E-ISSN: 2321–9637

Volume 1, Issue 5, December 2013

International Journal of Research in Advent Technology

Available Online at: http://www.ijrat.org

COMPARISON BETWEEN AUTHENTICATION CERTIFICATES

Sarvesh Tanwar[1], Dr. Prema K.V[2]
Faculty of Engineering ,CSE Department
Mody Institute of Technology & Science Mody Institute of Technology & Science
Lakshmangarh-332311, Rajasthan , India
[1]s.tanwar1521@gmail.com, [2]drprema.mits@gmail.com

ABSTRACT
A public-key cryptography is best suited for fulfilling the requirements of the secure communication overinternet. Each user of a public-key cryptosystem holds a pair of related keys- public and private key. Anything encoded with one key can only be decoded by its counterpart. Each user keeps one key secret and publishes the other. Thus other people can employ the user's public key to send messages that only the user can read, or the user can "sign" a message with her private key to authenticate it – other people can apply the user's public key to verify that the message came from the user. Computer security has been victim of the "year of the..." syndrome. First it was firewalls, then intrusion detection systems(IDS), then VPNs, and now certification authorities (CAs) and public key infrastructure (PKI). The problems faced by users of the Internet fall into two main categories: privacy and authentication. Privacy involves transmitting messages that cannot be altered or read in route, while authentication allows each party to a communication to be sure of the identity of the other (i.e. messages can't be forged). In this paper we compare the different certificates which are used for authentication such as: - X.509, Digital Certificates and Tesla.

Keywords*: private key, X.509, Tesla, PKI, certification authorities, IDS***.**

1. INTRODUCTION

Computers play an increasingly larger role in everyday life. From the embedded microprocessors found in virtually every electronic appliance, to the escalating number of personal computers used for business, entertainment and education, Nicholas Negroponte's statement that "computing is not about computers … it is about living", it is becoming truer by the day. Now, with the recent explosive growth of the Internet, all these computers are becoming interconnected in a global communications neStwork. Many view the Internet as a universal communications medium that can replace telephone, television and radio. It is still too easy to intercept, monitor and forge messages on the Internet, and people are reluctant to use the network for financially or legally sensitive data.

Cryptography holds the promise of a solution to these problems. Cryptography is the science of secret writing. The security mechanisms as authentication, non- repudiation and integrity control of the documents in organizations are commonly handled with digital signatures. Authorization is another crucial mechanism in a hierarchical document workflow. The digital signatures have deficiency to provide authorization of the signer or his/her signature on the document.

Key management phases

The key states, or transitions, can be grouped under four key management phases. They are as follows:-

- Pre-operational phase—The keying material is not yet available for normal cryptographic operations.
- Operational phase—The keying material is available for normal cryptographic operations and is in use.
- Post-operational phase—The keying material is no longer in use, but access to the material is possible.
- Destroyed phase—The keys are no longer available and they must be destroyed.

1.2 Methods of cryptanalytic attacks

Cryptanalytic attacks are keys that have been compromised by decipherment to find out the keys. The goal of cryptanalysis is to decipher the private key or secret key. The amount of information provided to the analyst, as well as the type of information provided, determines the type of attacks possible. The following are six possible attack scenarios:-

1. ***Cipher text only attack***: This type of attack refers to the availability of the cipher text (encrypted text) to the cryptanalyst. With large cipher text data, it may be possible to decipher the cipher text by analyzing the pattern.
2. ***Known-plaintext attack:*** This type of attack happens when a cryptanalyst obtains a cipher text as well as the corresponding plaintext. In this scenario, even if the data is small, it is possible to understand the algorithm.
3. ***Chosen-plaintext attack:*** This type of attack refers to the availability of a corresponding cipher text to the block of plaintext chosen by the analyst.
4. ***Adaptive-chosen-plaintext attack:*** This type of cryptanalytic attack is known as an adaptive-chosen-plaintext attack if the cryptanalyst can choose the samples of the plaintext based on the results of previous encryptions in a dynamic passion.
5. ***Chosen-cipher text attack:*** This type of attack is used to obtain the plaintext by choosing a sample of cipher text by the cryptanalyst.
6. ***Adaptive-chosen-cipher text attack:*** This type of attack is similar to the chosen-cipher text attack, but the samples of cipher text are dynamically selected by the cryptanalyst and the selection can be based on the previous results as well.

