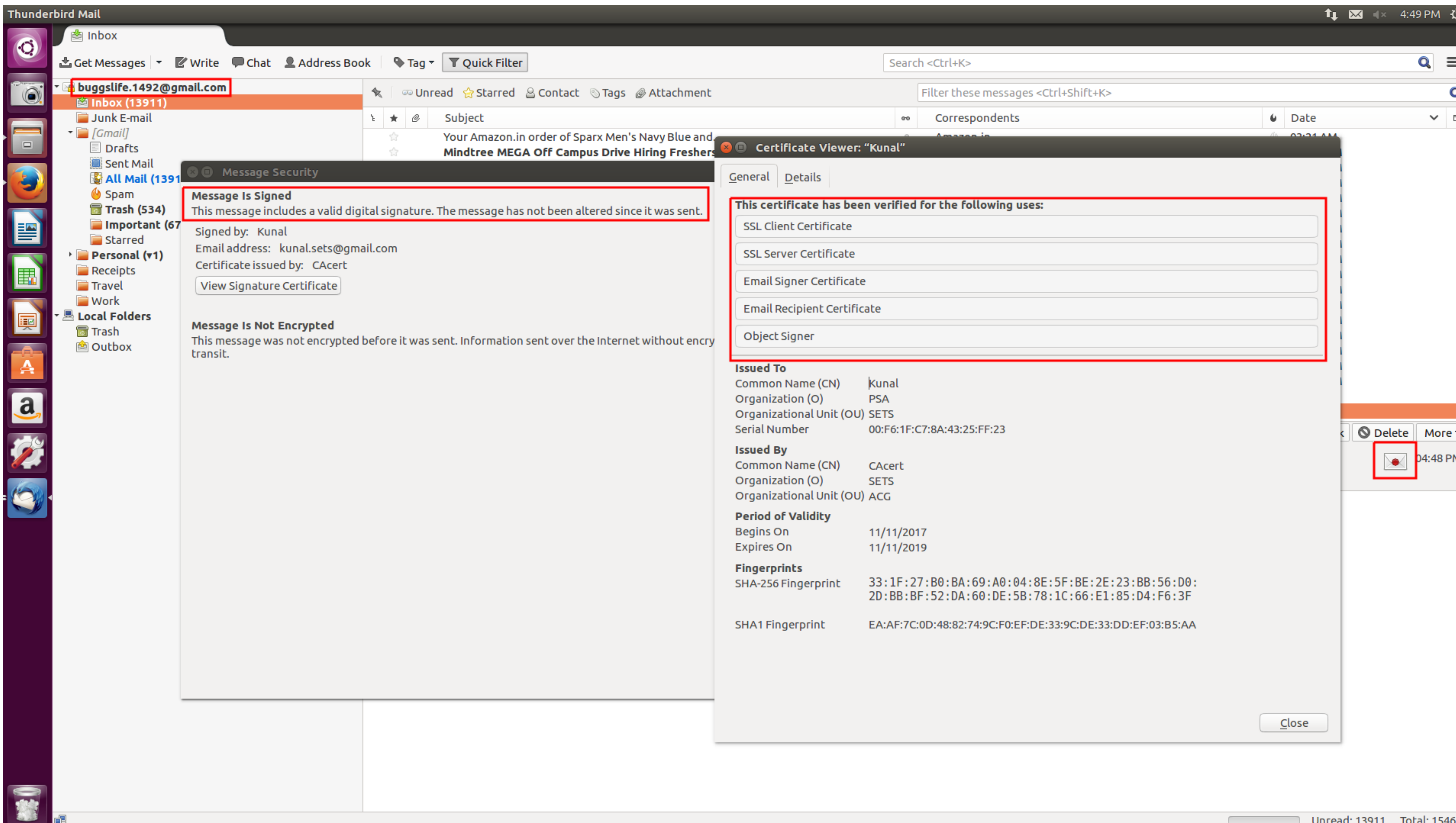
$$
\begin{aligned}
V &= u_1 G + u_2Q \\
&= s^{-1}m * G + s^{-1}xQ \\
&= s^{-1} (mG + xQ) \\
&= s^{-1}(mG + xaG) = s^{-1}G (m + ax) \\
&= s^{-1} * G * s * k = kG = R
\end{aligned}
$$

So, **V = R**

Strategy and Synergy for Security

Digital Signatures

Screenshot for E-mail Signing :



Digital Certificates

- CAs provide digital certificates as proof of the ownership of public keys.

