# Digital Certificates
(Public Key Infrastructure)

Reshma Afshar
Indiana State University

October 2015

# Contents

# List of Figures

# Abstract

## 1 Introduction

A **Digital Certificate** is an electronic document which provides information to prove the identity of an entity. It binds the identity of an entity to its public key. Digital certificates contain some standard information such as the name of the certificate holder, public key, validity period, and also the digital signature of the certification authority.

**Public Key Infrastructure** (PKI) is used to manage keys and certificates. It creates digital certificates which bind public keys to entities, stores them securely and revokes them when required. Digital certificates in public key infrastructure are used to establish integrity and ownership of a public key.

A **Certification Authority** (trusted third party) issues a certificate to an entity after verifying its identity. (Entity can be a web user or a web server). The certificate contains the entity's public key and identification information. It is signed by the certificate authority using its private key and the certificate is made publicly available. Any entity can validate the identity and public key of another entity, by obtaining its digital certificate and verifying the signature using the certificate authority's public key. This way the entity knows that the digital certificate is valid as it is signed by the trusted certificate authority and by obtaining another users public key from the certificate the entity knows that the public key is valid. So public key infrastructure provides a secure environment for online transactions, confidential email and e-commerce.

## 2 History

Public key infrastructure is based on asymmetric cryptography. In 1976, two mathematicians, Whitfield Diffie and Martin Hellman discovered asymmetric cryptography. Prior to asymmetric cryptography, symmetric cryptography was used. In symmetric cryptography the same key was used for encryption and decryption. So it was necessary to have a separate key for communication with each entity. Hence asymmetric cryptography which uses two keys (a private key for encryption and a public key for decryption) was introduced. This concept was only a theory at that time.

With the development of internet there was a need for secure communication, where the identity of an entity could be authenticated. There was also a need for development of encryption algorithms and an infrastructure. In 1977, three mathematicians, Ronald L.Rivest, Adi Shamir and Leonard M Adleman, applied Diffie and Hellman's theories and developed an encryption algorithm called RSA. Later SSL protocol was developed which provided authentication and key establishment.

The development of public key infrastructure for secure communication and business transaction began with **X.509** certificate standard. Public key infrastructure consists of key exchange mechanism, digital certificates, certification authority and encryption technologies. In the X.509 public key infrastructure standard, certificates are issued by a trusted third party called the certification authority. Certificate authority verifies the identity of the entities and it signs, encrypts and issues the certificate. The X.509 PKI provides a hierarchical architecture of certificate authorities to issue certificates. In this architecture a root certificate authority can issue a certificate to its subordinate certificate authority. There have been three versions of this standard, currently version 3 X.509 is used. It contains the following fields: version, serial number, signature algorithm , issuer, validity, subject, subject public key information, signature, issuer unique identifier, subject unique identifier and extensions. This standard includes concepts like certificate authorities, certificate trusts, certificate revocation lists which provide a framework for the public key infrastructure.

# 3 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a collection of servers used to create and manage public keys and digital certificates. It creates digital certificates which bind public keys to entities, stores them securely and revokes them when required.

Generally passwords are used for authentication, for the transfer of information, but for the transfer of confidential information in distributed environment, a more secure authentication method is needed. Such an authentication method must confirm the identity of the entities involved in the communication and must authenticate the information that is being transferred. One such method is the public key infrastructure.

So the public key infrastructure provides a secure environment for online transactions, confidential email and e-commerce by:

- Authenticating the identity of the entities (the sender and the receiver)
- Maintaining the data integrity.

Consider an example where asymmetric key encryption is used for communication between two entities say Alice and Bob. Alice uses Bob's public key to encrypt the message and sends it to Bob. Bob decrypts the received message using his private key and reads the message. The main drawback of this method is that there is no way to guarantee that the public key which Alice used for the encryption of the message actually belongs to Bob or some other malicious user claiming to be Bob.

To address this problem PKI has evolved. To ensure the identity of the entities in a communication, PKI uses a trusted third party to distribute keys and to authenticate the identities. This is done by integrating digital certificates.

Components of public key infrastructure are:

- Certificate Authorities
- Registration Authorities
- Certificate Repositories
- Digital Certificates