1.2.1 Cryptographic standards

Cryptography standards are related to the following:-

- Encryption
- Hashing
- Key Management
- Digital signatures
- Public Key Infrastructure

1.3 TYPES OF SIGNATURES

a) Typing a name

When a person types their name onto a file in electronic format, such as a letter, email or other form of document, the text added is a form of electronic signature (e-signature).

b) PIN number

The Pin number on a credit card or bank card has the same purpose as a signature- that is to authenticate the user. Banks deals two things-money and risk. Banks suffer regularly from people who forge signatures on cheques and credit cards, and they perceive that the risk can be reduced if they require users to use a PIN number, instead of signing their name. This will not prevent the fraudulent use of stolen cards but the risk should be with the bank or the retailer not the customer.

c) Biodynamic versions

There are products available that enable a person to produce a digital biodynamic version of theirmanuscript signatureby writing using a special pen and pad. The signature is reproduced on the computer screen and a series of measurements record the speed, rhythm, pattern, habit, stroke sequence and dynamics that are unique to the individual. The subsequent file can then be attached to any document in electronic format to provide a signature.

d) Scanned signatures

A manuscript signature can be scanned from the paper carrier and be transformed into digital format. The signature can then be attached to a document. This version of a signature is used widely in commerce, especially, when marketing materials are sent through the postal system and addressed to hundreds of thousands of addresses.

e) The digital signature

Digital signatures are supported by public key certificates and Public Key Infrastructures (PKI). A public key certificate commonly means an electronic document that binds securely a public key with some identification. The most common public key certificate standard is the recommendation X.509, developed by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) [5]. A PKI provides the tools and operations that enable practical deployment of applications using public key certificates and, therefore, digital signatures. The Internet X.509 Public-Key Infrastructure (PKIX) Working Group within the Internet Engineering Task Force (IETF) is specifying a PKI for the Internet [6] using as base the ITU-T recommendation X.509. The whole set of PKIX documents is usually called the X.509/PKIX framework.

2. X.509 Certificate (Digital Certificate)

A digital certificate is basically a collection of identifying information bound together with a public key and signed by a trusted third party to prove its authenticity. A digital certificate can be one of a number of different formats.

Two different certificate formats are:-

- PGP certificates
- X.509 certificate

Digital Certificate provides a means of proving one's identity in electronic transactions, just like a driver's license or a passport. We can present a Digital Certificate electronically to prove our identity or 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:

- Owner's public key
- Owner's name
- Expiration date of the public
- Name of the issuer (the CA that issued the Digital Certificate)
- Serial number of the Digital Certificate
- Digital signature of the issuer

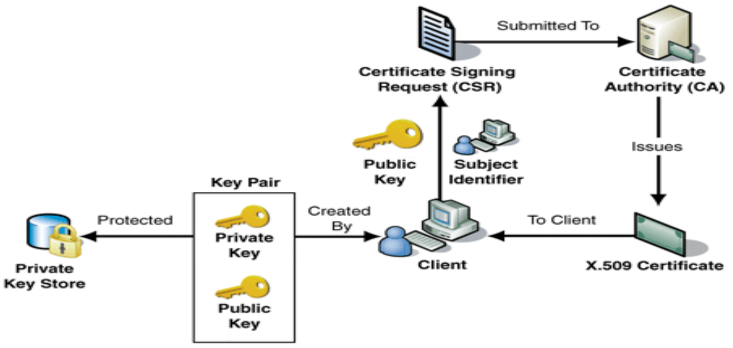


Figure 2.1: Requesting and obtaining a certificate from a CA

The X.509 standard defines what information can go into a certificate, and describes how to write it down (the data format). All X.509 certificates have the following data, in addition to the signature [6]:

Version

This identifies which version of the X.509 standard applies to this certificate, which affects what information can be specified in it.

Serial Number

The entity that created the certificate is responsible for assigning it a serial number to distinguish it from other certificates it issues. This information is used in numerous ways, for example when a certificate is revoked its serial number is placed in a Certificate Revocation List (CRL).

Signature Algorithm Identifier

This identifies the algorithm used by the CA to sign the certificate.

