Network Security
Unit-IV

Digital Certificate & Public Key Infrastructure (PKI)

Digital Certificate

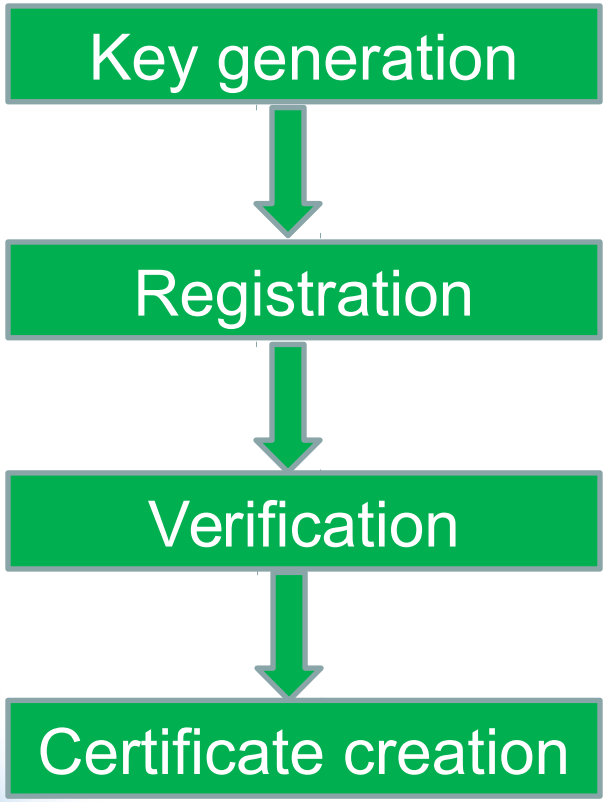
- To solve the man-in-the-middle attack, Digital Certificates were introduced.
- Digital certificate is similar to a passport, which give information of the issuer's name, serial number, public key, validity period.
- Digital Certificate is issued by a trusted agency called as CA (Certification Authority).
- Another third party called as RA(Registration Authority) acts as a intermediate entity between CA and end user.
- Satisfies the principle of Authentication, non-repudiation.

Fields of Version1	Description
Version	Version of X.509 protocol. Version can be 1,2 or 3
Certificate Serial No.	Contains unique integer which is generated by CA
Signature Algorithm Identifier	Identifies the algorithm used by CA to sign the certificate.
Issuer Name	Identifies the Distinguished Name that created & signed the certificate
Validity (not before/not after)	Contains two date-time value. This value generally specify the date & time up to seconds or milliseconds.
Subject name	Distinguished Name of the end user (user or organization)
Subject Public key info.	This field can never be blank. Contains public key & algorithm related.

Fields of Version 2	Description
Issuer Unique Identifier	Helps identify a CA uniquely if two or more CAs have used the same *IssuerName* over time.
Subject Unique Identifier	Helps identify a subject uniquely if two or more subjects have used the same *SubjectName* over time.

Fields of Version 3	Description
Authority Key Identifier	A CA may have multiple private-public key pairs. This field defines which key pairs is used to sign this certificate.
Subject Key Identifier	A subject have multiple private-public pairs. This field defines which key pairs is used to sign this certificate.
Key Usage	Defines the scope of operations of the public key of this particular certificate. For eg: key is used for encryption, Diffie Hellman Key exchange, digital signature, combination of these or all operations.
Extended key Usage	In addition to above operations, it also specifies which protocol this certificate can interoperate with. For eg: TLS, client or server authentication.
Private Key Usage period	Defines different usage period limits for the private & public keys
Certificate Policies	Defines the policies information that the CA associates with given certificate
Policy Mapping	Used when the subject of a given certificate is also a CA
Subject Alternative Name	Optionally defines one or more alternative names for subject.
Issuer Alternative Name	Optionally defines one or more alternative names for issuer.
Subject Directory Attributes	Can be used to provide additional information about the subject such as subject phone/fax numbers, email ids etc.
Basic Constraints	Indentifies whether the subject in this certificate may act as a CA.
Name Constraints	Specifies the name space.
Policy Constraints	Used only for CA certificates.

Certificate Creation Steps



•Either user creates a pair and sends public key & other information to RA

- RA creates a pair on user's behalf
- This field is required only if user generates the key pair.
- If RA generates the pair then this field is included in above step.

