Digital Certificates and Smart Cards

Digital certificates are files which are used to prove the authenticity of the user or computer to whom it is issued. It is very similar to an identification proof like passport, driving license or PAN, which gives assurance to the other party that the transaction of information from the certificate holder is authentic. A digital certificate might be issued for the following purposes:

1. Server Authentication
2. Client Authentication
3. Code Signing
4. Secure Email
5. Encrypting File System
6. File Recovery

Need of Digital Certificate

A digital certificate is required for electronic verification of an identity. It authenticates and assures the identity of a party. Digital certificates are extremely important while furnishing some confidential information like bank details, passwords, transaction details and personal details.

For example, a web browser checks digital certificate of the website to assure security, which it is attempting to connect.

How to get digital certificate

A digital certificate can be obtained using any of the three methods:

1. Issuing a digital certificate to self - A user can issue a certificate to him. But, of course this certificate will not be trusted by other users unless this certificate is installed in their system.

2. Purchasing a certificate from a trusted Certifying Authority - The requestor submits the details of the certificate needed and the information that would be incorporated in the certificate. The trusted CA would do the verification of the information and then create and issue the certificate.

3. Obtaining a certificate from an intermediate organization CA - An intermediate organization might be “certified” by a trusted CA to issue certificates. However, the client or browser might not recognize this intermediate CA as the trusted one. Therefore a chain of certificates is required to establish the trust. This chain of certificates would help the browser in identifying the trusted root CA.

Certificate Authority
A digital certificate can be issued from Certificate authority, which must contain CA's private key. Few of the recognized certificate authorities are Verisign, Entrust, and NIC etc.

**Components of Digital signature**

![Diagram of Digital Certificates]

Sample NETSCAPE digital signature look like is as below.

![NETSCAPE Digital Signature]

CA plays a very important role in PKI infrastructure. When an entity or organization requests a digital certificate from the CA, it is the responsibilities of CA to cross verify the applicant’s information. It is because once the certificate has been issued,
other people and applications will blindly start trusting it.

Commercial CAs charge fees for issuing the certificates.

**Classes of Digital Certificates**

Certificates are categorized based on the level of trust the certificate would provide.

If a certificate is needed for personal use, the class of certificate would need lesser verification than it would need for certificate issued to identify an organization.

The most commonly recognized classes are –

1. **Class 1** - meant for personal use. E.g. use with email.
2. **Class 2** - issued to organizations.
3. **Class 3** - issued to servers. Used for software signing.
4. **Class 4** - issued for e-business transactions

**Certificate store**

Certificates and the private keys are stored in the local computer in one of the logical stores.

1. Personal
2. Trusted Root Certification Authorities
3. Enterprise Trust
4. Intermediate Certification Authorities
5. Trusted People
6. Other People
7. Trusted Publishers
   All browsers have the ability to read the certificates from these stores and present whenever required.

In case of the user being a domain member, the certificates (public keys) are published in the LDAP directory. This is for establishing the PKI infrastructure.

**Smart Cards**

Smart cards are hardware device that have the capability to store the digital certificates for user.

The certificates meant for smart card logon are directly stored in the smart card. Windows server 2000 and later supports the Smart card authentication mechanism for logical resources like domain, internet etc.
Smart card based authentication provide two factor security by forcing the users to select a PIN for their cards. This prevents the risk of smart cards being misused.

**Usage of Digital Certificate in SSL handshake**

Secure Socket Layer protocol is used for all the transaction needing high security. It involves the use of Symmetric key and Asymmetric key encryption.

For establishing a SSL session, following steps are performed by the server and client application -

1. The client initiates the conversation by sending the cryptographic information such as the SSL version and some
2. The server replies with the session ID and its digital certificate
3. The client authenticates the server based on the SSL server's digital certificate
4. The client creates a pre-master secret for the session, encrypts it with the server's public key, and then sends this byte string to the server.
5. The SSL Server decrypts the pre-master key using its private key. After performing few cryptographic steps, the master key is calculated.
6. The master key generated will be used for deriving the session secret key at both the client and server end. This way, there is no need of sending across the secret key (which would have been very insecure).
7. After the establishment of SSL session, the server and client exchange messages by symmetrically encrypting with the shared secret key.