Issuer Name

The X.500 name of the entity that signed the certificate. This is normally a CA. Using this certificate implies trusting the entity that signed this certificate.

Validity Period

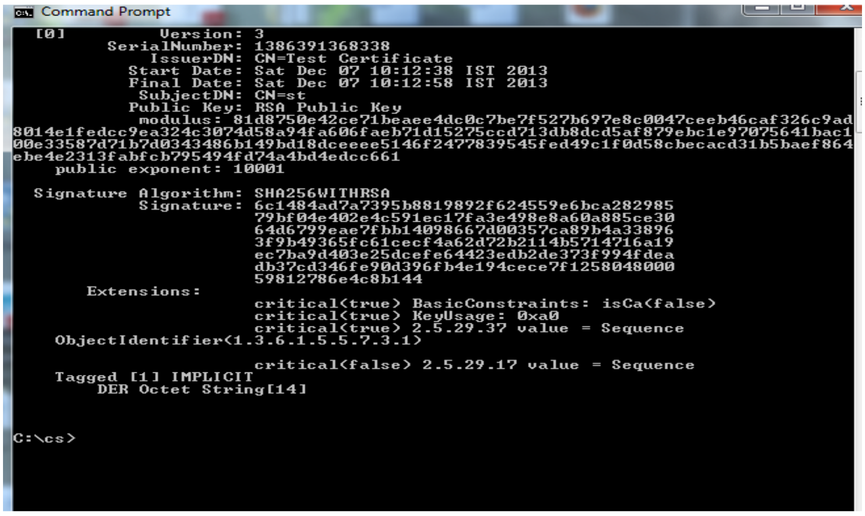
Each certificate is valid only for a limited amount of time. This period is described by a start date and time and an end date and time, and can be as short as a few seconds or almost as long as a century. The validity period chosen depends on anumber of factors, such as the strength of the private key used to sign the certificate or the amount one is willing to pay for a certificate. This is the expected period that entities can rely on the public value, if the associated private key has not been compromised.

Subject Name

The name of the entity whose public key the certificate identifies. This name uses the X.500 standard, so it is intended to be unique across the Internet. This is the Distinguished Name (DN) of the entity, for example,
CN=Test, OU= Security, O=MITS, C=IN
(These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)

Subject Public Key Information

This is the public key of the entity being named, together with an algorithm identifier which specifies which public key crypto system this key belongs to and any associated key parameters.
X.509 certificate is implemented using bouncy castle package.



```
  [0]         Version: 3
         SerialNumber: 1386391368338
             IssuerDN: CN=Test Certificate
           Start Date: Sat Dec 07 10:12:38 IST 2013
           Final Date: Sat Dec 07 10:12:58 IST 2013
            SubjectDN: CN=st
           Public Key: RSA Public Key
            modulus: 81d8750e42ce71beaee4dc0c7be7f527b697e8c0047ceeb46caf326c9ad
8014e1fedcc9ea324c3074d58a94fa606faeb71d15275ccd713db8dcd5af879ebc1e97075641bac1
00e33587d71b7d0343486b149bd18dceeee5146f2477839545fed49c1f0d58cbecacd31b5baef864
ebe4e2313fabfcb795494fd74a4bd4edcc661
    public exponent: 10001

  Signature Algorithm: SHA256WITHRSA
            Signature: 6c1484ad7a7395b8819892f624559e6bca282985
                       79bf04e402e4c591ec17fa3e498e8a60a885ce30
                       64d6799eae7fbb14098667d00357ca89b4a33896
                       3f9b49365fc61cecf4a62d72b2114b5714716a19
                       ec7ba9d403e25dcefe64423edb2de373f994fdea
                       db37cd346fe90d396fb4e194cece7f1258048000
                       59812786e4c8b144
       Extensions:
                       critical(true) BasicConstraints: isCa(false)
                       critical(true) KeyUsage: 0xa0
                       critical(true) 2.5.29.37 value = Sequence
    ObjectIdentifier(1.3.6.1.5.5.7.3.1)

                       critical(false) 2.5.29.17 value = Sequence
    Tagged [1] IMPLICIT
        DER Octet String[14]


C:\cs>
```

