Public Key Infrastructure (PKI)

Hari.K
NIELIT Calicu

Demo

- http://www.cs.toronto.edu/~arnold/427/19s/427_19S/tool/ssl/notes.pdf
-

Basics of Public Key Infrastructures

- A PKI is a **structure** that provides all of the necessary components for different types of users and entities to be able to communicate securely and in a predictable manner.
- A PKI is **made up of** hardware, applications, policies, services, programming interfaces, cryptographic algorithms, protocols, users, and utilities.

What does the “infrastructure” in “**public key infrastructure**” really mean?

- An infrastructure provides a sustaining groundwork for other things to be built upon.

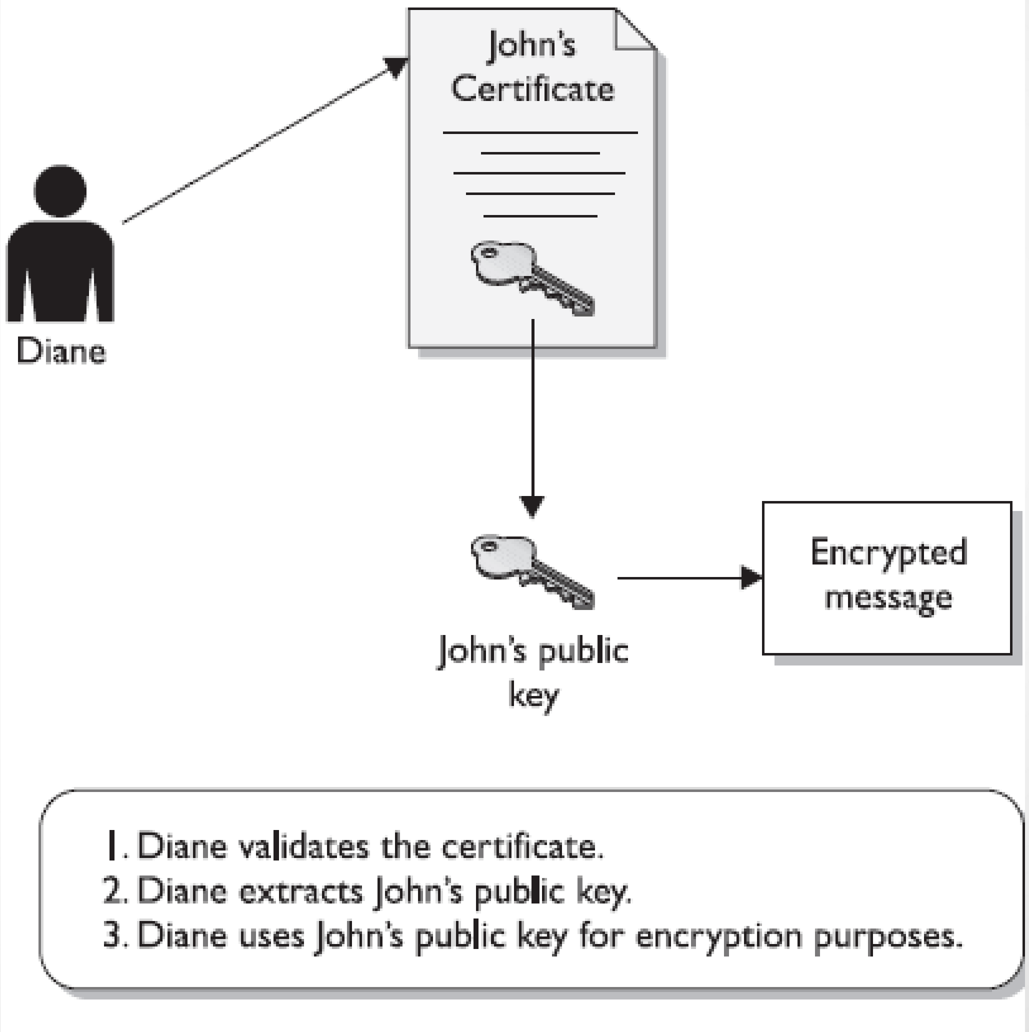
Digital Certificates

- A digital certificate binds an individual’s identity to a public key, and it contains all the information a receiver needs to be assured of the identity of the public key owner.
- The certificates are created and formatted based on the X.509 standard.

Digital Certificate....

- A digital certificate, also known as a public key certificate, is used to cryptographically link ownership of a public key with the entity that owns it.
- Digital certificates are for sharing public keys to be used for encryption and authentication.
- Digital certificates include:
  - The public key being certified
  - Identifying information about the entity
  - Metadata relating to the digital certificate
  - Digital signature of the public key the certificate issuer created.

Public key is part of Digital Certificate



1. Diane validates the certificate.
2. Diane extracts John's public key.
3. Diane uses John's public key for encryption purposes.

