Digital Certificate

Title : Digital Certificate

PRN : 2017BTECS000215

Theory :

Digital certificate is issued by a trusted third party which proves the sender's identity to the receiver and the receiver's identity to the sender. A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant’s public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or entity.

If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization. However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.

In a typical public-key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. By contrast, in a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public key certificate.

The most common format for public key certificates is defined by X.509.[2] Because X.509 is very general, the format is further constrained by profiles defined for certain use cases, such as Public Key Infrastructure (X.509) as defined in RFC 5280.

Digital certificate contains:-

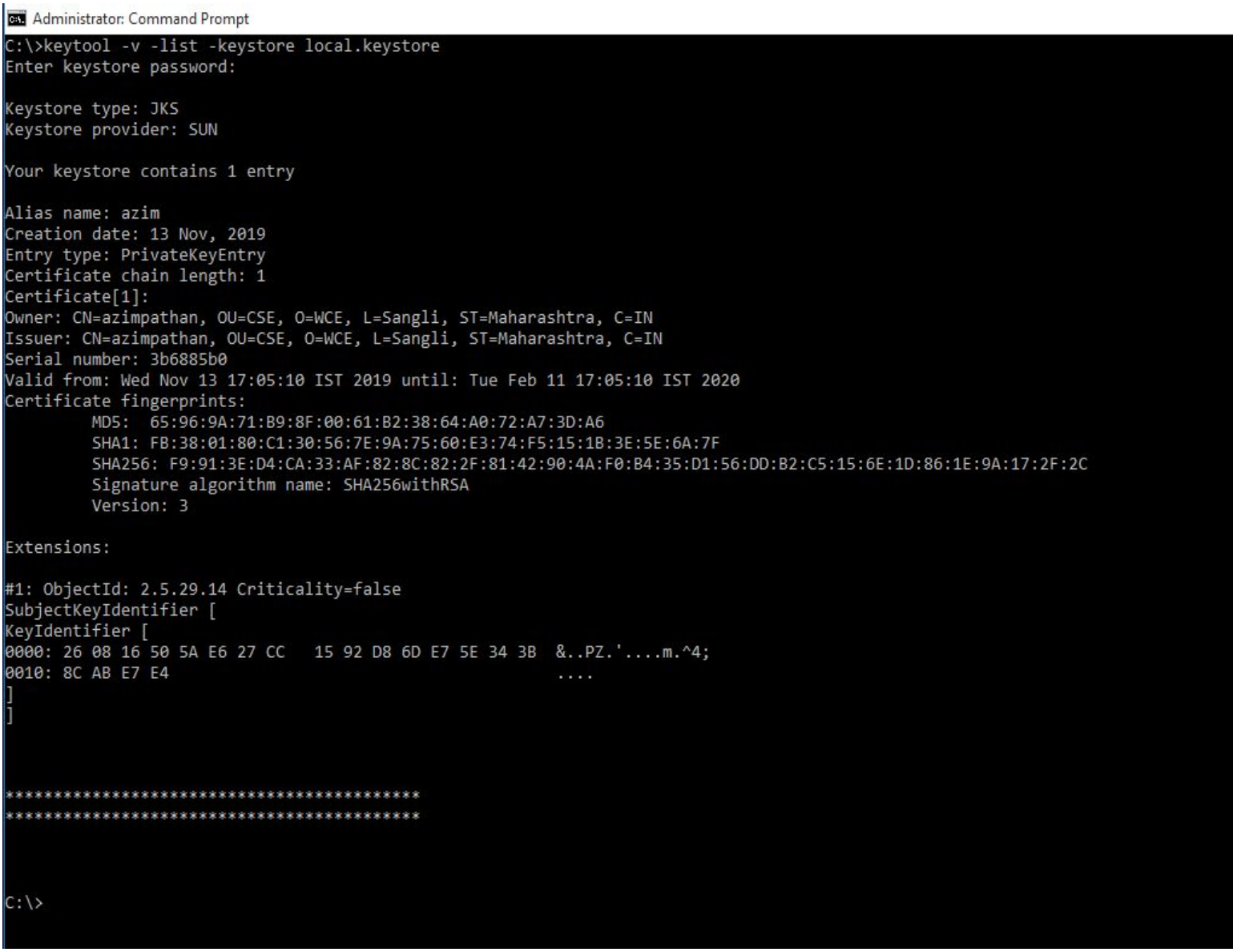
1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or entity identified by the certificate
3. Expiration dates.
4. Copy of the certificate holder's public key(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