Figure 2.1: X.509 v3 Certificate Generation

2.1 Application of Certificates

Probably the most widely visible application of X.509 certificates today is in web browsers (such as Mozilla Firefox and Microsoft Internet Explorer) that support the TLS protocol. TLS (Transport Layer Security) is a security protocol that provides privacy and authentication for your network traffic. These browsers can only use this protocol with web servers that support TLS.
Other technologies that rely on X.509 certificates include:

- Various code-signing schemes, such as signed Java Archives, and Microsoft Authenticode.
- Various secure E-Mail standards, such as PEM and S/MIME.
- E-Commerce protocols, such as SET.
- Banking
- E-Voting
- Web Applications

3. Digital Signature

In cryptography, a digital certificate is an electronic document that uses a digital signature to bind together a public key with an identity - this information can be a person's name or the name of an organization, etc. The certificate is used to confirm that a public key belongs to a specific individual.

The digital signature is simply a one-way hash (message digest) of the original data that has been encrypted with the signer’s private key and send message alonwith message digest to the receiver. To validate the data, the recipient uses the signer’s public key to decrypt the digital signature and obtain the hash. The original data is then run through the same hashing algorithm that generated the original hash. Information about the hashing algorithm is actually included with the digital signature. This new hash is compared to the original hash to verify that the data has not been changed since it was signed. Digital signature solutions produce legally enforceable electronic records, closing the gap in going fully paperless by completely eliminating the need to print documents for signing. Digital signatures enable the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones.

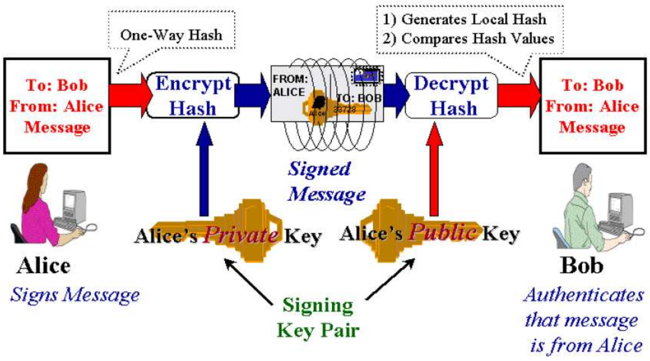
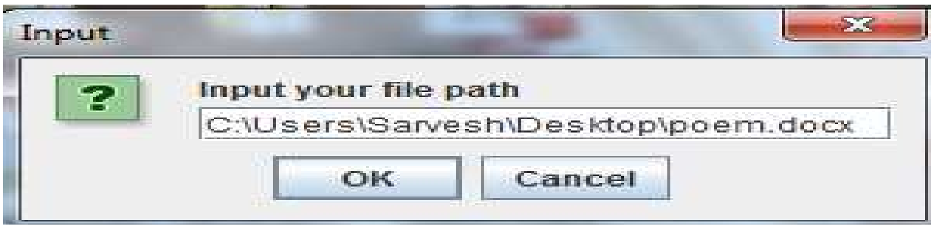


Figure 2.2 : Digital Signing (Authentication, Integrity, Non-repudiation) (From Morris, 2001, p. 9)

3.1 Hash Functions

Typically, to digitally sign a message or a file, rather than encrypt the message using a public key scheme, the message is hashed using a cryptographic hash function, and the hash is encrypted (Figure3.1 and 3.2). A cryptographic hash function maps an arbitrary-length message to a fixed number of bits. Hash functions have the following properties:

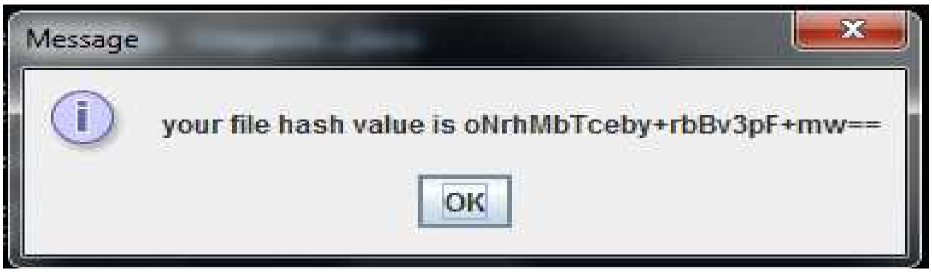
- They are collision-free: it is computationally infeasible to find two different messages that have the same hash.
- They are one-way: given a message hash, it is computationally infeasible to find any message with the same hash value.


