Assignment No: 3

Title: Digital Certificates

A digital certificate is a system that allows users to validate a document's authenticity. When the notion was first proposed, it was assumed that it would be used to verify the legitimacy of communications, legal documents, and so on. While digital certificates are used for these purposes, their most prevalent usage is to validate the validity of executable files downloaded from the Internet.

A digital certificate system should have the following characteristics:

- It can be verified. Anyone who receives the document should be able to do a calculation to verify the certificate's accuracy; it is not forgeable.
- Only the person, corporation, or computer system that claims to have created the certificate has the ability to do so.

We can generate a digital certificate by encrypting a file with our private key, as previously explained. In practice, this results in an extremely slow authentication process. To boost efficiency, the authenticated file is hashed to generate a relatively short message digest. We may then encrypt only the hash value with our private key.

A digital certificate, also known as a public key certificate, is used to cryptographically link public key ownership to the entity that holds it. Digital certificates are used to share public keys for encryption and authentication.

Digital certificates contain the certified public key, identifying information about the entity that owns the public key, metadata about the digital certificate, and a digital signature of the public key issued by the certificate issuer.

Key pairs are used in public key cryptography: one private key retained by the owner and used for signing and decrypting, and one public key that can be used for encrypting data sent to the public key owner or authenticating the certificate holder's signed data. The digital certificate allows organizations to communicate their public key for authentication. Digital certificates are most typically employed in public key cryptography functions to establish Secure Sockets Layer (SSL) connections between web browsers and web servers. Digital certificates are also used to share keys for public key encryption and digital signature authentication.

Digital certificates are used by all major web browsers and web servers to ensure that unauthorized actors have not altered published material and to share keys for encrypting and decrypting web content. Digital certificates are also used to provide cryptographic assurance and data privacy in different circumstances, both online and offline.

Mobile operating systems, laptops, tablet computers, internet of things (IoT) devices, and networking and software applications that enable digital certificates assist protect websites, wireless networks, and virtual private networks.

The distribution, authentication and revocation of digital certificates are the primary functions of the public key infrastructure (PKI), the system that distributes and authenticates public keys. Depending on the particular hash function that is used, this message digest will be anywhere from 128 to 256 bits. A hash function h = H(M) is designed to meet the following criteria:

- It can be applied to any size of message M.
- It produces a fixed-length output h.
- It is easy to compute h = H(M) for any message M.
- It is a one-way function. For a given hash value, it is not feasible to find the original message M.
- It has collision resistance. For a given message M1, it is not feasible to find another message M2 that has the same hash value.
  A number of hash functions are in use, including MD5, SHA-1, and SHA-256. Weaknesses have been discovered in MD5 and SHA-1, thus it is currently recommended that SHA-256 be used.

For Example:
Let us suppose that you receive a certificate that purports to come from Company ABC. How do you know that this is not a forgery? There are two approaches to creating certificates:

Self-certification: In this approach, a company announces its public key ahead of time. To verify a document, you obtain that company's public key and then use it to verify the certificate. This is relatively straightforward but leads to the question of whether you can really trust that company's public key. Perhaps it was published by a forger.
Trusted party: In this approach, a trusted third party signs the certificate. Since you trust the third party, you can trust the authenticity of the document. This approach leads to a question of who are the trusted third parties and how do you know if you can trust them?

In practice, the term digital certificate usually refers to a file that conforms to the X.509 international standard. An X.509 file will include demographic information (name, address of the creator of the certificate). The X.509 standard utilizes a trusted third-party mechanism-a set of companies/ organizations that are globally trusted. A digital certificate (called a root certificate) identifying each of these companies is included with the operating system. On MS Windows, you can view these certificates by selecting Control Panel- Internet Options- Content- Certificates.

If a company wishes to publish a digital certificate, it must provide that certificate to one of these trusted root authorities, who will then sign it with their private key. Thus, a digital certificate will include an identification of the trusted signer of that certificate. You can then look at that signer's digital certificate to obtain the public key to verify the certificate that you are looking at.

Let us consider another example. Managers at Company XYZ have created a digital certificate that they wish to publish. To guarantee the authenticity of the certificate, they submit it to Company ABC, which is a designated root certificate authority. ABC verifies that XYZ is a valid company and then places their name in the certificate and signs the certificate with ABC's private key.
ff you were to receive this signed certificate; you could verify its authenticity with the following steps:

1. Obtain the signer's name from the certificate.
2. Look up the signer's root certificate and obtain his or her public key. 3. Use that public key to decrypt the hash in the original certificate.
4. Verify the accuracy of the hash.

After completing these steps, you would know that this certificate was created by Company XYZ. A digital certificate can be attached to a file that is intended for download over the Internet. In that case, what is being hashed is the entire file. Once this certificate has been properly signed by a root authority, any user can download it and be assured that it was created by the company that purports to have created it.

How are digital certificates used?

Digital certificates are used in the following ways:

- Credit and debit cards use chip-embedded digital certificates that connect with merchants and banks to ensure that the transactions performed are secure and authentic.
- Digital payment companies use digital certificates to authenticate their automated teller machines, kiosks and point-of-sale equipment in the field with a central server in their data center.
- Websites use digital certificates for domain validation to show they are trusted and authentic.
- Digital certificates are used in secure email to identify one user to another and may also be used for electronic document signing. The sender digitally signs the email, and the recipient verifies the signature.
- Computer hardware manufacturers embed digital certificates into cable modems to help prevent the theft of broadband service through device cloning.

As cyberthreats increase, more companies are considering attaching digital certificates to all of the IoT devices that operate at the edge and within their enterprises. The goals are to prevent cyberthreats and protect intellectual property.

Different types of digital certificates :

Web servers and web browsers use three types of digital certificates to authenticate over the internet. These digital certificates are used to link a web server for a domain to the individual or organization that owns the domain. They are usually referred to as *SSL certificates* even though the Transport Layer Security protocol has superseded SSL. The three types are the following:

- Domain-validated (DV) SSL certificates offer the least amount of assurance about the holder of the certificate. Applicants for DV SSL certificates need only demonstrate that they have the right to use the domain name. While these certificates can ensure the certificate holder is sending and receiving data, they provide no guarantees about who that entity is.

- **Organization-validated (OV) SSL** certificates provide additional assurances about the certificate holder. They confirm that the applicant has the right to use the domain. OV SSL certificate applicants also undergo additional confirmation of their ownership of the domain.

- **Extended validation (EV) SSL** certificates are issued only after the applicant proves their identity to the CA's satisfaction. The vetting process verifies the existence of the entity applying for the certificate, ensures that identity matches official records and is authorized to use the domain, and confirms that the domain owner has authorized issuance of the certificate.

The exact methods and criteria CAs follow to provide these types of SSL certificates for web domains is evolving as the CA industry adapts to new conditions and applications. There are also other types of digital certificates used for different purposes:

- **Code signing certificates** may be issued to organizations or individuals who publish software. These certificates are used to share public keys that sign software code, including patches and software updates. Code signing certificates certify the authenticity of the signed code.
- **Client certificates**, also called a digital ID, are issued to individuals to bind their identity to the public key in the certificate. Individuals can use these certificates to digitally sign messages or other data. They can also use their private keys to encrypt data that recipients can decrypt using the public key in the client certificate.

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.