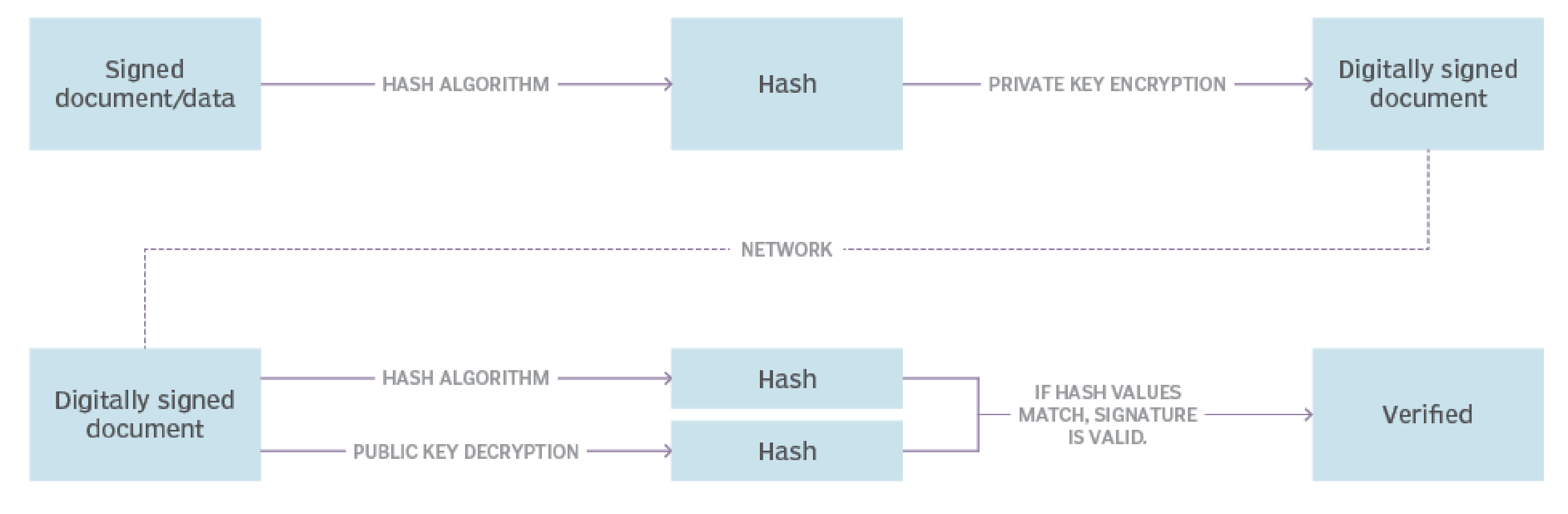
PKI vs Digital Certificates

- PKI is the system that distributes and authenticates public keys.
- The distribution, authentication and revocation of digital certificates are the primary functions of the public key infrastructure (PKI)

What is a digital signature ?

- Takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint.”
- This "fingerprint,” or coded message, is unique to both the document and the signer and binds both of them together.
- It is essentially required to prove his/her identity in an electronic transaction.

The Digital Signatue Process



Why digital signature is required for a electronic transaction ?

- A digital signature is used to achieve the properties of a manual signature:
- It establishes Authenticity (Establishing the identity of the Person who has signed it)
- Integrity (That the documents is unchanged after Signing it)
- Non repudiation (That the person who has signed cannot deny it later).

What is the legal validity of a digitally signed document ?

- The Information Technology act has accorded authentication of electronic document by the means of digital signature issued by a licensed Certifying Authority under the Controller of Certifying Authority, Ministry of IT, India.

Who is a CA (Certifying Authority) ?

- A certifying authority is a body entrusted to issue, revoke, and renew Digital Signature Certificate.
- The digital signature certificate of the applicant is signed by the CA.
- Under Sec 24, of the Information Technology Act 2000 a Certifying Authority means a Person who has been granted license to issue Digital Signature Certificates.
- A list of Valid CA in India can be traced at https://cca.gov.in/cca/?q=licensed_ca.html

Where can I use a digital signature ?

A digital Signature Can be used for:

- Securing mail by signing and Encrypting the Same
- Signing PDF, Word, Excel Files
- Filing Income Tax Return
- Filing E Forms with the Ministry of Corporate affairs
- Submit of E Tenders , Bids.

Where can I apply/procure DSC ?

- A Digital Signature Certificate can be procured from any CA (Certifying authority) in India.
- A list of Valid CA in India can be traced at https://cca.gov.in/cca/?q=licensed_ca.html.
- In India, CA's generally appoints RA/LRA (Licensed Registration Authority) who undertake the verification of the digital signaure subscriber on behalf of the CA.
- DSC can also be procured though such RA/LRA

Different types of certificate

Class of Signature are legally valid and used generally are:

- **Class 2 Digital Signature**: Here the identity of the person is verified against a trusted and pre verified database.
- **Class 3 Digital Signature:** This provides highest level of assurance as the certificate applicant has to prove his identity in front of the Registration Authority.

What is revocation of a certificate ?

- A DSC can be revoked if the DSC private key has been compromised, the subscriber details are changed, or change in relationship with the employer.
- For details on revocation you can contact the CA (Certifying Authority) or RA/LRA (Licensed Registration Authority) from whom you have validated and purchased you certification

How do I ensure security of my digital signature ?

A digital signature private key has to be stored securely; you can do the same by

- Protecting the private key with good password
- Storing the digital signature in Crypto Tokens/USB Based Smart Cards or Tokens
- Protect computer from unauthorized access

What should I do if I lose my DSC ?

- You should immediately apply for revocation of the certificate and apply for new one.

What is a crypto token (e-Token) ?

- A crypto Token is a smart card based USB device which is used for the storage of your DSC.
- A crypto token is called by other name like dongles, USB etc.
- It has a USB interface which can be easily connected to he computer USB port for easy usage.

e-Token

- USB e-Token is looks like a USB drive but these are secured by Federal Information Processing Standard (FIPS).
- Digital Signature Certificates stored in e-Token can not be copied to any other device thus providing another layer to your identity security.