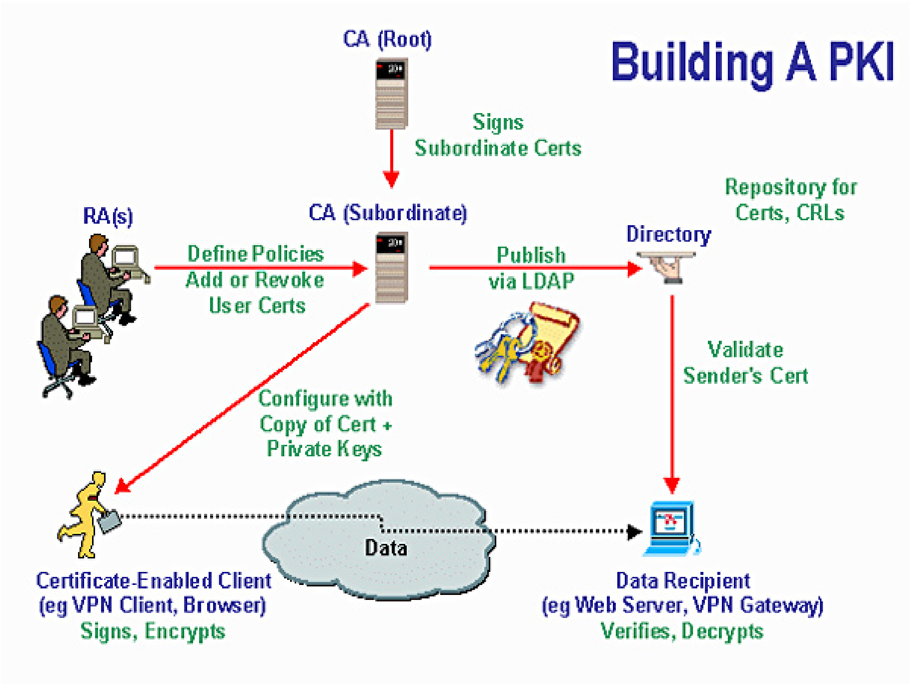


Figure 1: PKI Components

### 3.1 Certificate Authority

Certificate Authority (CA) is a trusted third party that authenticates the identities of servers, individuals and other entities. A CA confirms the identity of the entity by issuing a digital certificate that binds the identity with the pubic key of that entity.

Functions of the CA are:

- Issuing certificates
- Maintain and issue Certificate Revocation Lists (CRLs)
- Publish its certificates and CRls
- Maintain status information of certificate expiration dates

These tasks may be delegated by the CA.

One of the main function of a certificate authority is issuing certificates (i.e. creating the certificates and signing them). Consider a server that has requested for a digital certificate for itself. After its identity has been verified by the registration authority, the request is then forwarded to the certificate authority. The certificate authority generates a certificate in a standard format (X.509 certificate standard). The certificate contains the identity of the server and its public key. This certificate is then signed by the certificate authority with its own private key and the certificate is issued to the requesting server. The CA's signature on the certificate verifies the integrity of the certificate. A copy of the certificate is locally saved and it may also be published in public repositories.

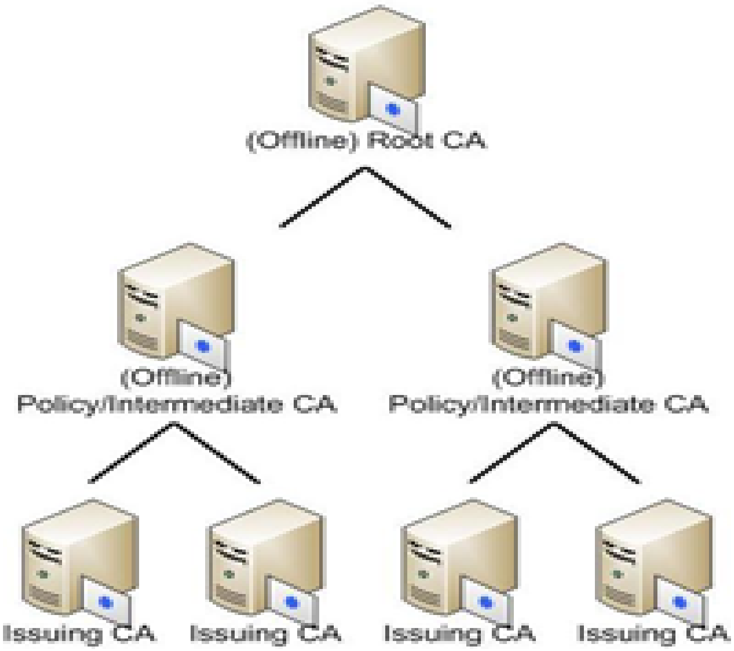
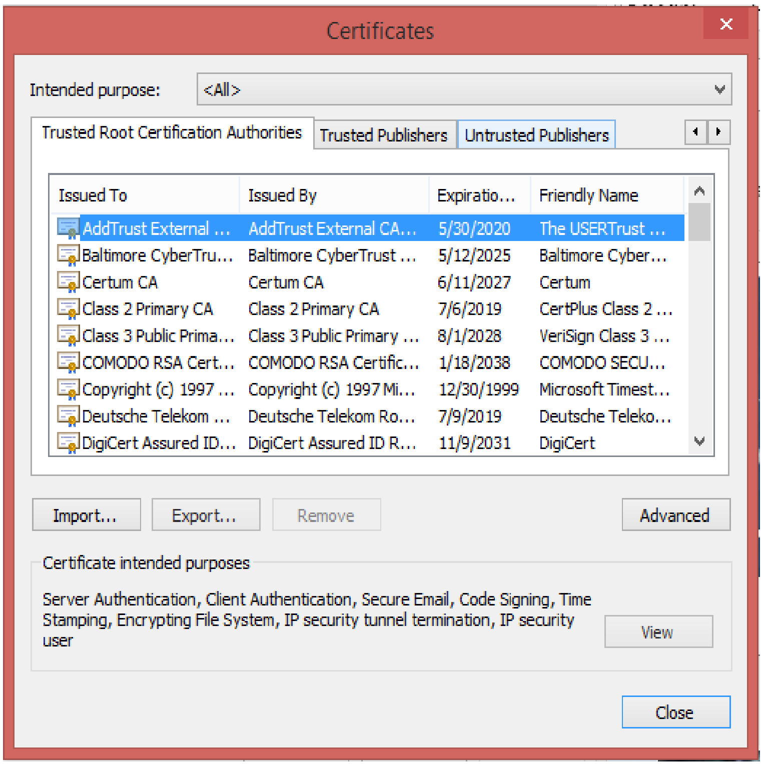

