Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Enormous Certificate: Digital Signature Certificate

Mr. Vinod Saroha, Annu Malik, Madhu Pahal
Computer Science and Engineering
(Network Security)
India

Abstract— This paper presents a survey on Digital Signature Certificate. This discussion is centered on overview of digital signature certificate authority, creation of digital certificate, revocation of DSC and its authentication procedures . A Digital Signature Certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender can not revoke or deny. A Digital Signature Certificate is not only a digital equivalent of a hand written signature it adds extra data electronically to any message or a document where it is used to make it more authentic and more secured. Digital Signature ensures that no tampering of data is done once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which renewal is required.

Keywords— digital signature certificate, certificate, certificate authority(CA), message, authentication

I. INTRODUCTION

A digital certificate establishes your credentials when doing business or other transactions on the Web. In simple words Digital Certificate is the attachment to an electronic message used for security purposes. The common use of a digital certificates is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. Digital Certificate provides a means of proving your identity in electronic transactions; just like a driver's license or a passport does. You can present a Digital Certificate electronically to prove your identity or your right to access information or services online.

A Digital Certificate is issued by a Certification Authority (CA) and signed with the CA's private key. It typically contains:

A. Owner's public key
B. Owner's name
C. Expiration date of the public
D. Name of the issuer (the CA that issued the Digital Certificate)
E. Serial number of the Digital Certificate
F. Digital signature of the issuer

The most widely accepted format for digital certificates is defined by the CCITT X.509 international standard. And the most widely used standard for digital certificates is X.509.

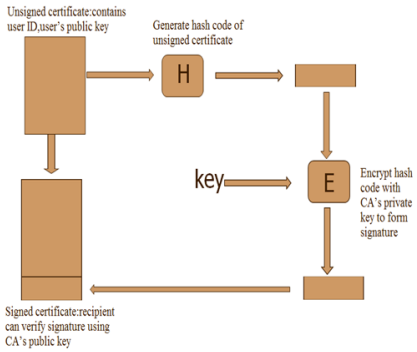
Digital Certificates are the framework for identification information, and bind identities with public keys. An electronic signature duly issued by the certifying authority that shows the authority of the person who is signing the e-form.Each Certificate contains the public key of the user and is signed with the private key of the certification authority.X.509 certificate format is used in S/MIME, IP Security, SSL/TLS and SET.

X.509 was initially issued in 1988.

Security of document requires:

1)Authenticity
2)Confidentiality
3)Integrity
4)Non-repudiation

Creation of digital certificate of any user:



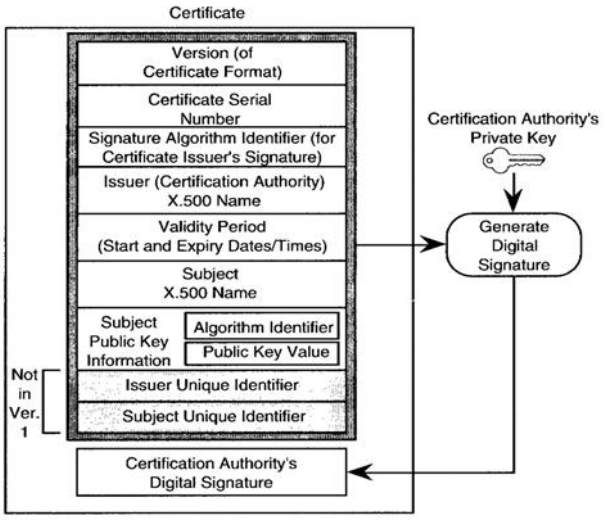
Public Key Certificate Use

II. Certificate Authority

A certificate authority issues digital certificates. It is also responsible for the generation, distribution and management of public keys. In order to obtain a digital certificate a user will establish a trust relationship with a CA. The CA will then authenticate the user according to guidelines in the CA's Certificate Practices Statements (CPS). The user is then issued a digital certificate. Even though individuals may not directly trust each other, they can establish an indirect relationship through a CA. Most CAs are composed of a number of components but the two most important components of a CA are the Registration Authorities (RA) and the Certificate Repository. The RA performs most of the administrative tasks of a CA. It registers users for a Digital Certificate, and it verifies all the information that goes into a digital certificate. The RA may even perform diligence test on a user to keep the information up to date. The Certificate Repository is a public database that keeps a record of current certificates and revocation lists need to be keeping updated or if a user's private key has been compromised the certificate repository ensures that only legitimate digital certificates and key pairs are being used.