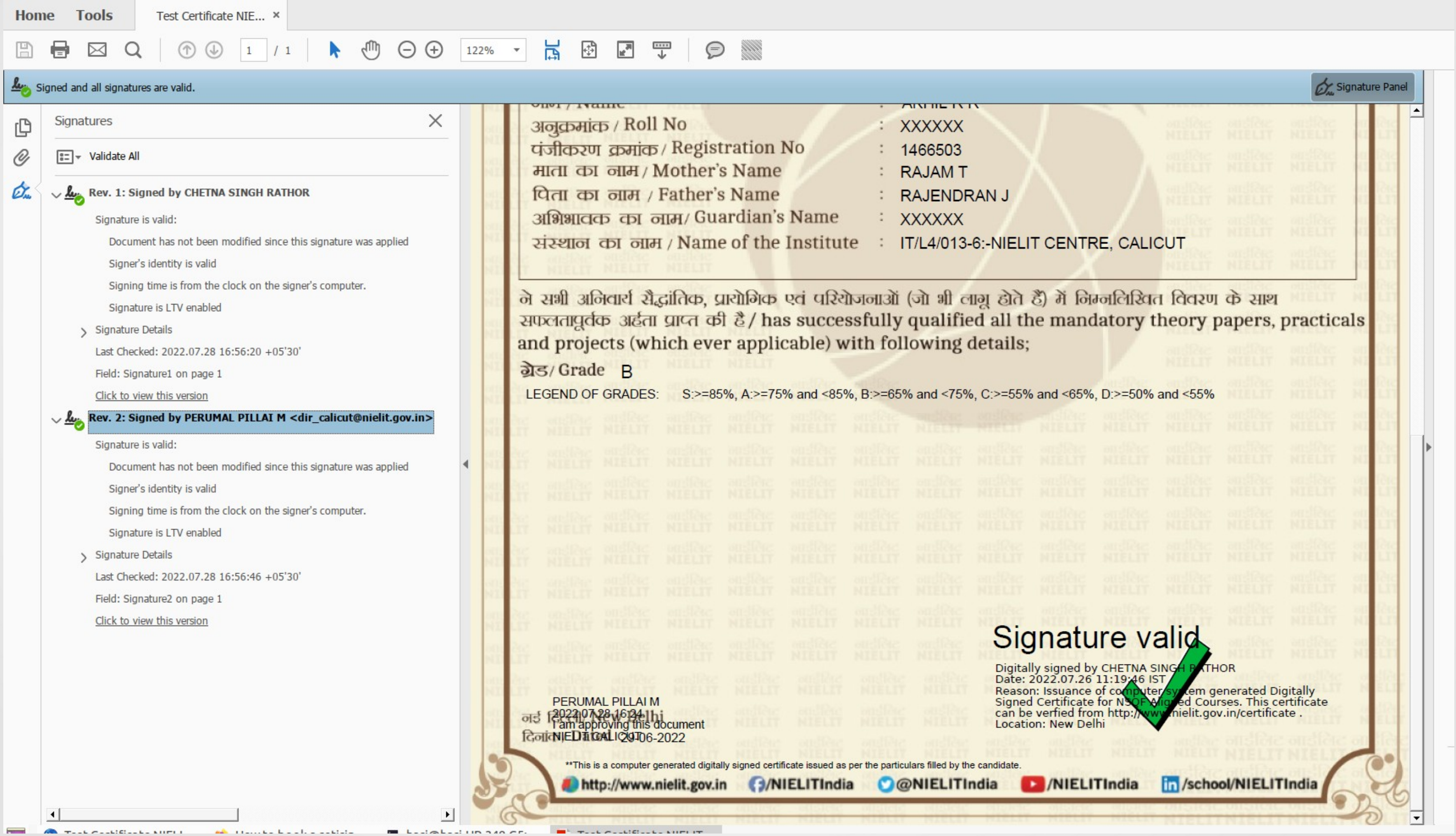
Why do I require a USB crypto token ?

- A USB Crypto token securely stores your DSC with Strong passwords.
- Further it provides mobility to your DSC when you have to perform signing on multiple computers.
- Your digital signature is vulnerable to key compromise if many users access the same machine on which you sign the documents with you DSC - the same can be avoided with the help of a token.
- CCA (Controller of Certifying Authorities) vide its office order dated 25th Oct 2013 has mandated issuance of class 2 and class 3 digital signatures on a FIPS level 2 certified token

What is FIPS 140-2 encryption?

- FIPS (Federal Information Processing Standards) is a set of standards that describe document processing, encryption algorithms and other information technology processes for use within non-military federal government agencies and by government contractors and vendors who work with these agencies.
- The publications pertaining to these standards (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to FISMA.
- The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating that the cryptographic modules produced by private sector companies meet well-defined security standards. FIPS PUB 140-2 provides details about the Security Requirements For Cryptographic Modules.

Signed Document - sample



Signed and all signatures are valid.