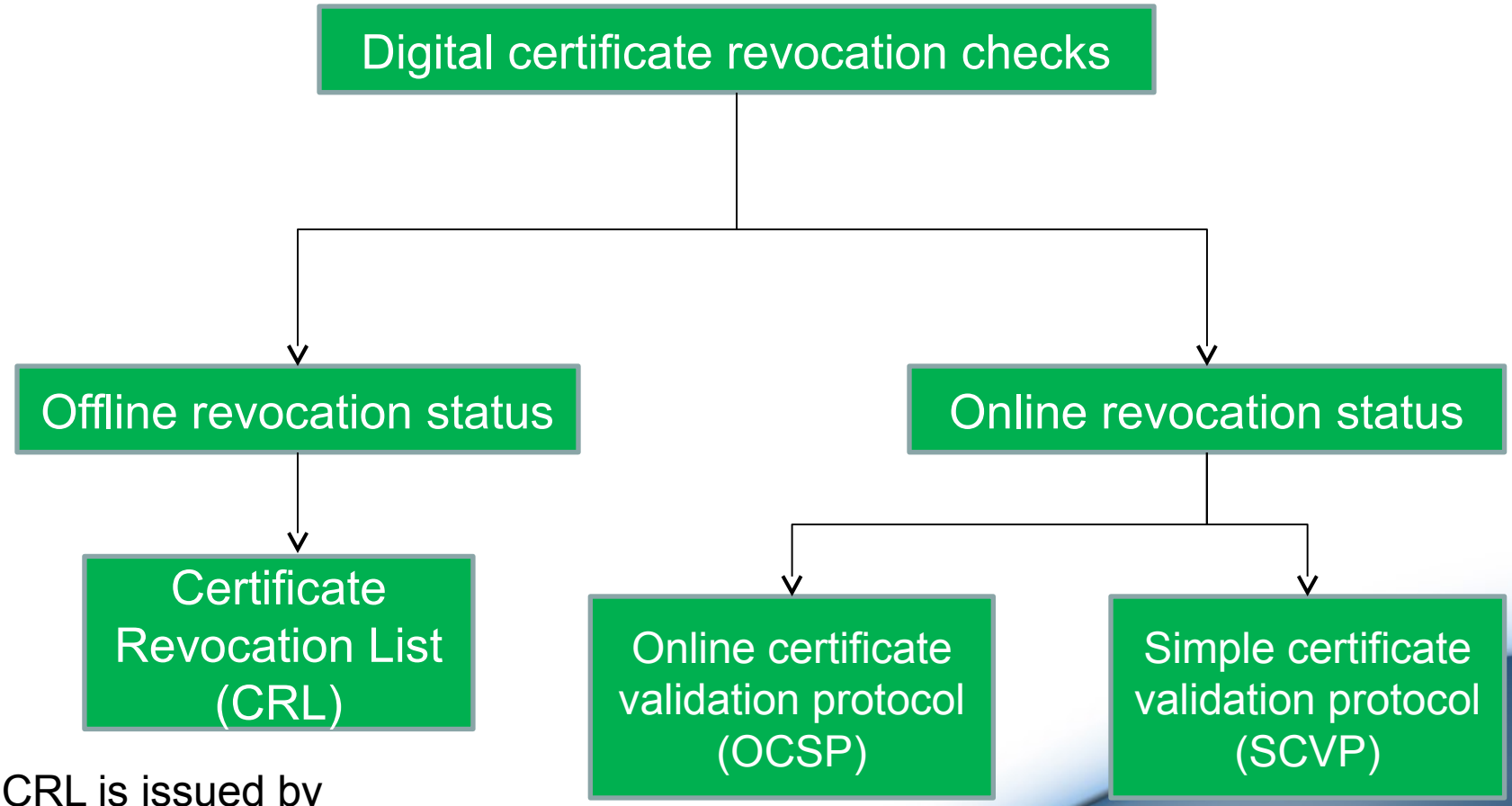
•The certificate request format has been standardized called as CSR

•CSR is one of the PKCS#10

- Firstly the RA verifies the credentials & evidences of the end user.
- The second check is to ensure that the end user posses as private key. This check is called as Proof of Possession (POP).
- After satisfying above steps, the RA sends details to CA.
- The CA does its own verification & creates a digital certificate.
- A copy of the digital certificate is maintained by CA in Certificate Directory.
- The directory clients can access the directory using LDAP (Lightweight Directory Access Protocol) depending on their privileges.