III. X.509 Digital Certificate

The heart of the X.509 scheme is the public key certificate associated with each user. These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user. The directory server itself is not responsible for the creation of public keys or for the certification function, it merely provides an easily accessible location for users to obtain certificates.



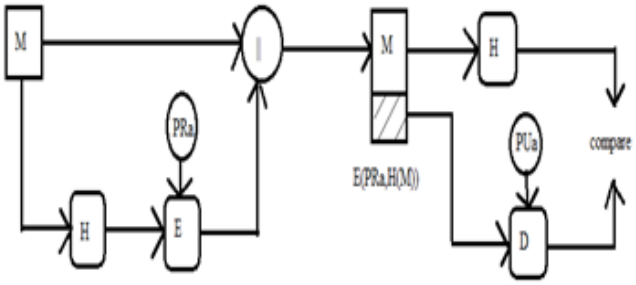
General format of X.509 certificate

X.509 certificate includes the following elements:

1. *Version*: - Differentiate among successive versions of certificate format, the default is version 1. If the issuer unique identifier and the subject unique identifier is present, the value must be version 2. If one or more extensions are present, the version must be version 3.
2. *Serial number:* - An integer value, unique within the issuing CA, that is unambiguously associated with each certificate.
3. *Signature algorithm identifier*: - The algorithm used to sign the certificate together with the associated parameters.
4. *Issuer name*: - X.500 name of the CA that created and signed this certificate.
5. *Period of validity:* - Consist of 2 dates: the first and last on which the certificate is valid.
6. *Subject name*: - The name of the user to whom this certificate refers. That is, this certificate certifies the public key of the user who holds the corresponding private key.
7. *Subject's public key information*: - The public key of the user plus the identifier of the algorithm for which this key is to be used, together with any associated parameters.
8. *Issuer unique identifier:* - An optional bit string used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
9. *Subject unique identifier:* - An optional bit string used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
10. *Extensions*: - A set of one or more extension fields.
11. *Signature*: - Covers all the other field of the certificate; it contains the hash code of the other fields, encrypted with the CA's private key. This field includes the signature algorithm identifier.

The unique identifier fields were added in version 2 to handle the possible reuse of subject and issuer names over time.
Notation to define a certificate

CA<<A>> = CA {V, SN, AI, CA, T_A, A, A_P}
Where
Y<<X>> = the certificate of user X issued by certification authority Y.
Y{I} – the signing of I by Y. It consists of I with an encrypted hash code appended.
The CA signs the certificate with its private key.if the corresponding public is known to a user, then that user can verify that a certificate is signed by the CA is valid.

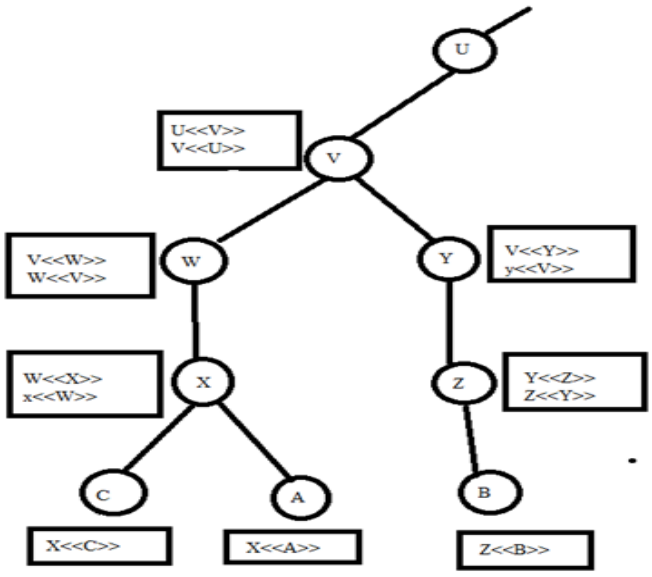


Obtaining a user certificate:
User certificate generated by a CA have the following certificates:
1. Any user with access to the public key of the CA can verify the user pubic key that was certified.
2. No party other than the CA can modify the certificate without this being detected.