Input

Input your file path

C:\Users\Sarvesh\Desktop\poem.docx

Figure 3.1: select the path of the file


Message

your file hash value is oNrhMbTceby+rbBv3pF+mw==

Figure 3.2: hash value of file

For computing hash value MD5 and SHA 256,512bits can be used.

3.2 CoSign Digital Signature

Whether it is adding digital signatures/digital seals with the click of a mouse or having the ability to sign any document and turn it into a PDF, CoSign provides users with a comprehensive and easy-to-use digital signing solution. CoSign's design ensures that anyone can verify the signature and content integrity of a signed document anywhere at any time with a simple click, and it allows multiple signatures to be placed on a document (one after another) while maintaining the documents integrity [4].

CoSign® digital signatures enable the replacement of slow, expensive, and non-productive paper-based approval, collaboration, and delivery processes with fast, low-cost, and efficient electronic operations.

CoSign works seamlessly with all common document formats such as Microsoft® Word, Excel®, Outlook®, InfoPath®, Adobe® PDF, AutoCAD®, Bentley® MicroStation, TIFF, and other document types. CoSign is standards-based (based on Public Key Infrastructure – PKI), avoiding vendor lock-in and allowing the document to be verified by anyone, anywhere, anytime without the need for proprietary verification software or third party support.

CoSign is offered in two versions – CoSign Desktop is meant for individual users, while CoSign Central is designed for a multiple-user organization. CoSign Central is based on easy-to-use software that communicates with a centralized and secure digital signature server. It is quick-to-deploy and ideal for mid to large sized organizations, offering seamless integration with content management and workflow systems. For smaller organizations (up to 10 signers), CoSign Desktop is offered as a standalone solution that does not require any hardware component.

3.2.1 CoSign Features (Desktop and Central) [4]

- **Digitally sign with a simple click of a mouse** - Equipped with an intuitive user interface, a simple right click is all that is required to sign and seal the document.
- **Digitally sign any document type** - CoSign works with all standard file formats: Microsoft® Word, Excel®, Outlook®, InfoPath®, Adobe® PDF, AutoCAD®, Bentley® MicroStation, TIFF, and other document types.
- **Turn any document into a digitally signed and sealed PDF** - CoSign's integrated virtual signing feature converts any electronic document into a signed PDF. CoSign can convert any document format into a signed PDF document.
- **Ensure external acceptance** - CoSign embeds the digital signature directly into the document itself, enabling it to serve as a form of self contained e-record. After signature capture, anyone can verify the signature and content integrity anywhere at any time - with a simple click.
- **Add your graphical signature and signing rationale** - The signer's graphical signature is placed on the document as well as the reason for signing (e.g., I approve, I agree, etc.).
- **Approve along with your colleagues** - CoSign allows multiple signatures to be placed on a document (one after another) while ensuring document integrity. This is useful in scenarios that require a series of approvers and an audit trail.
- **Approve only designated areas of the document** - Digital signatures can be applied to a specific area of the document. This is particularly effective for spreadsheets.

3.2.2 Enterprise-ready features (CoSign Central only)

- ***Workflow Integration*** -CoSign integrates perfectly with leading workflow and Content Management Systems such as Microsoft SharePoint®, enabling automated formal approval processes from within your organization's existing workflow systems.
- ***Simple Central Control***- CoSign leverages existing user management systems, such as Microsoft Active Directory®, for control over signer authorizations (new employees are added and employees leaving the organization are removed from the authorized signer list with a simple click). CoSign ensures quick deployment and minimal ongoing IT management requirements, translating into enhanced security and a very low total cost of ownership.
- ***Easy to integrate with existing infrastructure***- CoSign is designed as a plug-in for DM/ECM/BPM systems or whatever existing infrastructure is in place. CoSign comes with SAPI®, a robust API that enables intuitive web service interfacing.
- ***Scalability***- CoSign is scalable from a few signers to several million users and will work in your existing authentication environment.
- ***Quick deployment***- CoSign is typically deployed in a matter of hours.