(Offline) Root CA
(Offline) Policy/Intermediate CA
(Offline) Policy/Intermediate CA
Issuing CA
Issuing CA
Issuing CA
Issuing CA

Figure 2: Certificate Hierarchy

The certificate authority is the root of trust in a public key infrastructure. When a hierarchical architecture of CA is followed, there is a root CA which has its own digital certificate. Such a certificate is self-signed. The root CA creates a chain of trust by signing certificates of the subordinate certificate authorities. This means that the certificates issued by subordinate CA's are trusted by the root CA. So a web browser or a user can trust a certificate issued by the subordinate CA if it trusts the root CA. Most web browsers and operating systems have the certificate of the root CA embedded in them. For example in Internet Explorer, if we go to the Content tab in Internet Options, we can see the certificates. It has all certificates of the CA's that the browser trusts.



Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| AddTrust External ... | AddTrust External CA... | 5/30/2020 | The USERTrust ... |
| Baltimore CyberTru... | Baltimore CyberTrust ... | 5/12/2025 | Baltimore Cyber... |
| Certum CA | Certum CA | 6/11/2027 | Certum |
| Class 2 Primary CA | Class 2 Primary CA | 7/6/2019 | CertPlus Class 2 ... |
| Class 3 Public Prima... | Class 3 Public Primary ... | 8/1/2028 | VeriSign Class 3 ... |
| COMODO RSA Cert... | COMODO RSA Certific... | 1/18/2038 | COMODO SECU... |
| Copyright (c) 1997 ... | Copyright (c) 1997 Mi... | 12/30/1999 | Microsoft Timest... |
| Deutsche Telekom ... | Deutsche Telekom Ro... | 7/9/2019 | Deutsche Teleko... |
| DigiCert Assured ID... | DigiCert Assured ID R... | 11/9/2031 | DigiCert |

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user

Figure 3: Internet Explorer's installed CA certificates

Another function of certificate authority is to maintain and issue Certificate Revocation List's (CRLs). The certificate authority has the right to suspend , revoke or renew a certificate. During the life of any certificate it can be suspended by the CA. At this stage its validity is temporarily suspended. The CA can revoke a certificate any time before its normal expiration. At this stage the certificate is not valid. This may happen when a private key is lost or when an unauthorized user gains knowledge of the private key. In such cases the CA updates the CRLs and its internal records with the required certificate information and time stamp. The CRLs are signed by the CA and are placed in a public repository.

Certificate Authority issues the certificates with an expiration date. Once the certificate has expired, it can no longer be used for authentication. The owner of a certificate is informed about an upcoming expiration of the certificate so that the user can follow a renewal process.

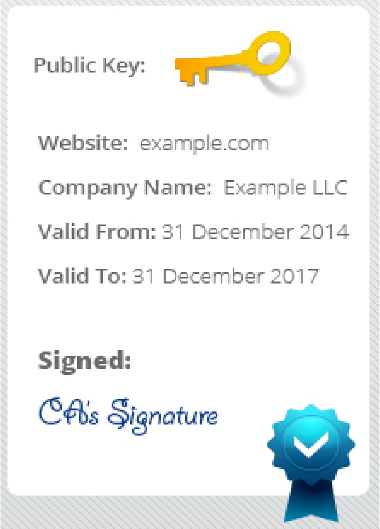
## 3.2 Registration Authority

Registration authority is a part of the public key infrastructure. It verifies the requests for digital certificates by validating the identity of the entity that places the request. For example if a company requests for a digital certificate, then the RA verifies the identity of the owner by checking various identity documents such as divers license or a pay stub etc. After verifying the identity, the RA then forwards the valid request to the CA. Then a digital certificate is issued by the CA. A CA can have more than one RA's. Each RA has a name and public key by which the CA can recognize it.Each RA is certified by its corresponding CA. Any message that the CA receives with the RA's signature is a trusted message.

## 3.3 Certificate Repositories

Certificate repositories are mainly used to store and distribute certificates. All the issued certificates are stored in the repository so that the applications can retrieve them easily. A directory system is best used for this process. Lightweight Directory Access Protocol (LDAP) is one of the best technology at present for certificate repositories. These directories store the certificates and make it easier for applications to retrieve these certificates for a user. This directory system supports a large number of certificates. It stores the certificates and the public keys for those certificates. The main advantage of these directories is that they can be used in highly distributed networks and they are made publicly accessible. It also makes the search easier by storing the certificates in a hierarchical structure. The certificate repository also contains certificate status information and revocation information. Apart from storing and distributing it also updates the certificates and their status.