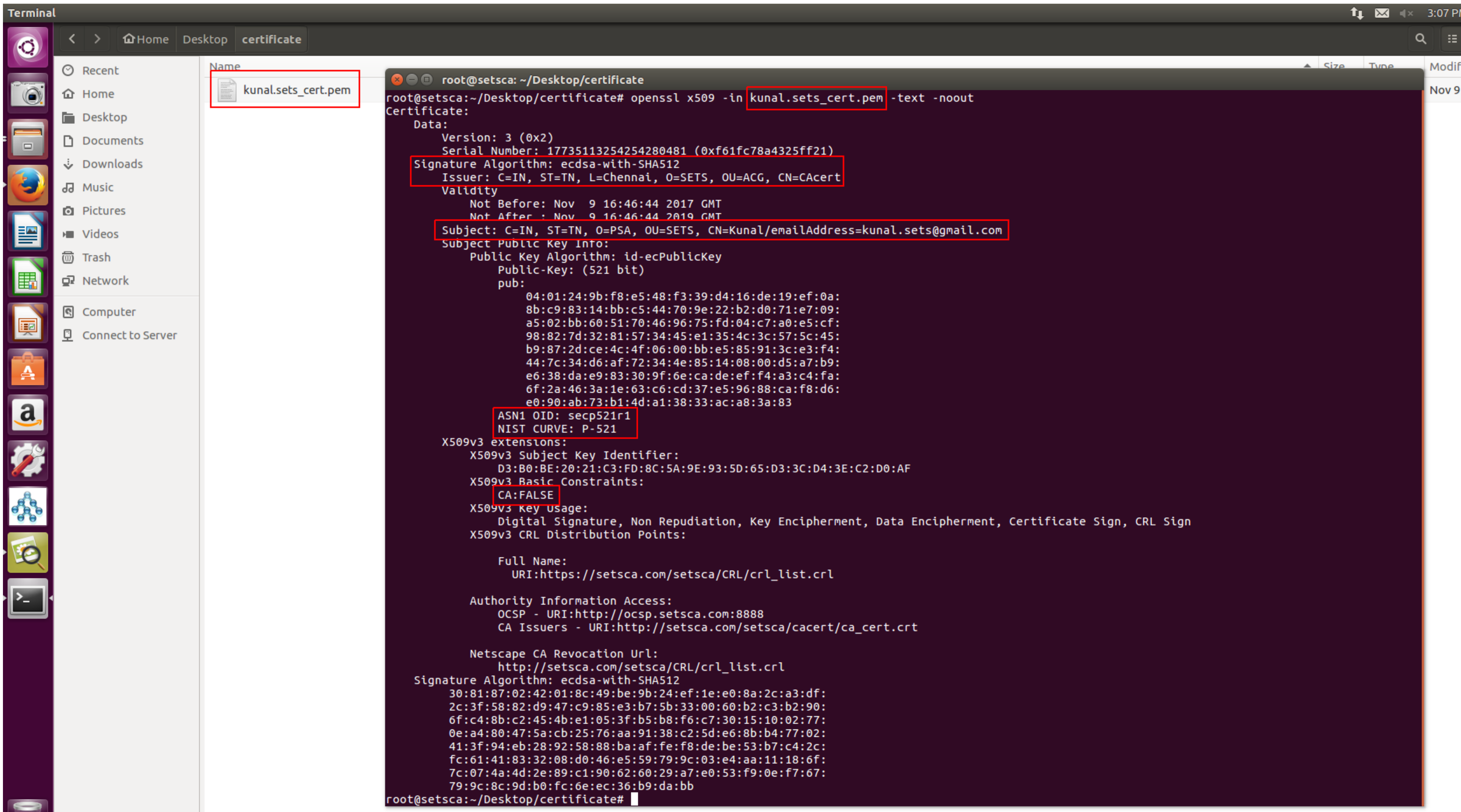
- A digital certificate binds the owner's public key, name, E-mail and other necessary information together.

