H. J. THIM TRUST'S

THEEM COLLEGE OF ENGINEERING, BOISAR

DEPARTMENT OF COMPUTER ENGINEERING

2022-23

TE 6TH(CE)

EXPERIMENT NO 4 : CASE STUDY

SUBJECT: CRYPTOGRAPHY AND SYSTEM SECURITY

SUBJECT TEACHER: KETAKI PATIL

CASE STUDY ON

Digital Certificate [X.509]

SUBMITTED BY:

Gauravi Mokashi (29)

Digital Certificate [X.509]

Introduction: -

It is basically a certificate issued digitally, issued to verify a user's authenticity i.e., verifying the user sending a message is who he or she claims to be, and also to provide the receiver with the means to encode a reply.

Whoever wants to or an individual who wants to send encrypted messages applies for a digital certificate from a Certificate Authority (CA).

Digital certificate contains
Certificate version no.
Certificate serial no.
Algorithm for signature identify
Certificate issuer name
Validity details
Name of the certificate owner
Public key of certificate owner
Issuer unique identifier
Owner unique identifier
Extensions to certificate
Certificate authority and digital signature

Fig. Digital Certificate

1) Certificate version No. : It provides the particular version Do. of X.509

2) Certificate serial No: It is a unique integer no generated by certification authority.

3) Algorithm for signature identity: Algorithm which is used for identifying the authority signature

4) Certificate issues name:

5) Algorithm for signature identify:

6) Name of certificate owner : it identifies emailid contact no.

7) Public key certificate owner: the key which is used for communication between sender & receiver

8) Issues unique identify : it identifies the certificate authority

9) Owner unique identifier:

10) Extensions to certificate: additional information to certificate.

11) Certificate authority & digital signature: It is the information which is used for creating the digital certificate which is signed by certificate authority.

Digital certificate benefits: -

Digital certificates provide the following benefits:

- **Privacy.** When you encrypt communications, digital certificates safeguard sensitive data and prevent the information from being seen by those unauthorized to view it. This technology protects companies and individuals with large troves of sensitive data.
- **Ease of use.** The digital certification process is largely automated.
- **Cost effectiveness.** Compared to other forms of encryption and certification, digital certificates are cheaper. Most digital certificates cost less than $100 annually.
- **Flexibility.** Digital certificates do not have to be purchased from a CA. For organizations that are interested in creating and maintaining their own internal pool of digital certificates, a do-it-yourself approach to digital certificate creation is feasible.

Digital certificate limitations: -

Some limitations of digital certificates include the following:

- **Security.** Like any other security deterrent, digital certificates can be hacked. The most logical way for a mass hack to occur is if the issuing digital CA is hacked. This gives bad actors an on-ramp into penetrating the repository of digital certificates the authority hosts.
- **Slow performance.** It takes time to authenticate digital certificates and to encrypt and decrypt. The wait time can be frustrating.

- **Integration.** Digital certificates are not standalone technology. To be effective, they must be properly integrated with systems, data, applications, networks and hardware. This is no small task.
- **Management.** The more digital certificates a company uses, the greater the need to manage them and to track which ones are expiring and need to be renewed. Third parties can provide these services, or companies can opt to do the job themselves. But it can be expensive.

Conclusion:-

In this case study, we have studied ‘Digital Certificate’ its working, benefits and limitations.