Signatures

Validate All

Rev. 1: Signed by CHETNA SINGH RATHOR

Signature is valid:

- Document has not been modified since this signature was applied
- Signer's identity is valid
- Signing time is from the clock on the signer's computer.
- Signature is LTV enabled

Signature Details

Last Checked: 2022.07.28 16:56:20 +05'30'

Field: Signature1 on page 1

Click to view this version

Rev. 2: Signed by PERUMAL PILLAI M <dir_calicut@nielit.gov.in>

Signature is valid:

- Document has not been modified since this signature was applied
- Signer's identity is valid
- Signing time is from the clock on the signer's computer.
- Signature is LTV enabled

Signature Details

Last Checked: 2022.07.28 16:56:46 +05'30'

Field: Signature2 on page 1

Click to view this version

अनुक्रमांक / Roll No	:	XXXXXX
पंजीकरण क्रमांक / Registration No	:	1466503
माता का नाम / Mother's Name	:	RAJAM T
पिता का नाम / Father's Name	:	RAJENDRAN J
अभिभावक का नाम/ Guardian's Name	:	XXXXXX
संस्थान का नाम / Name of the Institute	:	IT/L4/013-6:-NIELIT CENTRE, CALICUT

ने सभी अनिवार्य सैद्धांतिक, प्रायोगिक एवं परियोजनाओं (जो भी लागू होते हैं) में निम्नलिखित विवरण के साथ सफलतापूर्वक अर्हता प्राप्त की है / has successfully qualified all the mandatory theory papers, practicals and projects (which ever applicable) with following details;

ग्रेड/ Grade B

LEGEND OF GRADES: S:>=85%, A:>=75% and <85%, B:>=65% and <75%, C:>=55% and <65%, D:>=50% and <55%

PERUMAL PILLAI M
2022.07.28 16:24
I am approving this document
NIELIT CALICUT

नई दिल्ली / New Delhi
दिनांक / Dated : 29-06-2022

Signature valid

Digitally signed by CHETNA SINGH RATHOR
Date: 2022.07.26 11:19:46 IST
Reason: Issuance of computer system generated Digitally Signed Certificate for NSQF Aligned Courses. This certificate can be verfied from http://www.nielit.gov.in/certificate .
Location: New Delhi

**This is a computer generated digitally signed certificate issued as per the particulars filled by the candidate.

http://www.nielit.gov.in /NIELITIndia @NIELITIndia /NIELITIndia /school/NIELITIndia

Demo

- tinyCA/XCA

Additional Points

Certification practices statement (CPS)

- Every CA should have a *CPS* that outlines how identities are verified, the steps the CA follows to generate, maintain, and transmit certificates, and why the CA can be trusted to fulfill its responsibilities.
- It describes how keys are secured, what data is placed within a digital certificate, and how revocations will be handled.

Certificate server

- The *certificate server* is the actual service that issues certificates based on the data provided during the initial registration process.
- The server constructs and populates the digital certificate with the necessary information and combines the user’s public key with the resulting certificate.
- The certificate is then digitally signed with CA’s private key.

Registration Authorities

- The *registration authority (RA)* is the component that accepts a request for a digital certificate and performs the necessary steps of registering and authenticating the person requesting the certificate.
- The authentication requirements differ depending on the type of certificate being requested.

Certificate Repositories

- A *certificate repository* is a holding place for individuals’ certificates and public keys that are participating in a particular PKI environment.
- The directories are usually LDAP-compliant.

Trust and Certificate Verification

- When a user chooses to trust a CA, they will download that CA’s digital certificate and public key, which will be stored on their local computer.
- Most browsers have a list of CAs configured to be trusted by default, so when a user installs a new web browser several of the most well-known and most trusted CAs will be trusted without any change of settings

Steps for validating a certificate

1. Compare the CA that digitally signed the certificate to a list of CAs that have already been loaded into the receiver's computer.
2. Calculate a message digest for the certificate.
3. Use the CA's public key to decrypt the digital signature and recover what is claimed to be the original message digest embedded within the certificate.
4. Compare the two resulting message digest values to ensure the integrity of the certificate.
5. Review the identification information within the certificate, such as the e-mail address.
6. Review the validity dates.
7. Check a revocation list to see if the certificate has been revoked.

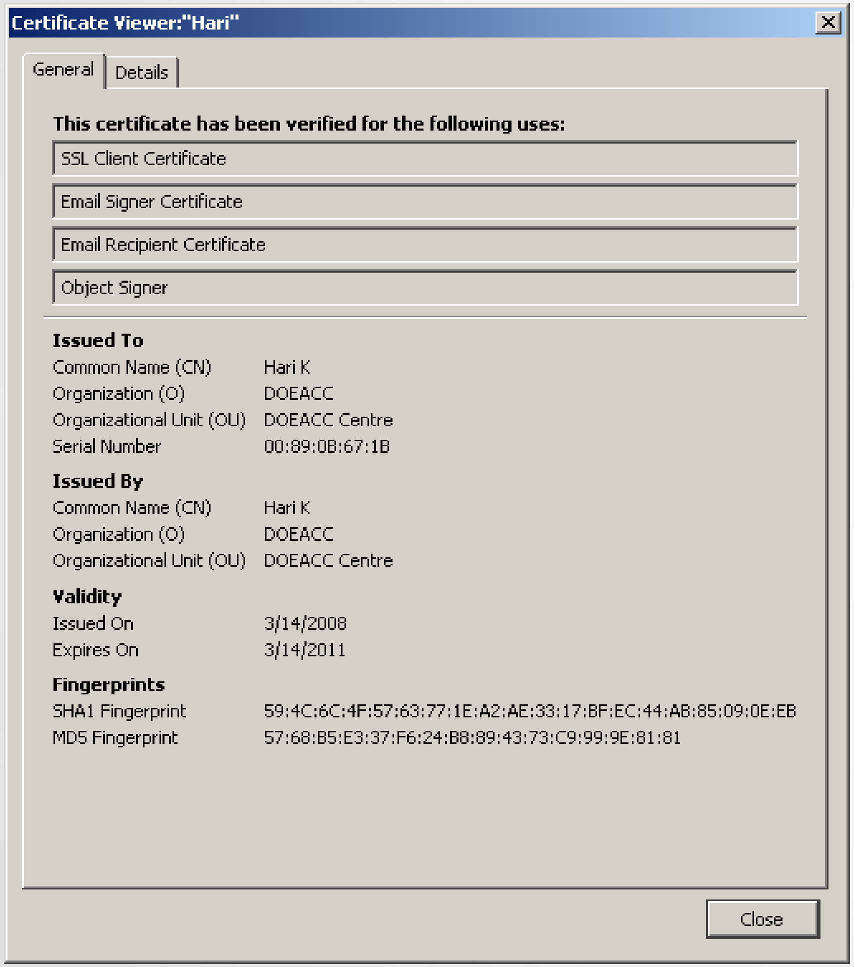
The different fields within a digital certificate

