Experiment No. 13

Create and Verify Digital Certificate Using Tool

Theoretical Background

What is a digital certificate

A digital certificate is an electronic document that verifies the identity of a user and prevents forgery of the document content. Simply put, the certificate makes sure the author of a document is who he claims to be and the content of the document was indeed written by the this author A digital certificate is issued by a Certificate Authority (CA, the issuer) an entity that verifies the identity of the applicant. CA signs the public key of the applicant with its own digital signature trusted and publicly available. This allows any software to identify this public key as valid and trusted and use it to encrypt or sign documents. To get a digital certificate you must submit an inquiry to a Certificate Authority that will issue a digital certificate. Common sources of digital certificates are:

VeriSign:

Verisign Inc. is an American company based in Reston, Virginia, United States that operates a diverse array of network infrastructure, including two of the Internet's thirteen root nameservers, the authoritative registry for the .com, .net, and .name generic top-level domains and the .cc and .tv country-code top-level domains, and the back-end systems for the .jobs, .gov, and .edu top-level domains. Verisign also offers a range of security services, including managed DNS, distributed denial-of-service (DDoS) attack mitigation and cyber-threat reporting.In 2010, Verisign sold its authentication business unit – which included Secure Sockets Layer (SSL) certificate, public key infrastructure (PKI), Verisign Trust Seal, and Verisign Identity Protection (VIP) services – to Symantec for $1.28 billion.The deal capped a multi-year effort by Verisign to narrow its focus to its core infrastructure and security business units. Symantec later sold this unit to DigiCert in 2017.

Fig:VeriSign

Thawte:

Thawte Consulting (pronounced "thought") is a certificate authority (CA) for X.509 certificates. Thawte was founded in 1995 by Mark Shuttleworth in South Africa. As of December 30, 2016, its then-parent company, Symantec Group, was collectively the third largest public CA on the Internet with 17.2% market share

Fig:Thawte

DigiCert:

DigiCert, Inc. is a US-based technology company focused on digital security and headquartered in Lehi, Utah with international offices in Australia, Ireland, Japan, India, South Africa, Switzerland and United Kingdom. As a certificate authority (CA) and trusted third party, DigiCert provides the public key infrastructure (PKI) and validation required for issuing digital certificates or TLS/SSL certificates. These certificates are used to verify and authenticate the identities of organizations and domains and to protect the privacy and data integrity of users' digital interactions with web browsers, email clients, documents, software programs, apps, networks and connected IoT devices.The company's products and services also include private and managed PKI deployments, the DigiCert CertCentral certificate management platform, the DigiCert PKI Platform and full customer support.

Fig:digicert

GlobalSign:

GlobalSign provides PKI and Identity and Access Management services to provide enterprises with a platform to manage internal and external identities for the Internet of Everything. The services allow organizations to deploy secure e-services, manage employee and extended enterprise identities and automate PKI deployments for users, mobile, and machine GlobalSign's identity and access management portfolio includes access control, single sign-on (SSO), federation and delegation services to help organizations and service providers create new business models for customer and partner interactions.GlobalSign's core PKI services allow its thousands of authenticated customers to conduct SSL-secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Additionally GlobalSign’s PKI services include a trusted root-chaining program for trusted PKI deployments, which allows the widely distributed and trusted GlobalSign root CA certificates to cryptographically chain subordinate root CAs for use in Microsoft CA and in other in-house CAs. Such chaining allows these non-commercial CAs to control their own internal PKI, typically issuing SSL and digital IDs for secure email and two-factor authentication.

Fig:Globalsign

DocuSign:

DocuSign, Inc. is an American company headquartered in San Francisco, California that allows organizations to manage electronic agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature, a way to sign electronically on different devices. DocuSign claims it has over 475,000 customers and hundreds of millions of users in more than 180 countries.Signatures processed by DocuSign are compliant with the US ESIGN Actand the European Union's Electronic Signatures Directive .In April 2018, DocuSign filed for an initial public offering. At the time of the IPO, the largest shareholders were venture investment firms Sigma Partners, Ignition Partners, Frazier Technology Ventures, and former CEO Keith Krach was the largest individual shareholder. None of the original founders, or current CEO Daniel Springer, are major shareholders.The company went public on the NASDAQ on April 27, 2018.

Fig:DocuSign:

Some Certificate Authorities offer digital certificates for free, others require payment. You can also create a self-signed certificate yourself using free Open SSL. Please refer to the Digital Certification Manager section to learn how you can do this.

- The Basics of Cryptography and Digital Certificates

If you think about it, it takes a great deal of trust, even courage, to go on the Internet, especially if you're sending credit card information, personal history, medical information and more. On its own, the network is simply a highway for data super highway, as it's always been called. But on its own, it is an unsecured network. Everyone with a connection can hop on and be themselves, or pretend to be themselves. Some people are out there not simply to receive information, but to steal or obtain it with trickery. That's where security data protection measures like cryptography come into the picture.

- How do I create a digital certificate?

Click Start, point to All Programs, click Microsoft Office, click Microsoft Office Tools, and then click Digital Certificate for VBA Projects. The Create Digital Certificate box appears. In the Your certificate's name box, type a descriptive name for the certificate. Click OK.

- How do I verify a certificate?

To verify a certificate, a browser will obtain a sequence of certificates, each one having signed the next certificate in the sequence, connecting the signing CA's root to the server's certificate. This sequence of certificates is called a certification path.

- Type of Digital Certificate?

Secure Socket Layer Certificate [SSL] Digi-SSL™

Software Signing [Code Signing Certificate] Digi-Code™

Client Certificate [Digital ID] Digi-ID™

- Digital certificates: secret-key encryption.

The other type of encryption uses a different process. A digital certificate is one example. Digital certificates are issued to individuals by a certificate authority (CA), a private company that charges either the user or the receiver for issuing a certificate. The company DocuSign is an example of an issuer of digital certificates. Organizations will use digital certificates to verify the identities of people and organizations they do business with...and need to trust. For example, an online retail store, or even an organization accepting a payment for merchandise, wants to make sure that someone sending credit card information is the actual owner of the card and not someone with a stolen credit card number trying to use it from a foreign country. A digital certificate contains information that helps guarantee a person is not an impostor. You get a digital certificate by request by visiting a CA website and providing information that identifies you.

Your digital certificate will contain:

Your name

The name of the certificate authority

A unique certificate serial number, its expiration date, etc.

A unique private key (to include with messages you send)

The digital signature of the CA

Once it's issued, the CA will put the certificate on your hard drive, along with a private key. Once that's all in place, you're ready to send certified emails. Oftentimes, an organization will request that you obtain a digital certificate before you can communicate with them digitally, for their own protection. When you send an email using a digital certificate, it contains only the public information of the user such as ID, name, and public key. The personal component of your signature credentials, the private key, is not included in the certificate. Compared to a handwritten signature, which few people bother to verify, a digital signature is hard to forge or imitate because of all the safeguards that are in place.

Conclusion

We have conclude that how should we Create and Verify Digital Certificate Using Tool.

Exercise

1) What is a Digital Certificate?
2) How do I create a Digital Certificate?
3) How do I Verify a Certificate?
4) Write A Type of Digital Certificate?

Answers

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

Marks obtained			Dated signature of Teacher
Process Related (15)	Product Related (10)	Total(25)	