## 3.4 Digital Certificates



Public Key:

Website: example.com

Company Name: Example LLC

Valid From: 31 December 2014

Valid To: 31 December 2017

Signed:

CA's Signature

Figure 4: Digital Certificate

A Digital Certificate is an electronic document which provides information to prove the identity of an entity. It binds the identity of an entity to its public key. Digital certificates are generated in a standard format.

Consider a user who wants to shop online through an online shopping web site such as Amazon. The user types the link to the Amazon web site and the web browser connects to the web site. The main concern here is whether the web site truly belongs to Amazon company or is it a malicious party posing to be Amazon. To solve this trust issue, digital certificates are used in a public key infrastructure, and a trusted third party is used which can establish the identity of the entity and integrity of the public key.

### 3.4.1 Certificate Structure

The X.509 certificate standard is widely used to structure digital certificates. There have been three versions of this standard and at present version 3 of this standard is being used.

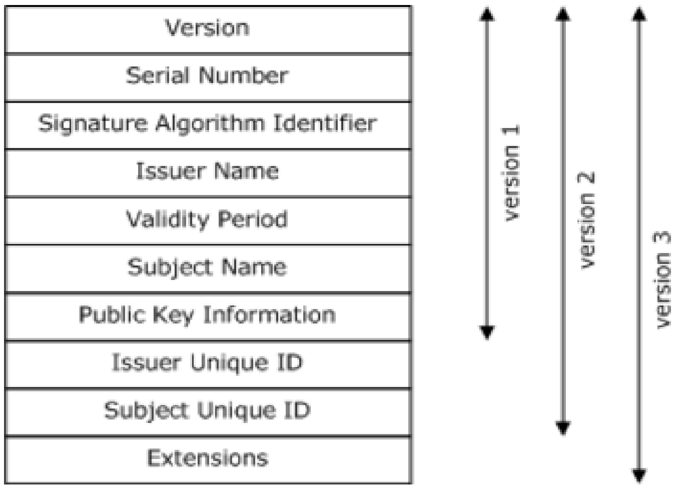


Figure 5: Structure a of X.509 Digital Certificate

There are ten basic fields in a digital certificate. Six of which are mandatory and four are optional fields.

The mandatory fields are:

- Serial number
- Signature algorithm
- Issuer name
- Validity period
- Subject name
- Public key information

The optional fields are:

- Version
- Issuer unique ID
- Subject unique ID
- Extensions

These optional fields are used in version 2 and version 3.

**Version:** This field specifies the version number of the certificate. This can be either version 1 or 2 or 3. When extensions are included in a certificate, this field indicates version 3. If the it includes unique identifiers without extensions, then it is version 2. If it does not include extensions and unique identifiers, then it is version 1.

**Serial number:** It is a unique positive number assigned for each certificate. It is assigned by the issuer to identify the certificate.

**Signature Algorithm:** This field indicates the algorithm used by the issuer to sign the certificate. Some examples are: RSA encryption algorithm with SHA-1 hashing algorithm, RSA with MD5 or DSA with SHA-1 algorithm.

**Issuer:** This field indicates the X.500 Distinguished Name of the trusted third party which signed and issued the certificate.

**Validity:** Validity indicates the date from when the certificate is valid (i.e. valid from) and the date until when the certificate is valid (i.e. valid to).

**Subject:** Subject is the distinguished name of the entity that owns the certificate. The owner is the entity associated with the public key in the certificate. Owner can be a CA, RA, person, company, or application.

**Public key information:** This field contains the public key of the subject and the algorithm identifier.

**Issuer unique ID:** This is a unique identifier to facilitate the reuse of issuer's name over time.

**Subject unique ID:** This field contains a unique identifier to facilitate the reuse of subject's name over time.

**Extensions:** This field is present in version 3 certificates. The extensions are used to give more information about the certificate which is not given by the basic fields. Extensions have three basic elements: an extension identifier, criticality flag and extension value. Extension identifier gives the format of the extension value, criticality flag indicates that the extension is important. Some of the extensions are: key usage, subject name alternative, basic constraints, policy constraints, name constraints etc.

### 3.4.2 Types of Certificates

Based on the usage, digital certificates can be of different types. Such as:

- **Personal:** Certificates which are used by individuals for secure email.

- **Organisation:** Certificates used by corporate companies for internal use, to identify employees of the company for secure email.
- **Server:** Certificates used by web site owners to establish a secure connection with a user by proving the ownership of the domain name.
- **Developer:** Certificates used by developers to prove the identity of the applications and the software programs.
- **Government:** Certificates used for government security.

Based on the different classes of certificates, CA performs different levels of verification to check the identity of the owner. If a certificate belongs to a higher class, such as certificates used for online transactions, then a higher level of verification is performed. For certificates which are used for personal email, a lower amount of verification may be needed. Depending on the usage of the certificates different levels of verification are performed by the CA.