- **Version number** Identifies the version of the X.509 standard that was followed to create the certificate. The version number indicates the format and fields that can be used.
- **Subject** Specifies the owner of the certificate.
- **Public key** Contains the public key being bound to the certified subject. The public key also identifies the algorithm that was used to create the private/public key pair.
- **Issuer** Identifies the CA that generated and digitally signed the certificate.
- **Serial number** Contains a unique number identifying this one specific certificate issued by a particular CA

different fields contd..

- **Validity** Specifies the dates through which the certificate is valid for use.
- **Certificate usage** Specifies the approved use of certificate, which dictates what the user can use this public key for.
- **Signature algorithm** Identifies the hashing algorithm and digital signature algorithm used to digitally sign the certificate.
- **Extensions** Allow additional data to be encoded into the certificate to expand the functionality of the certificate. Companies can customize the use of certificates within their environment by using these extensions. X.509 version 3 has extended the extension possibilities.

Examples – from Mozilla Firefox



This certificate has been verified for the following uses:

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

Issued To

Common Name (CN)	Hari K
Organization (O)	DOEACC
Organizational Unit (OU)	DOEACC Centre
Serial Number	00:89:0B:67:1B

Issued By

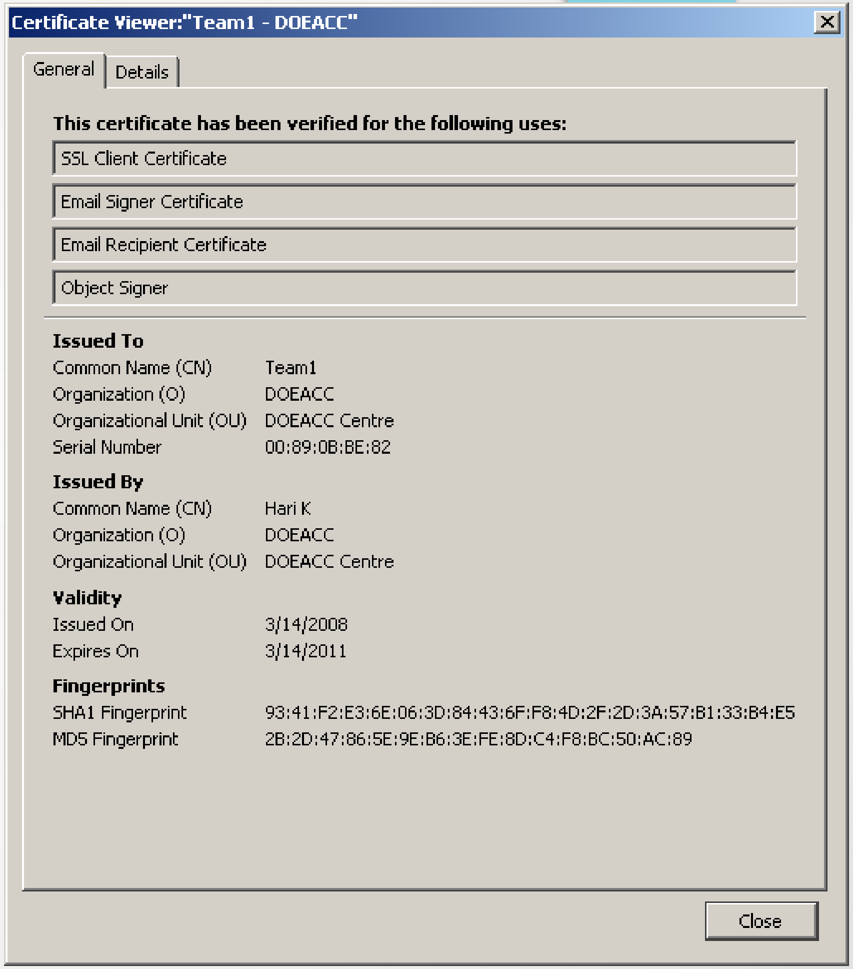
Common Name (CN)	Hari K
Organization (O)	DOEACC
Organizational Unit (OU)	DOEACC Centre

Validity

Issued On	3/14/2008
Expires On	3/14/2011

Fingerprints

SHA1 Fingerprint	59:4C:6C:4F:57:63:77:1E:A2:AE:33:17:BF:EC:44:AB:85:09:0E:EB
MD5 Fingerprint	57:68:B5:E3:37:F6:24:B8:89:43:73:C9:99:9E:81:81



This certificate has been verified for the following uses:

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

Issued To

Common Name (CN)	Team1
Organization (O)	DOEACC
Organizational Unit (OU)	DOEACC Centre
Serial Number	00:89:0B:BE:82

Issued By

Common Name (CN)	Hari K
Organization (O)	DOEACC
Organizational Unit (OU)	DOEACC Centre