Because certificates are unforgetable, they can be placed in a directory with the need for the directory to make special to protect them.

IV. X.509 Hierarchy

The connected circles indicate the hierarchical relationship among the CAs; the associated boxes indicate certificates maintained in the directory for each certificate entry.
The directory entry of each certificate authority includes two types of certificates:
1. *Forward certificates:* Certificates of X generated by other CAs
2. *Reverse Certificates*: Certificates generated by X that are the certificates of other CAs.
In this example, user A can acquire the following certificates from the directory to establish a certification path to B.
X<<W>>W<<V>>V<<U>>V<<Y>>Y<<Z>>Z<<B>>



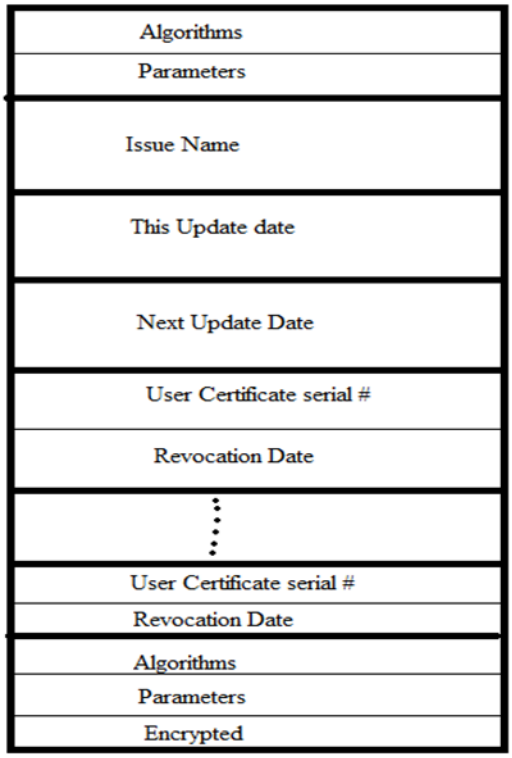
X.509 Hierarchy

When A has obtained these certificates, it can unwrap the certification both in sequence to uncover a trusted copy of B's public key. Using this public key, a can send encrypted message to B. If A wishes to receive encrypted message back from B, or sign messages sent to B then B will require A's public key, which can be obtained from the following certification path.
Z<<Y>>Y<<V>>V<<W>>W<<X>>X<<A>>
B can obtain this set of certificates from the directory or A can provide them as part of its initial message to B.

V. Revocation Of Certificate

Each certificate includes a period of validity, much like a credit card. Typically, a new certificate is issued just before the expiration of the old one. In addition, it may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons:

1. The user's private key is assumed to be compromised.
2. The user is no longer certified by this CA.
3. The CA's certificate is assumed to be compromised.



Certificate Revocation List

Each CA must maintain a list consisting of all revoked but not expired certificates issued by that CA, including both those issued to users and to other CAs. This list should also be posted on the directory. Each certificate revocation list (CRL) posted to the directory is signed by the issuer and includes the issuer's name the date list was created, the date the next CRL is scheduled to be issued and an entry for each revoked certificate.

Each entry consists of the serial number of a certificate and revocation date for that certificate. Because the serial nos. are unique within a CA, the serial no. is sufficient to identify the certificate. When a user receives a certificate in a message, the user must determine whether the certificate has been revoked. The user could check the directory each time a certificate is received. To avoid delays associated with directory searches, it is likely that the user would maintain a local cache of certificates and list of revokes certificates.