### 3.4.3 Working of Digital Certificates

Digital Certificates in a Public Key Infrastructure work in the following way:

1. Consider an online shopping web site such as Amazon. The server of the Amazon company requests for a digital certificate from a certificate authority.
2. The certificate authority verifies the identity of the company and generates a digital certificate. It hashes the contents of the certificate and signs (encrypts) the hash value using its private key. It includes this signature in the certificate and issues the certificate to the company.
3. A user who wants to connect to the Amazon web site enters the HTTPS web address in his browser. The browser tries to connect to the web site.
4. A digital certificate is sent from the web server of the Amazon company to the browser.
5. When the browser receives a certificate from the web server it performs the following tasks:
    - It checks whether the CA who signed the certificate is trusted by the browser. The browser already has the trusted CA

certificates installed, so it has the public key information of the CA.

- With the public key of the CA, the browser decrypts the signature in the company's certificate and obtains a hash.
- It also computes a new hash of the content in the certificate..
- If both the hashes match, then the signature in the certificate is verified to be signed by the trusted CA and the public key in the certificate is valid.
- Now the name in the certificate is checked against the web site's name. If it matches then a secure connection is established for the online transactions.
- The browser also checks whether the certificate is within its expiry period.

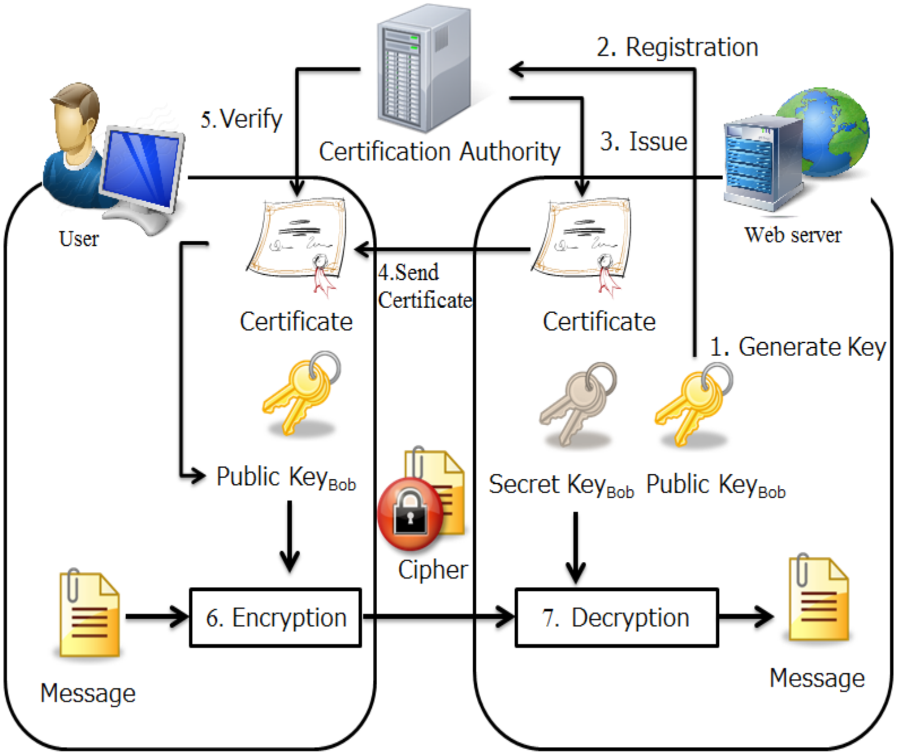


Figure 6: Working of Digital Certificates

All this process is transparent to the user and it is carried out in milliseconds. The integrity of the certificate is guaranteed, as long as the CA's signature can be verified. It also makes sure that the public key in the certificate is valid and has not been tampered with. It guarantees that the public key belongs to the owner of the certificate and it can be used for secure communication. Checking the name on the certificate against the web site's name helps in preventing man-in-the-middle attacks, where a malicious user modifies the certificate and claims to be the site that the user wants to establish communication with.

### 3.4.4 How to know that a web site has valid certificate.

A site which is secured with a digital certificate has a 'https://' as a prefix to the web address. This means "secure HTTP". When a browser connects to a https site, it displays a padlock symbol or a green browser bar (depending on the browser being used), to show that the web site has a valid certificate and is trusted. Internet explorer shows a locked icon in the status bar, whereas Google Chrome shows a padlock with green address bar. Clicking on the padlock shows which certificate authority signed the certificate, which algorithms are used for encryption and authentication etc.