Certificate Revocation

- Reasons for revocation:
- If the private key corresponding to the public key is stolen.
- The CA realizes that it had made mistake while issuing the certificate.
- The certificate holder leaves a job and the certificate was issued specifically while the person was employed in that job.
- If Alice wants to send message to Bob:-
- Then Alice arises some questions as:
- Does this certificate really belong to Bob?
- Is this certificate valid, or is it revoked?



•A CRL is issued by CA on regular basis.
•A CRL contains info about valid certificate but are revoked .

•Client sends a OCSP request to the server.
•The server check the details in X.500 directory.
•Accordingly sends the response.

•Similar to OCSP.
•Apart from the revocation detail, we get other details also.

Private Key Management

- To protect the private key by means:-
- Password protection
- PCMCIA cards (Personal Computer Memory Card International Association)
- Tokens
- Biometrics
- Smart Cards
- Apart from these, the private key used for digital signing must be destroyed. In contrast, the private key used for encryption/decryption must be archived.
- In case of certificate expiration, the user need to update its key.
- The CA should maintain history of certificates & keys to prevent any legal problems.

The PKIX (Public Key Infrastructure X.509) model

- PKIX Services:
- Registration
- Initialization
- Certification
- Key-pair recovery
- Key generation
- Key update
- Cross certification
- Revocation

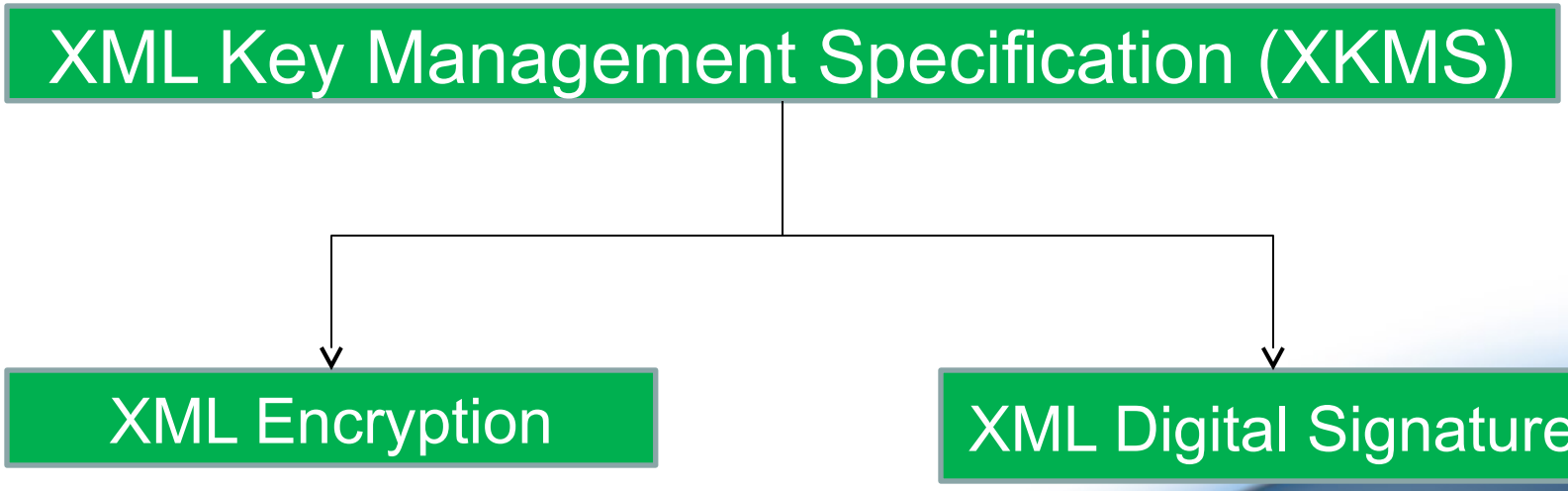
PXIX Architectural model

- **X.509 v3 Certificate & v2 Certificate Revocation List profiles**: (lists the use of various options while describing extensions of a digital certificate).
- **Operational Protocol**: (defines the underlying protocols that provide the transport mechanism).
- **Management Protocol**: (enables exchange of information between the various PKI entities. Specifies the structure & details of PKI messages).
- **Policy outlines**: (defines policies for the creation of Certificate Policies & Certificate Practice Statements.)
- **Timestamp & Data Certification Services**: (both are the trusted third parties that provide services to guarantee the existence of certificate & DCS verifies the correctness of data that it receives).