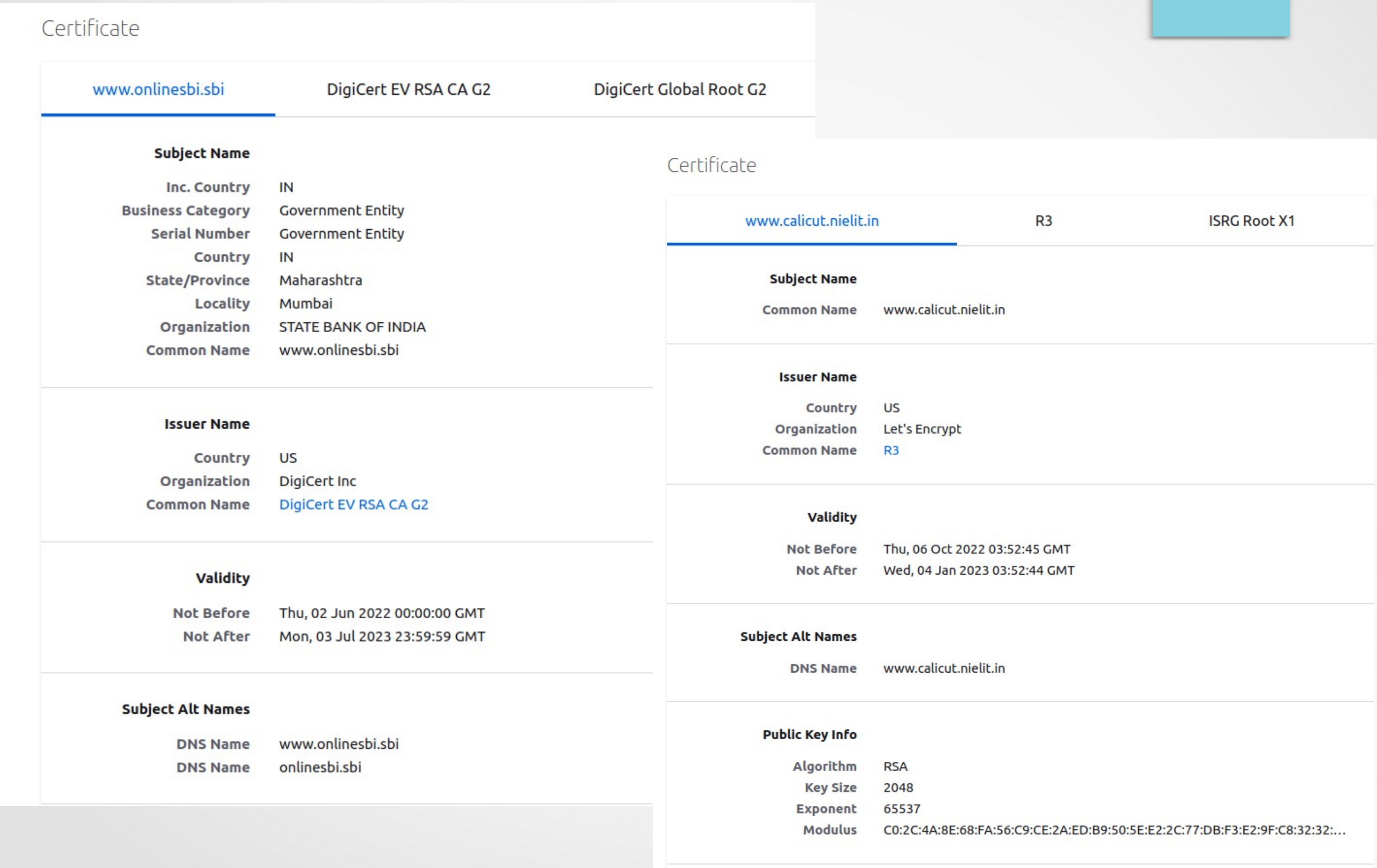
Validity

Issued On	3/14/2008
Expires On	3/14/2011

Fingerprints

SHA1 Fingerprint	93:41:F2:E3:6E:06:3D:84:43:6F:F8:4D:2F:2D:3A:57:B1:33:B4:E5
MD5 Fingerprint	2B:2D:47:86:5E:9E:B6:3E:FE:8D:C4:F8:BC:50:AC:89

SSL Certificate - example



Certificate

www.onlinesbi.sbi | DigiCert EV RSA CA G2 | DigiCert Global Root G2

Subject Name

Inc. Country	IN
Business Category	Government Entity
Serial Number	Government Entity
Country	IN
State/Province	Maharashtra
Locality	Mumbai
Organization	STATE BANK OF INDIA
Common Name	www.onlinesbi.sbi

Issuer Name

Country	US
Organization	DigiCert Inc
Common Name	DigiCert EV RSA CA G2

Validity

Not Before	Thu, 02 Jun 2022 00:00:00 GMT
Not After	Mon, 03 Jul 2023 23:59:59 GMT

Subject Alt Names

DNS Name	www.onlinesbi.sbi
DNS Name	onlinesbi.sbi

Certificate

www.calicut.nielit.in | R3 | ISRG Root X1

Subject Name

Common Name	www.calicut.nielit.in

Issuer Name

Country	US
Organization	Let's Encrypt
Common Name	R3

Validity

Not Before	Thu, 06 Oct 2022 03:52:45 GMT
Not After	Wed, 04 Jan 2023 03:52:44 GMT

Subject Alt Names

DNS Name	www.calicut.nielit.in

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	C0:2C:4A:8E:68:FA:56:C9:CE:2A:ED:B9:50:5E:E2:2C:77:DB:F3:E2:9F:C8:32:32:...