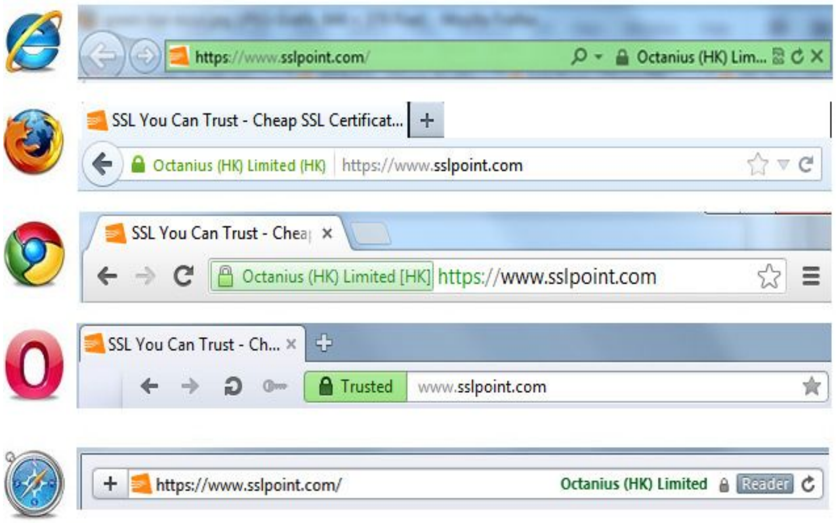
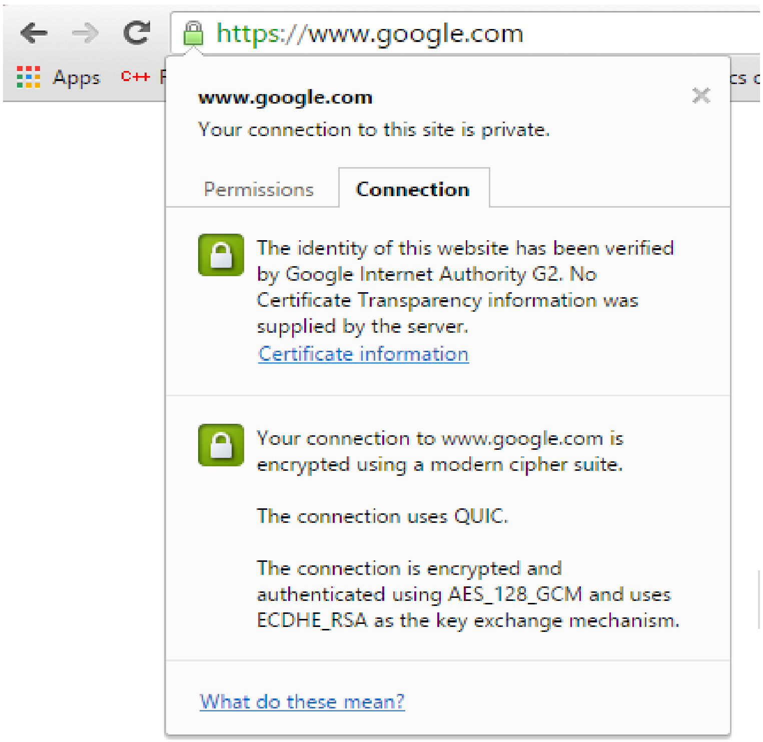

https://www.sslpoint.com/
Octanius (HK) Lim...
SSL You Can Trust - Cheap SSL Certificat...
Octanius (HK) Limited (HK)
https://www.sslpoint.com
SSL You Can Trust - Cheap
Octanius (HK) Limited [HK]
https://www.sslpoint.com
SSL You Can Trust - Ch...
Trusted
www.sslpoint.com
https://www.sslpoint.com/
Octanius (HK) Limited
Reader

Figure 7: Different web browsers showing valid certificates.



www.google.com

Your connection to this site is private.

The identity of this website has been verified by Google Internet Authority G2. No Certificate Transparency information was supplied by the server.

Certificate information

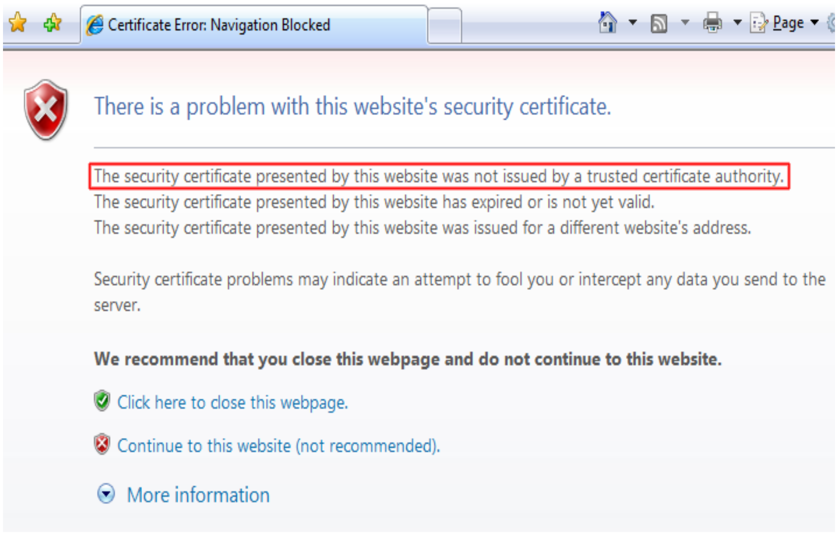
Your connection to www.google.com is encrypted using a modern cipher suite.