- 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.

Digital Certificates

- X.509 Certificate (Elliptic Curve based)

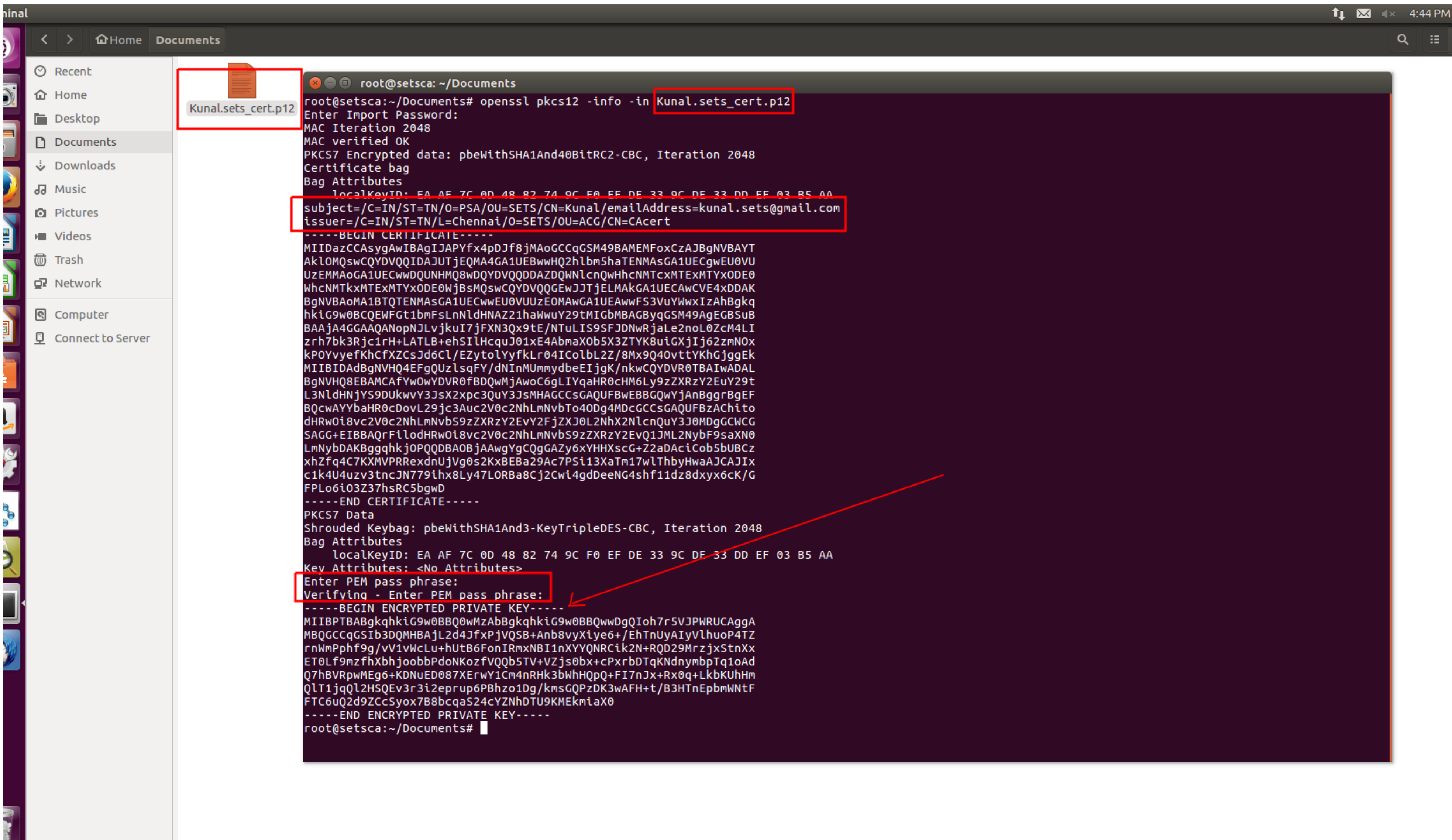