VI. Authentication Procedures

X.509 also includes three alternatives authentication procedures that are intended for use across a variety of applications. All these procedures make use of public-key signatures. It is assumed that the two parties know each other's public key, either by obtaining each other's public key, and either by obtaining each other's certificates from the directory or be Z the certificate is included in the initial message from each side.

Three procedures:

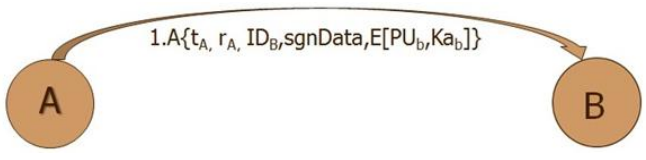
1. One-Way Authentication

It involves a single transfer of information from one user (A) to another (B) and establishes the following:

•The identity of A and that the message was generated by A

•That the message was intended for B.

•The integrity and originality (it has not been sent multiple times) of the message.

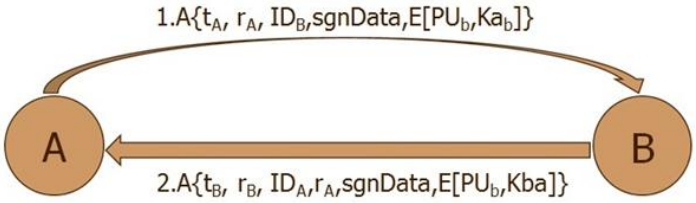


Note: Only the identity of the initiating entity is verified in this process, not the responding entity. At a minimum, the message includes a timestamp t_A a nonce r_A, and the identity of B and is and is signed with A's private key. The timestamp consist of an optional generation time and an expiration time. This prevents delayed delivery of messages. The nonce can be used to detect replay attacks. The value of nonce must be unique within the expiration time of the message. Thus , B can store the nonce until it expires and reject any new messages with the same nonce. sgnData, guaranteeing its authenticity and integrity. The message may also be use to convey the session key to B, encrypted with B's.

2. Two-Way Authentication:

It establishes the following elements;

1. The identity of A and that the message was generated by A.
2. That the message was intended for B.
3. The integrity and originality (it has not been sent multiple times)of the message.

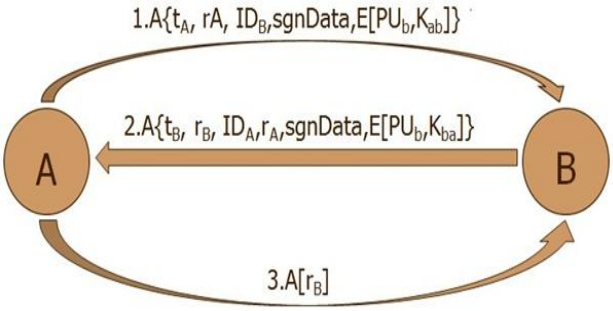


4. The identity of B and the reply message generated by B.
5. That the message was intended for A.
6. The integrity and the originality of the reply.

Two way authentication thus permits both parties in a communication to verify the identity of the other.

The reply message includes the nonce from A, to validate the reply. It also includes the timestamp nonce generated by B. The message may include signed additional information and a session key encrypted with A's public key.

3. Three way authentication



A final message from A to B is included which contains a signed copy of the nonce r_B.

VII. Conclusion

Digital Signature Certificate can be used to access secured zones of web sites where member login is required, surpassing the requirement of entering the user name and password. It insures by means of verification and validation that the user is whom he/she claims to be. This is done by combining the users credential to the digital certificate and in turn this method uses one point of authentication. Digital certificates ensure confidentiality and ensure that messages can only be read by authorized intended recipients. Digital certificates also verify date and time so that senders or recipients can not dispute if the message was actually sent or received.

References

- www.google.com
- Network Security by William Stallings
- http://digitalsignatureindia.com/
- http://deity.gov.in/content/digital-signature-certificates
- http://www.sans.org/reading_room/whitepapers/infosec/digital-signature-multiple-signature-cases-purposes_1154