The connection uses QUIC.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

What do these mean?

Figure 8: Shows which CA signed the certificate and the encryption algorithm used.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

More information

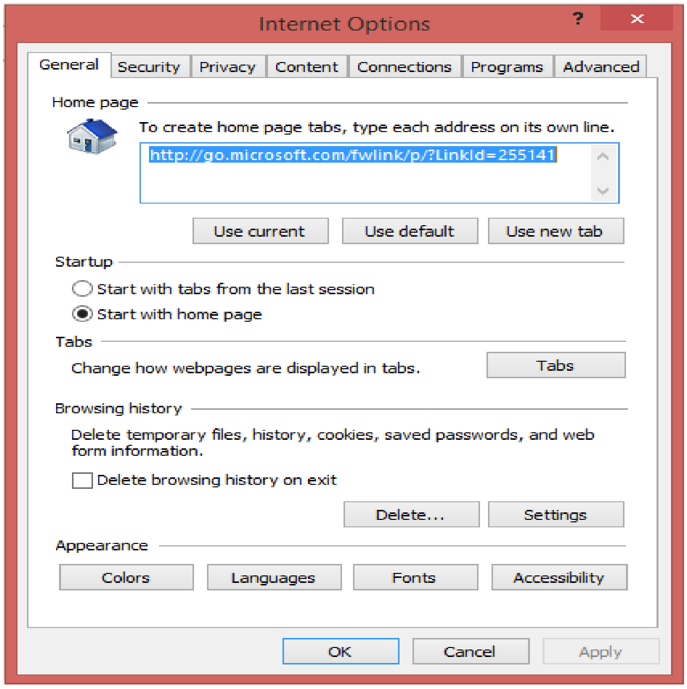
Figure 9: Browser indicating that the certificate is not valid

### 3.4.5 How to view Digital Certificates on personal computer.

The trusted CA certificates are stored by the operating system and the browser. To view stored digital certificates in Internet Explorer:

1. Open Internet Explorer and click on Tools
2. Select Internet Options from the drop down list
3. Click on Content tab
4. Click on Certificates button.

This shows various tabs which have personal certificates, Intermediate certificates, trusted root certificates etc. To view the certificate details, select the certificate and click view button. this shows the issuer, subject, validity period, version, signature algorithm and other certificate details.



Internet Options

Home page

To create home page tabs, type each address on its own line.

http://go.microsoft.com/fwlink/p/?LinkId=255141

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs.

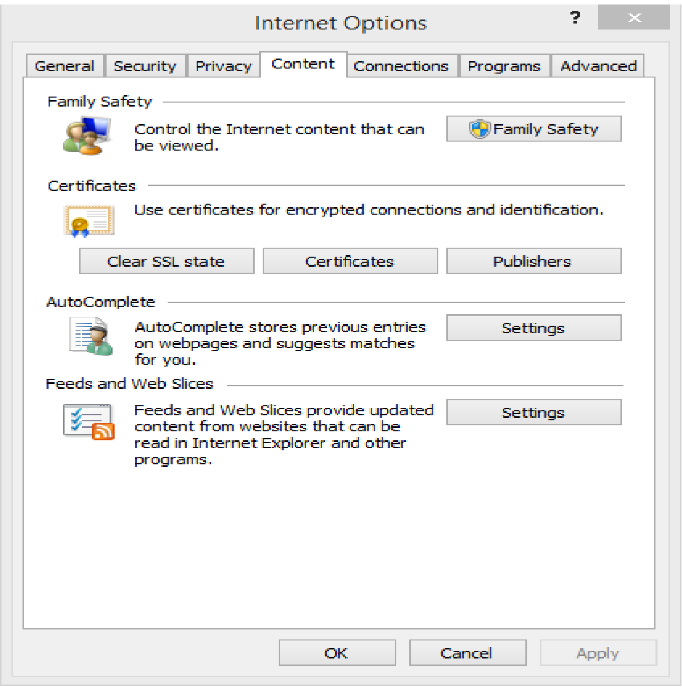
Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Appearance

Figure 10: Internet Options in Internet explorer



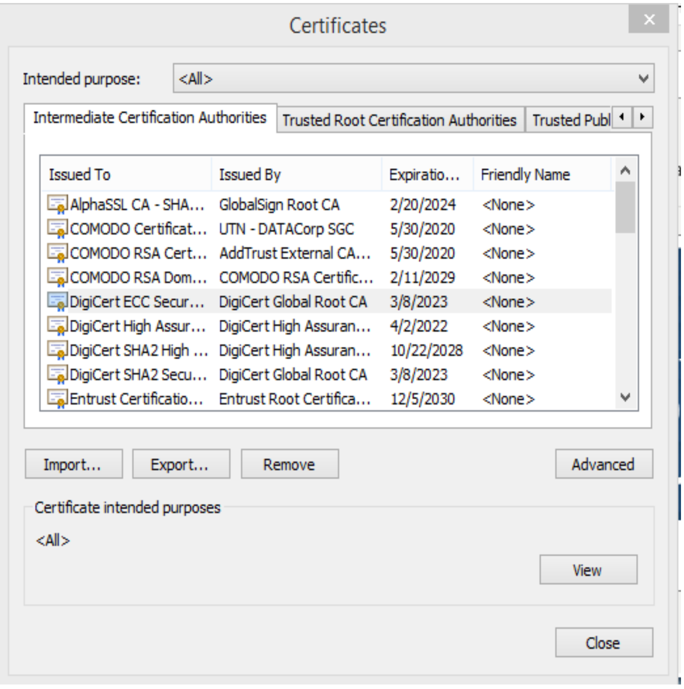
Control the Internet content that can be viewed.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Figure 11: Internet Options->Content