Certificate Extensions

- Certificate extensions allow for further information to be inserted within the certificate, which can be used to provide more functionality in a PKI implementation.
- *Standard certificate extensions* are implemented for every PKI implementation.
- *Private certificate extensions* are defined for specific organizations (or domains within one organization), and they allow companies to further define different, specific uses for digital certificates to best fit their business needs.

Some key examples of certificate extension

- **DigitalSignature** The key is to be used to verify a digital signature.
- **KeyEncipherment** The key is to be used to encrypt other keys used for secure key distribution.
- **DataEncipherment** The key is to be used to encrypt data and cannot be used to encrypt other keys.
- **CRLSign** The key is used to verify a CA signature on a revocation list.
- **KeyCertSign** The key is used to verify CA signatures on certificates.
- **NonRepudiation** The key is used when a nonrepudiation service is being provided.

Critical and Non-Critical Extensions

- Certificate extensions are considered either *critical* or *non-critical*, which is indicated by a specific flag within the certificate itself.
- When this flag is set to critical, it means that the extension *must* be understood and processed by the receiver.

Certificate Lifecycles

- Keys and certificates should have lifetimes set, which will force the user to register for a new certificate after a certain amount of time.

Registration and Generation

- A key pair (public and private keys) can be generated locally by an application and stored in a local key store on the user’s workstation.
- The key pair may also be created by a central key-generation server, which will require secure transmission of the keys to the user.

Key Strength-RSA

- If you choose a key size of 128 bits, the estimated time necessary to break this cryptosystem is less than five minutes, if the hacker could dedicate at least 105 computers just to this task.
- If you choose a key size of 1,024 bits, the time estimated to break it would increase to three million years if the hacker has at least 114 computers dedicated to this task, with 170GB of memory, and that much time to kill.

Renewal

- The certificate itself has its own lifetime, which can be different than the key pair’s lifetime.
- The certificate’s lifetime is specified by the validity dates inserted into the digital certificate.

Revocation

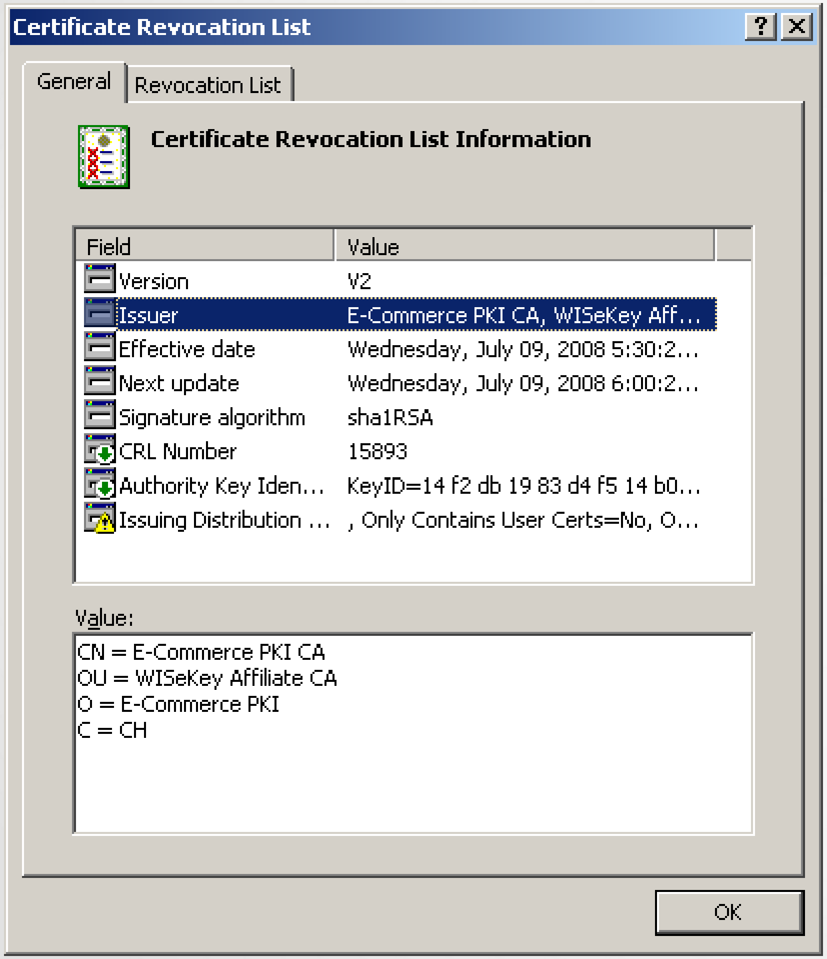
- **Certificates are revoked when the certificate's validity needs to be ended before its actual expiration date is met.**

- **There are several reasons why a certificate may need to be revoked:**
  - a user may have lost a laptop or a smart card that stored a private key
  - an improper software implementation may have been uncovered that directly affected the security of a private key,
  - a user may have fallen victim to a social engineering attack and inadvertently given up a private key
  - data held within the certificate may no longer apply to the specified individual, or
  - perhaps an employee left a company and should not be identified as a member of an in-house PKI any longer.

Certificate revocation list

- If a Certificate gets compromised, the CA can provide a type of protection by maintaining a *certificate revocation list (CRL)*, which is a list of serial numbers of certificates that have been revoked.
- The CRL also contains a statement indicating why the individual certificates were revoked and a date when the revocation took place.
- The list usually contains all certificates that have been revoked within the lifetime of the CA.