Digital Certificates

- 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

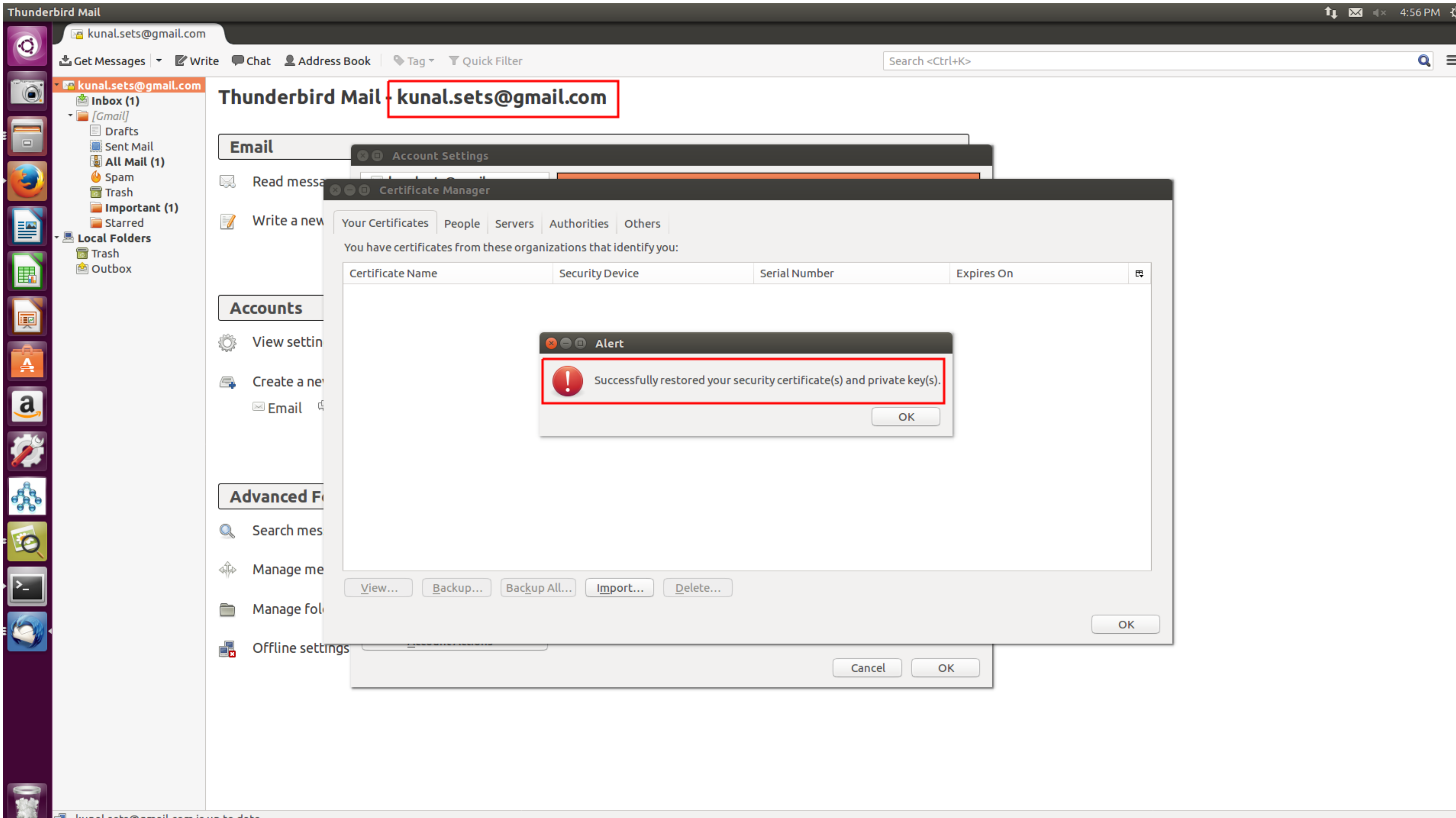
- Example : Screenshot of .p12 certificate structure