- ***Minimal IT ongoing management*** - Once in place, CoSign typically requires less than 10 hours of annual IT management.
- ***Web-based forms***- CoSign enables compliant digital signatures in an external-facing portal.
- ***Batch signing***- With high throughput, CoSign can sign millions of documents, making it an ideal solution for bulk signing needs such as eInvoicing and eArchiving.

4 TESLA

The TESLA is a Broadcast Authentication Protocol [2]. A viable broadcast authentication protocol has the following requirements:

- ✓ Low computation overhead for generation and verification of authentication information.
- ✓ Low communication overhead.
- ✓ Limited buffering required for the sender and the receiver, hence timely authentication for each individual packet.
- ✓ Robustness to packet loss.
- ✓ Scales to a large number of receivers.

Data authentication is an important component for many applications, for example audio and video Internet broadcasts, or data distribution by satellite. This document specifies TESLA, a secure source authentication mechanism for multicast or broadcast data streams. The main idea of TESLA is that the sender attaches to each packet a MAC computed with a key k known only to itself. The receiver buffers the received packet without being able to authenticate it. A short while later the sender discloses k and the receiver is able to authenticate the packet. Consequently, a single MAC per packet suffices to provide broadcast authentication, provided that the receiver has synchronized its clock with the sender ahead of time [1].

TESLA certificates rely upon a trade-offs between computation and authentication delay in order to achieve a certificate infrastructure that reduces computational complexity associated with certificate verification when compared with traditional public key infrastructure certificates. Further, we introduce a modification to the TESLA protocol that provides partial authentication of multicast data, which allows for partial authentication in our TESLA certificate framework. As an application, we apply TESLA certificates to the problem of maintaining authentication during handoff in a generic mobile network.

Background and Assumptions

TESLA requires that the receivers are loosely time synchronized with the sender. TESLA also needs an efficient mechanism to authenticate keys at the receiver. TESLA [1][3] is a broadcast authentication technique that achieves asymmetric properties, in spite of using purely symmetric cryptographic functions (MAC functions). Due to the use of MACs, TESLA enables low powered nodes to perform source authentication. TESLA is based upon the principle of delayed key disclosure, which has found application in several works on authentication for network communication [6][7]. TESLA divides time into intervals of equal duration. Time slot n is assigned a corresponding key tKn. For each packet generated during time interval n, the sender appends a MAC that is created using the secret key tKn. Each receiver buffers the packets, without being able to authenticate them, until the sender discloses the key tKnby broadcasting the corresponding keyseedsn. Once snis disclosed, anyone with sncan calculate tKnand can pretend to be the sender by forging MACs. Therefore, the use of tKnfor creating MACs is limited to time interval n, and future time intervals use future keys. Further, snisn’t disclosed until d time slots later, where d is governed by an estimate of the maximum network delay for all recipients [2].

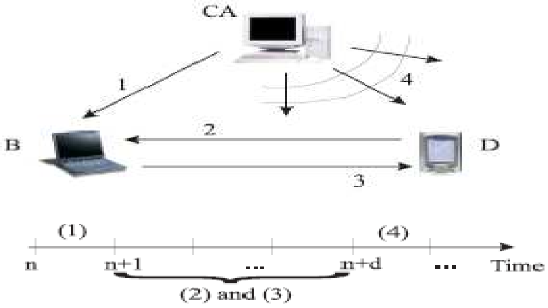


Figure 4.1:The steps involved in using TESLA certificates.

Conclusion

After studying all of the certificates we can say that digital certificates aremore important than the other mechanisms. Tesla can be used for MANET because they have limited energy as it is used for a time period. But digital signatures are suitable for E-commerce. As today everything is going to be online, it is difficult to recognize the sender and receiver but because of digital certificates it is possible to make transactions in a secure way.

REFERENCES

[1]A. Perrig, R. Canetti, B. Brisco, D. Song, and D. Tygar, "TESLA: Multicast source authentication transformintroduction," IETF working draft, draftietfmsecteslaintro01.txt.
[2]A. Perrig, R. Canetti, J.D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," in RSA Cryptobytes, 2002.
[3] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and secure source authentication for multicast," in Proceedings of Network and Distributed System Security Symposium, February 2001.
[4]http://www.arx.com/digital-signature/how-it-works
[5]"ITU-T Recommendation X.509: Information Technology—Open Systems Interconnection—The Directory: Authentication Framework," 2000.
[6]"RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Apr. 2002.