PKCS (Public Key Cryptography Standards)

Standard	Description
PKCS#1	RSA Encryption Standard. Defines rules for calculating digital certificate.
PKCS#2	RSA Encryption Standard for Message Digest.
PKCS#3	Diffie-Hellman Key Agreement Standard.
PKCS#4	NA. merged with PKCS#1
PKCS#5	Password Based Encryption(PBE). Defines KEK method to encrypt symmetric key.
PKCS#6	Extended Certificate Syntax Standard. Defines syntax for extending the basic attribute of an X.509 digital certificate.
PKCS#7	Cryptographic Message Syntax Standard.
PKCS#8	Private Key Information Standard.
PKCS#9	Selected Attribute Types. Defines selected attribute for use in PKCS#6 extended certificates.
PKCS#10	Certificate Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard. Specifies interfaces for single user
PKCS#12	Personal Information Exchange Syntax Standard.
PKCS#13	Elliptic Curve Cryptography Standard
PKCS#14	Pseudo –Random Number Generation Standard.
PKCS#15	Cryptographic Token Information Syntax standard

XML, PKI and Security



Using XML encryption, we can encrypt an entire document or its element or its sub-element.

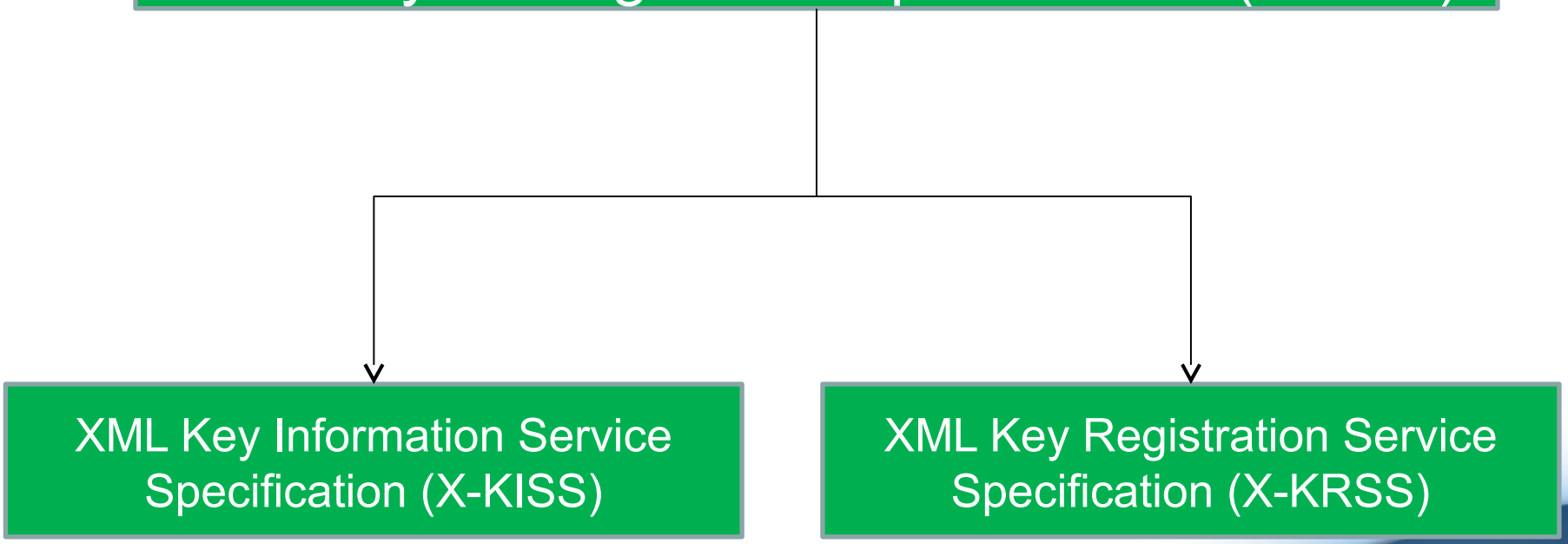
XML Digital Signature also can authorize selected part of XML document.