Strategy and Synergy for Security

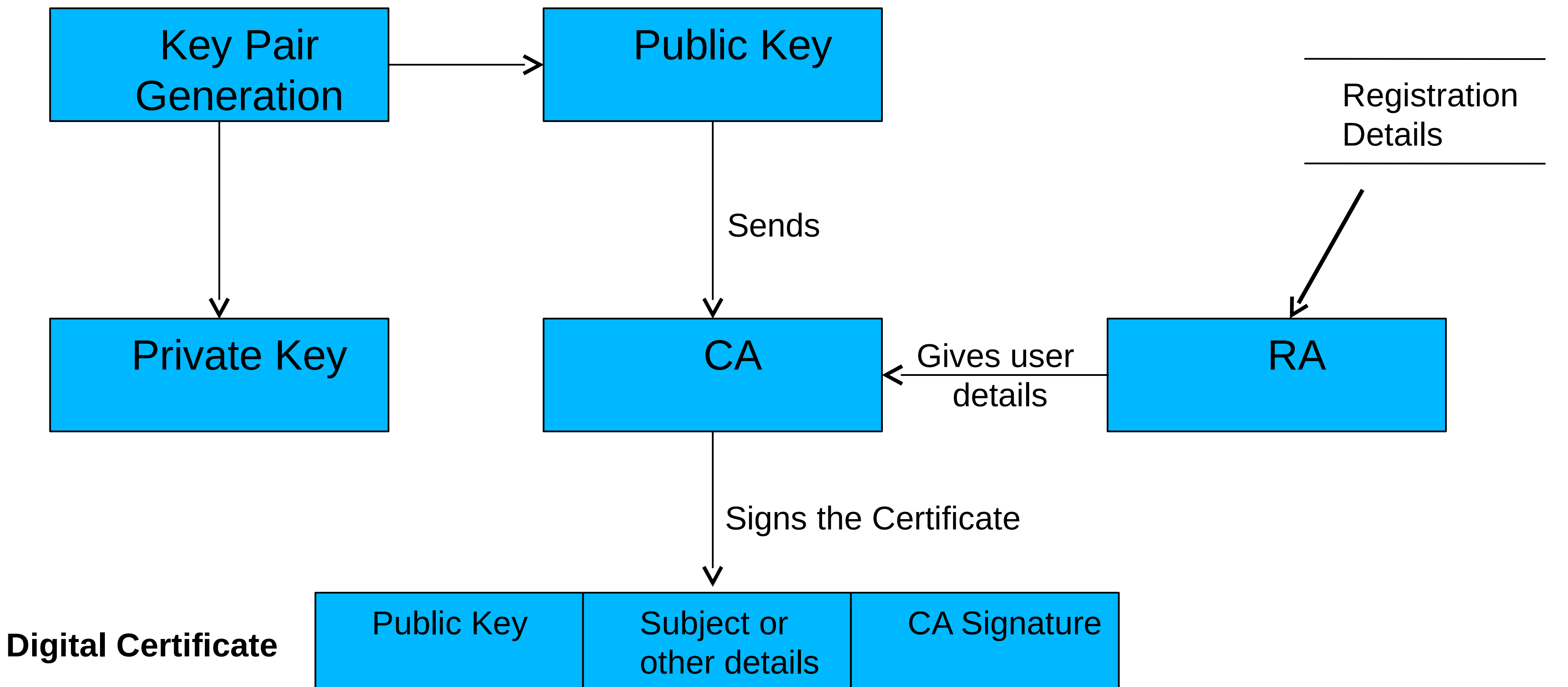
Digital Certificates

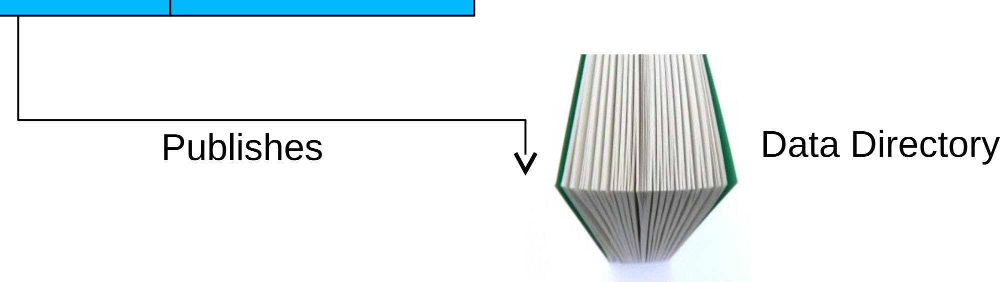
Screenshot : User certificate in P12 format having encrypted private key



Digital Certificates

- Public Key Distribution through digital Certificate :





Public keys are distributed in certificates, which are signed by a trusted CA.