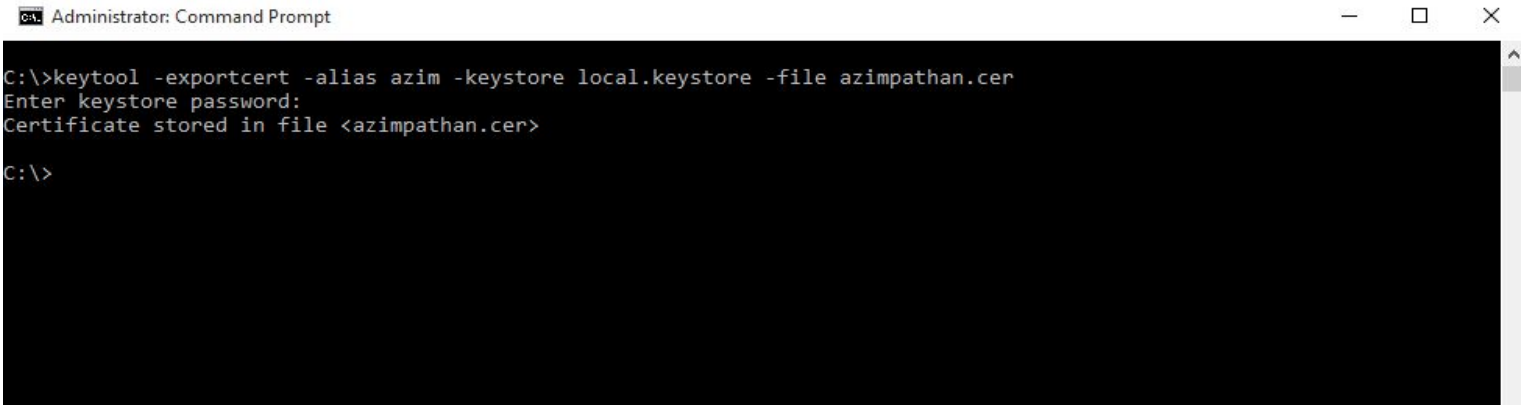
Questions and Answers :

Q.1) List out the contents of the digital certificate and write down the meaning of each.

Answer :

1. *Owner*
   Indicates name of certificate holder
2. *Issuer*
   Indicates the certification authority (CA) that issued the certificate
3. *Serial number*
   Uniquely identifies a certificate, the individual or entity identified by the certificate
4. *Valid from*
   Indicates the date when certificate was issued
5. *Until*
   Indicates the date of expiry of certificate
6. *Signature algorithm name*
   Indicates the algorithm used for generating digital certificate
7. *Version*
   Indicates the X.509 standard version





Q.2) Who the certificate is issued to?

Answer : azimpathan

Q.3) Who is the issuer of the certificate?

Answer : azimpathan

Q.4) What version of X.509 certificate is?

Answer : 3

Q.5) What cryptographic algorithm was used to generate the certificate?

Answer : SHA256withRSA

Q.6) What's the valid duration of the certificate?

Answer : Wed Nov 13 17:05:10 IST 2019 to Tue Feb 11 17:05:10 IST 2020

Q.7) What's the serial number of the certificate?

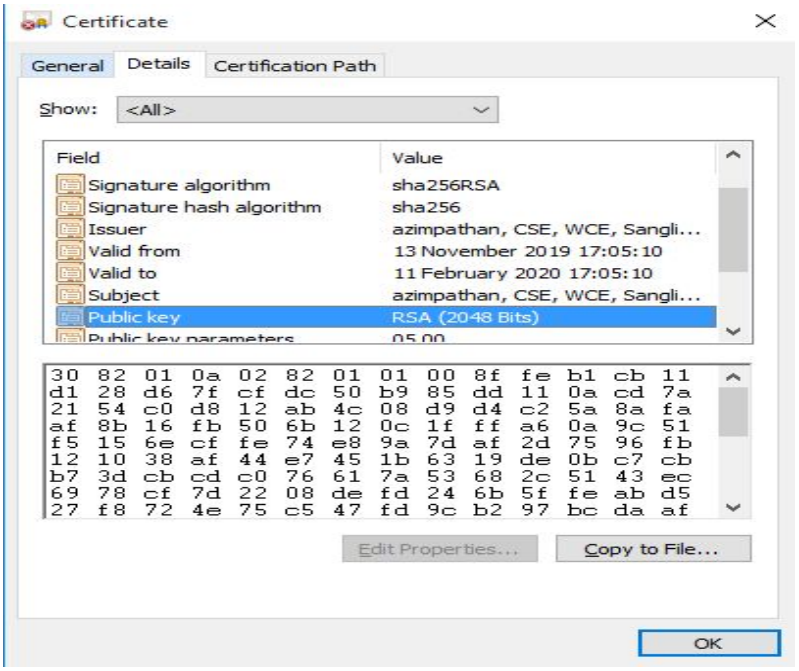
Answer : 3b6885b0

Q.8) The span of time during which the certificate is valid?

Answer : 10 days

Q.9) Show your certificate using at least two web browsers.

Answer :



Conclusion :

We studied how to use Java utilities like keytool and keystore to demonstrate generation of our own digital certificate. We also studied about the contents of the digital certificate.