1.) **<Signature>……</Signature>** : identifies the start and end of the XML digital signature.

2.) **<SignedInfo>….. </SignedInfo>** : specifies the algorithm used. Firstly, for calculating MD and then for preparing the XML digital signature.

3.) **<SignatureValue>…… </SignatureValue>** : contains the actual XML digital signature

XML Key Management Specification (XKMS)



Specifies a protocol for **trust service which resolves public-key information** contained in documents that conform to the XML signature standard.

Specifies a protocol for a **Web Service that accepts the registration of public key information**. This protocol can also be used to later retrieve the private key.

Hashing & Hash Functions

- Hashing is a method to store data in an array.
- The basic idea is :-
- to use a fixed length message,
- use a function h,
- It will return the position and same is stored in the array.
- Array stores the key and the index of array is called hash value.
- A collision happens when the hash function generates same index value, then the new value is shifted to empty slot of array.

Birthday attacks

- Birthday attacks are often used to find collisions of hash functions.
- These methods take advantage of function which when supplied with a random input, return one of equally likely values.
- By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about $1.2\sqrt{365}$ evaluations.

Key Predistribution

- Key Predistribution is the method of distribution of keys onto nodes before deployment.

Blom's Scheme

- Pair wise key pre-distribution.
- Scheme was proposed by Swedish cryptographer Rolf Blom in early 1980s.
- Here a trusted party gives each participant a secret key and a public identifier, which enables any two participants to independently create a shared key for communicating.
- Blom's scheme uses public matrix G and private matrix D (Symmetric).
- TA chooses a random & secret symmetric matrix D_k where k is the finite field over GF(p), where p is a prime number.

Suppose k=3 and p=17 and

$$D=\begin{bmatrix}1 & 6 & 2\\ 6 & 3 & 8\\ 2 & 8 & 2\end{bmatrix} \bmod 17$$

Now Alice's identifier I_{Alice}:- $\begin{bmatrix}3\\10\\11\end{bmatrix}$

Bob's identifier I_{Bob}:- $\begin{bmatrix}1\\3\\15\end{bmatrix}$

TA then computes their private key as :-

$g_{Alice} = D\ I_{Alice}$

$$\begin{bmatrix}1 & 6 & 2\\ 6 & 3 & 8\\ 2 & 8 & 2\end{bmatrix}\begin{bmatrix}3\\10\\11\end{bmatrix}=\begin{bmatrix}85\\136\\108\end{bmatrix} \bmod 17=\begin{bmatrix}0\\0\\6\end{bmatrix}$$

$g_{Bob} = D\ I_{bob}$

$$\begin{bmatrix}1 & 6 & 2\\ 6 & 3 & 8\\ 2 & 8 & 2\end{bmatrix}\begin{bmatrix}1\\3\\15\end{bmatrix}=\begin{bmatrix}49\\135\\56\end{bmatrix} \bmod 17=\begin{bmatrix}15\\16\\5\end{bmatrix}$$

Then both will generate the shared key as follows:-

$$K_{Alice/Bob} = \begin{bmatrix} 0 \\ 0 \\ 6 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 15 \end{bmatrix} \bmod 17 = 5$$

$$K_{Alice/Bob} = \begin{bmatrix} 15 \\ 16 \\ 5 \end{bmatrix} \begin{bmatrix} 3 \\ 10 \\ 11 \end{bmatrix} \bmod 17 = 5$$

Station to Station Protocol

- The Station-to-Station protocol is a cryptographic key agreement scheme based on the classic Diffie-Hellman exchange that provides mutual key and entity (party) authentication.
- STS was originally presented in 1987 in the context of ISDN security, finalized in 1989 & presented by Whitefield Diffie, Paul C. vanOorschot and Michael J.Wiener in 1992.
- In addition, the STS protocol uses no timestamps and provides prefect forward secrecy.
- It also requires two-way explicit key confirmation, making it an Authenticated key agreement with Key Confirmation (AKC) protocol.

Thank You