PKI Components

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

PKI Functions

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

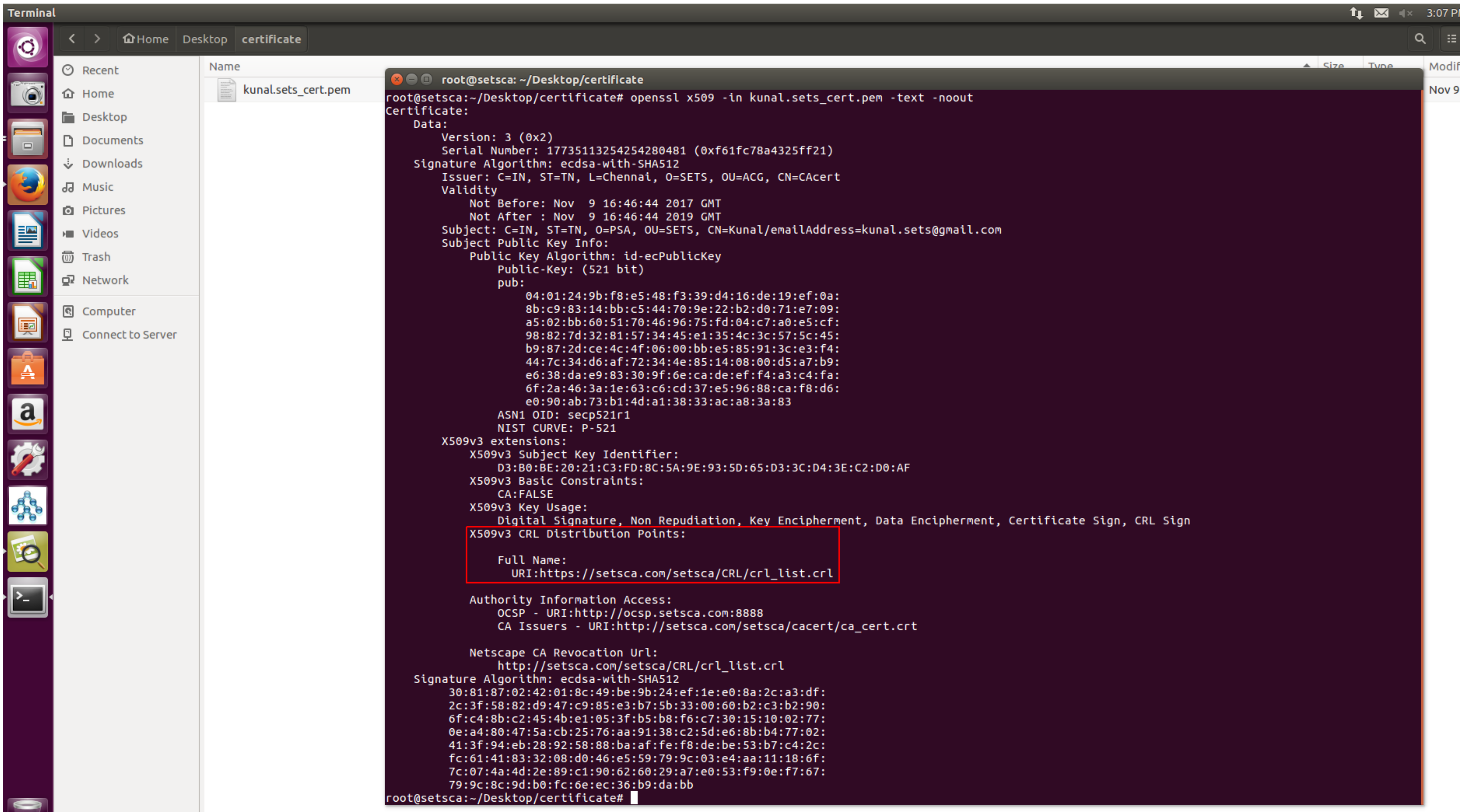
PKI Functions

- 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.