CRL Example

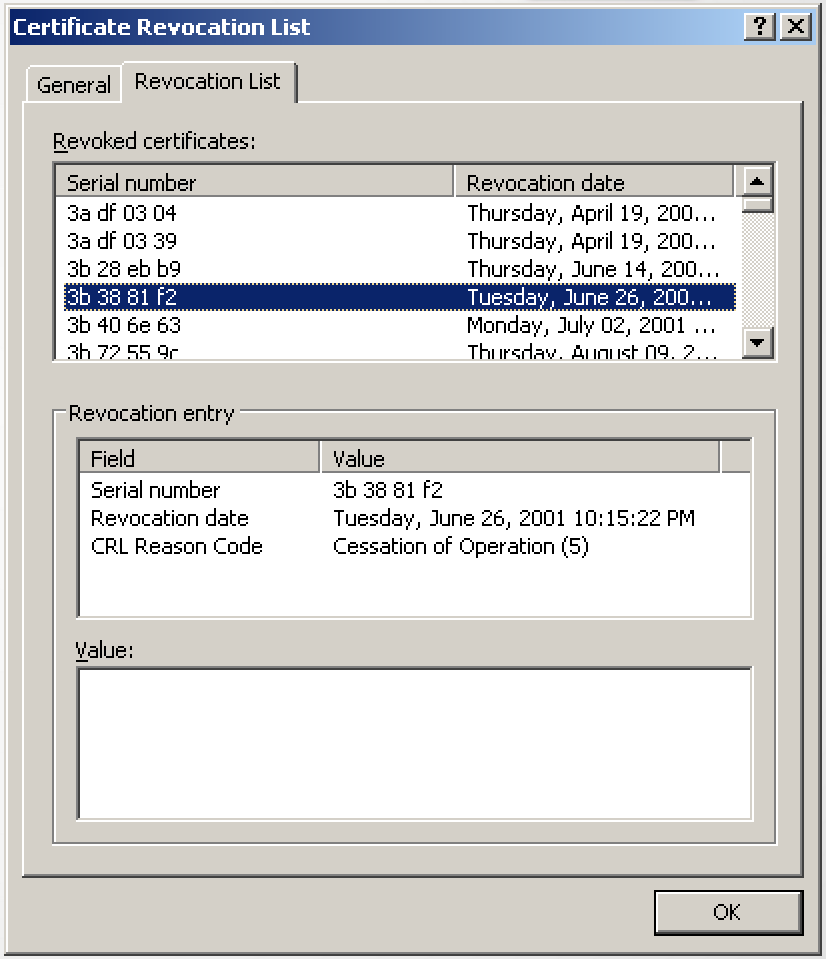


Certificate Revocation List Information

Field	Value
Version	V2
Issuer	E-Commerce PKI CA, WISeKey Aff…
Effective date	Wednesday, July 09, 2008 5:30:2…
Next update	Wednesday, July 09, 2008 6:00:2…
Signature algorithm	sha1RSA
CRL Number	15893
Authority Key Iden…	KeyID=14 f2 db 19 83 d4 f5 14 b0…
Issuing Distribution …	, Only Contains User Certs=No, O…

Value:

CN = E-Commerce PKI CA
OU = WISeKey Affiliate CA
O = E-Commerce PKI
C = CH



Revoked certificates:

Serial number	Revocation date
3a df 03 04	Thursday, April 19, 200…
3a df 03 39	Thursday, April 19, 200…
3b 28 eb b9	Thursday, June 14, 200…
3b 38 81 f2	Tuesday, June 26, 200…
3b 40 6e 63	Monday, July 02, 2001 …
3b 72 55 9c	Thursday, August 09, 2…

Revocation entry

Field	Value
Serial number	3b 38 81 f2
Revocation date	Tuesday, June 26, 2001 10:15:22 PM
CRL Reason Code	Cessation of Operation (5)

Value:

CRL Distribution

- The CRL can be pulled (downloaded) by individual users when needed,
- or the CRL can be pushed down (sent) to all users within the PKI on a timed interval.
- Online services (*Online Certificate Status Protocol (OCSP)*)

Suspension

- The certificate temporarily puts on hold.

Key Destruction

- Key pairs and certificates have set lifetimes, meaning that they will expire at some specified time.
- It is important that the certificates and keys are properly destroyed when that time comes, wherever the keys are stored.
- The goal is to make sure that no one can gain access to a key after its lifetime has ended and use this key for malicious purposes.

key history maintenance

- In modern PKIs, encryption key pairs usually must be retained long after they expire so that users can decrypt information that was encrypted with the old keys.
  - For example, if Bob encrypts a document using his current key and the keys are updated three months later, Bob's software must maintain a copy of the old key so he can still decrypt the document. In the PKI world, this issue is referred to as ***key history maintenance***

Characteristics and requirements of proper private key use

- The key size should provide the necessary level of protection for the environment.
- The lifetime of the key should correspond with how often it is used and the sensitivity of the data it is protecting.
- The key should be changed and not used past its allowed lifetime.
- Where appropriate, the key should be properly destroyed at the end of its lifetime.
- The key should never be exposed in clear text.

Characteristics and requirements of proper private key use ..

- No copies of the private key should be made if it is being used for digital signatures.
- The key should not be shared.
- The key should be stored securely.
- Authentication should be required before it can be used.
- The key should be transported securely.
- Software implementations that store and use the key should be evaluated to ensure they provide the necessary level of protection.

Other terminologies

Key Recovery

Key Escrow

Public Certificate Authorities

In-House Certificate Authorities

Questions