Mini-report about Certificate

Name:杜峯　　Student number:109550096

1. Definition and Creation
   a. Definition

      A certificate for digital signature is defined as a mathematic way to allow the receiver to verify the authenticity of data from the sender. As a valid digital signature, the receiver can apply an algorithm on this digital signature and check whether the result is corresponded to the data from the sender, which can make sure the data is not tampered and is precisely from the sender.

   b. Creation

      There are four steps to establish the certificate of digital signature.

      Step-1: Users generate public key with their own private key. And then the generated public key is sent to registration authority.

      Step-2: Registration authority receives the public key and registers the user.

      Step-3: A verification is performed by registration authority on the user's credentials, which also check if the public key is corresponded to the user's private key.

      Step-4: The verified certificate of digital signature and the details of this certificate are sent to certificate authority by the registration authority. These data will also be sent to the user and remains a copy at the registration authority.

2. Certificate of Digital Signature-USERTrust RSA Certification Authority
   a. Edition number: V3

      To record the version of this certificate.

   b. Serial number: 01fd6d30fca3ca51a81bbc640e35032d

      User's identity code, it's impassible to generate the same code from the same CA.

   c. Digital signature algorithm: sha384RSA

A kind of algorithm conducted on this certificate.

d. Digital signature hash algorithm: sha384

   To generate a hash value for the digital signature algorithm in this certificate.

e. Issuer: CN=USERTrust RSA Certification Authority, O=The UserTRUST Network, L=Jersey City, S=New Jersey, C=US

   This certificate is issued by which CA.

f. Certificate subject: USERTrust RSA Certification Authority, O=The UserTRUST Network, L=Jersey City, S=New Jersey, C=US

   This certificate belongs to whom. In other words, this field means the owner of this certificate.

g. Not valid before: 2010-02-01 00:00:00 UTC

   The moment of this certificate becomes valid.

h. Not valid after: 2038-01-18 23:59:59 UTC

   The moment of this certificate becomes not valid.

i. Public key: RSA (4096bits)

   e=65537, n=

   934531470562694352326420909292795235888177164888262850683721539678050956124169721994088574974187454706040713477339336636514965791214417037085702791321057057528041219541100351783037216389291652903951262111844115558886198326740546232998005068695460739667763010881129441005554808798344484280514250394265058817365502773946925002534170358694150157474917137414970257188637270699134940023998433713504835350556664139727362897651812977796506155648682461572152279735676656891023541017242600453448352418772095711226503281897288485475738859562911853234613166360

611487489661284171333795649659356084670651052966401440845161008499607073136615907378100085329195962244536712980754060152868575958685606542348890023252875705976377915102356641973905524545194694757926954034988569804724627717032598080382292214975374670727157388411625327657588856969112182127276711023709520289464073251908634558051980681975972815395283519450040111936347049451972500570674519557586929770927261206733076239655399337744207232659595592182989805548977494161980819892107555620784097482228285271062298315039556086151625002653140203113289963304730593750126639864995140551566822299980512542433769042996362005308534089742426761635303327039941446161227818388717441428228560585960334775826613276549780 63

j. Public key parameter: 05 00

It is used in the ECDSA certificate in original. But now in RSA, this field must contain “NULL”. “05 00” also means “NULL” in DER(Distinguished Encoding Rules).

k. Subject key identifier: 5379bf5aaa2b4acf5480e1d89bc09df2b20366cb

This field provide a means of identifying certificates that contain a particular public key.

l. Key usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

In order to mark the key usage extension as critical and only.

m. Basic constraints: Subject type=CA, Path length constrain=None

Used to identify the type of the certificate holder/subject.

n. Fingerprint: 2b8f1b57330dbba2d07a6c51f70ee90ddab9ad8e

This is the unique identifier of the certificate.

3. Application and Security

-Make sure the software definitely comes from the software publisher

When we download a software from Internet, most people can't check whether this software is safe or not. Certificate is precisely a great method to solve this problem.

There are two part we need to check.

1. If the developer of this software is legal company or individual.
2. Is it tampered in the process when download this software to the host from Internet?

After download the software, we use the certificate to get the hash value. And then check this value whether it is corresponded to the hash value announced on the source website.

If these two values are the same, we can trust this software that indeed comes from the software publisher and it is not tampered by someone else.