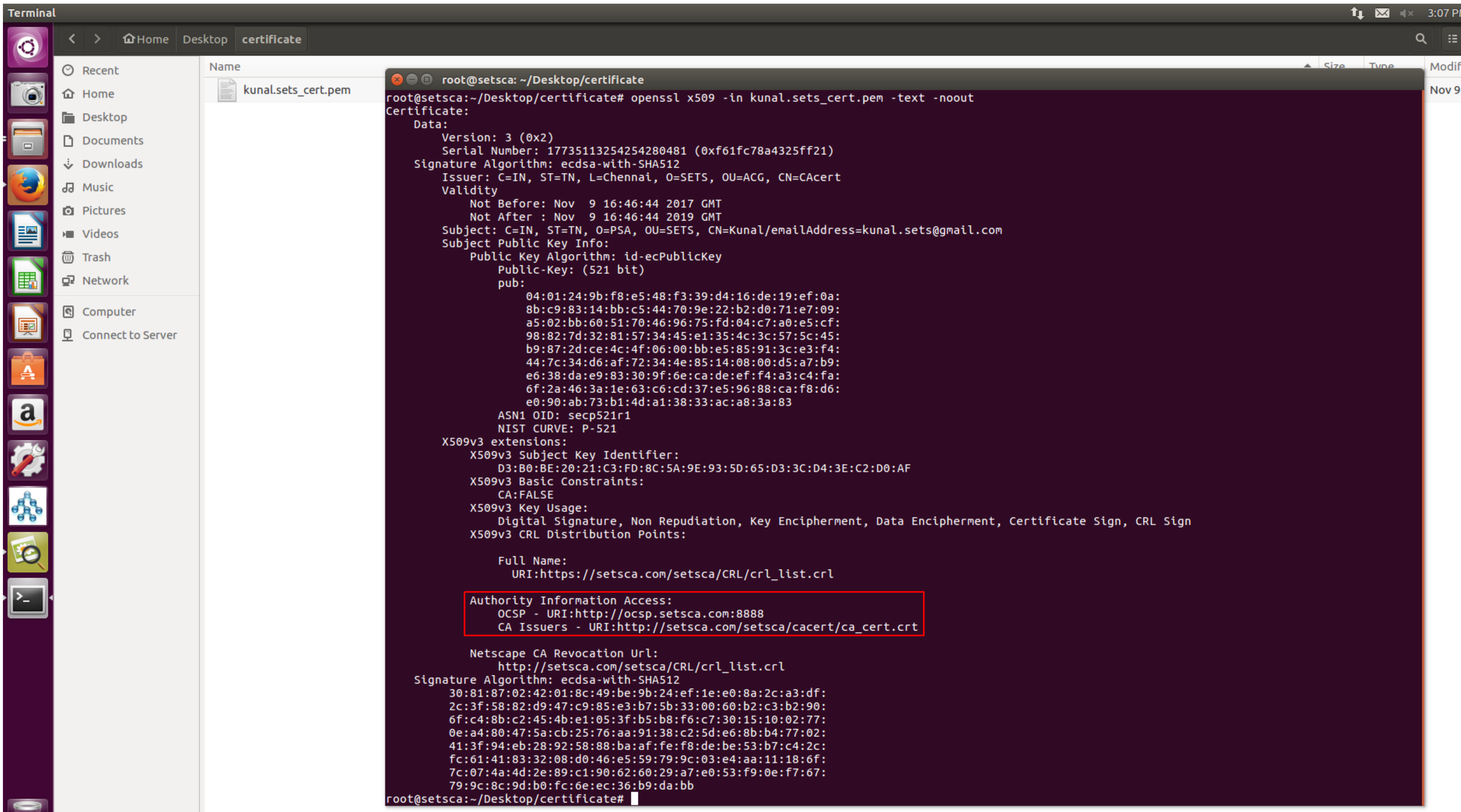
Strategy and Synergy for Security

PKI Functions



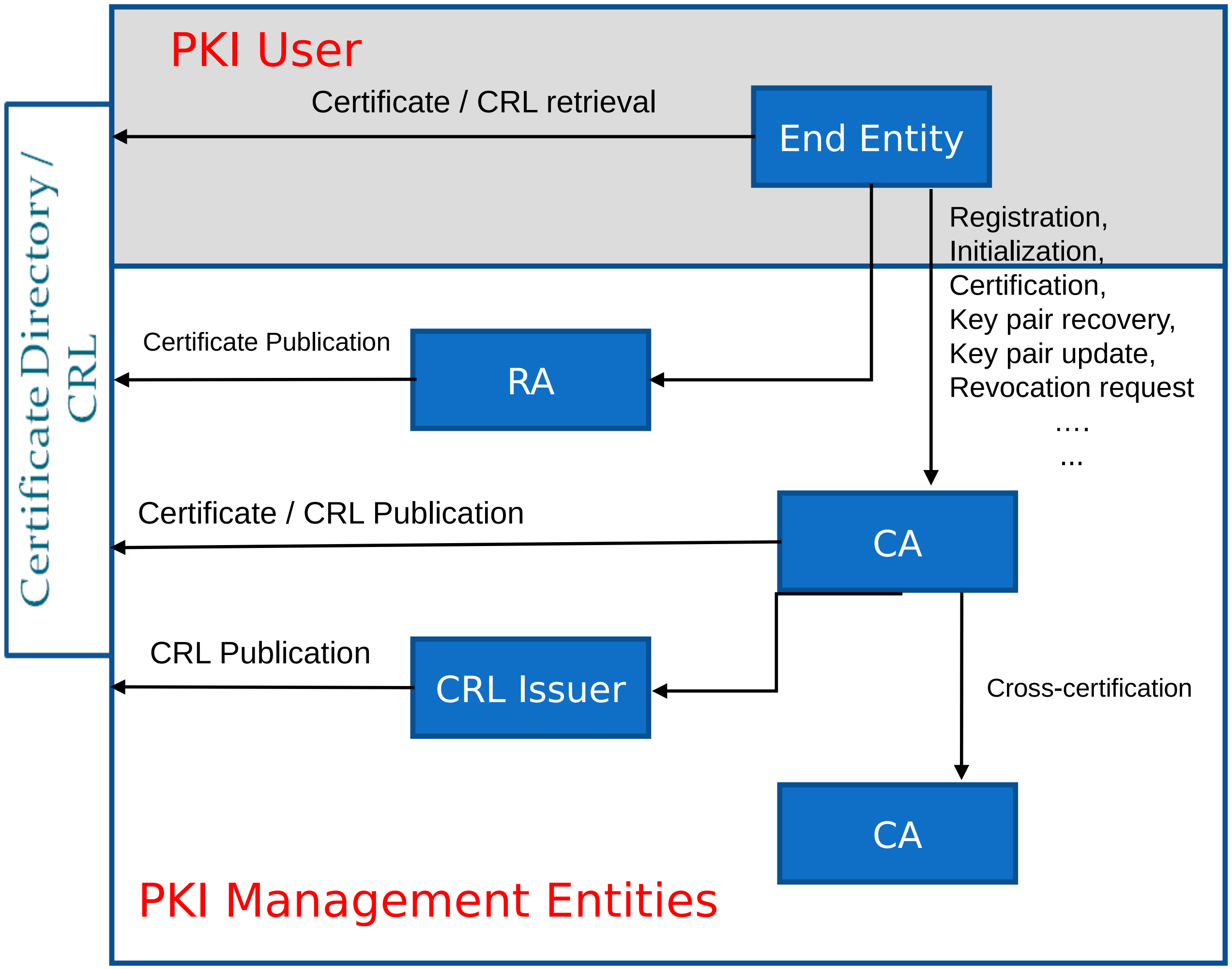
PKI Functions

- Online Certificate Status Protocol (OCSP)



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

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.

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.

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.

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.

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.

Part IV

RFCs and Standards on ECC based PKI

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

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

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

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 depoyment of PKI would be easier and comfortable afterwards.

Strategy and Synergy for Security

Thank You!