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
View
Close

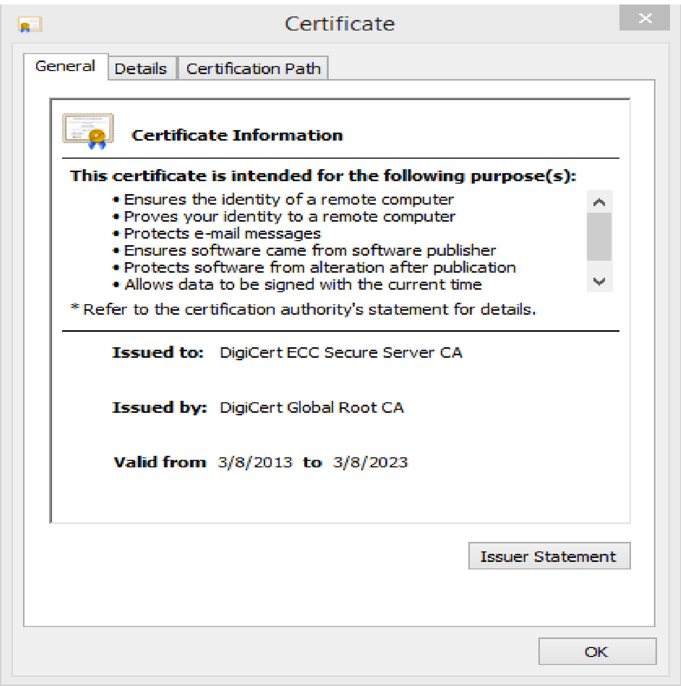
Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| AlphaSSL CA - SHA... | GlobalSign Root CA | 2/20/2024 | <None> |
| COMODO Certificat... | UTN - DATACorp SGC | 5/30/2020 | <None> |
| COMODO RSA Cert... | AddTrust External CA... | 5/30/2020 | <None> |
| COMODO RSA Dom... | COMODO RSA Certific... | 2/11/2029 | <None> |
| DigiCert ECC Secur... | DigiCert Global Root CA | 3/8/2023 | <None> |
| DigiCert High Assur... | DigiCert High Assuran... | 4/2/2022 | <None> |
| DigiCert SHA2 High ... | DigiCert High Assuran... | 10/22/2028 | <None> |
| DigiCert SHA2 Secu... | DigiCert Global Root CA | 3/8/2023 | <None> |
| Entrust Certificatio... | Entrust Root Certifica... | 12/5/2030 | <None> |

Certificate intended purposes

<All>

Figure 12: Intermediate Certificates list



**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

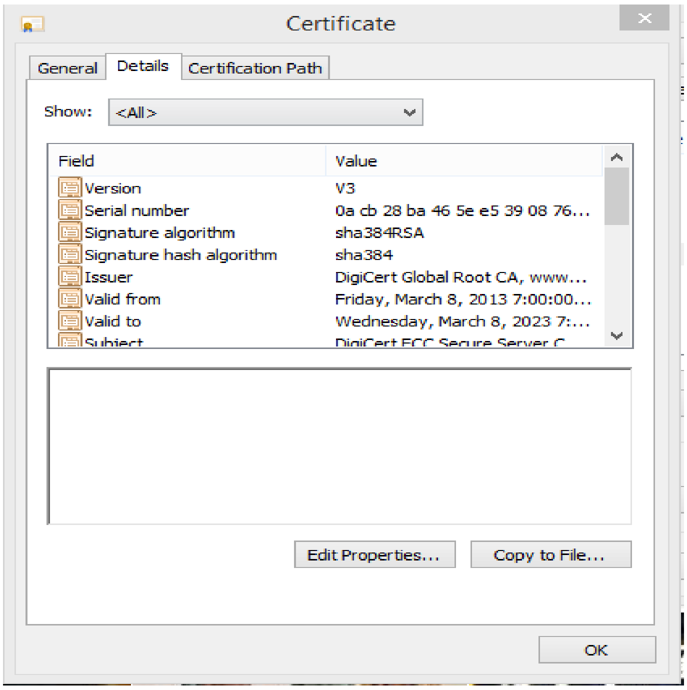
* Refer to the certification authority's statement for details.

**Issued to:** DigiCert ECC Secure Server CA

**Issued by:** DigiCert Global Root CA

**Valid from** 3/8/2013 **to** 3/8/2023

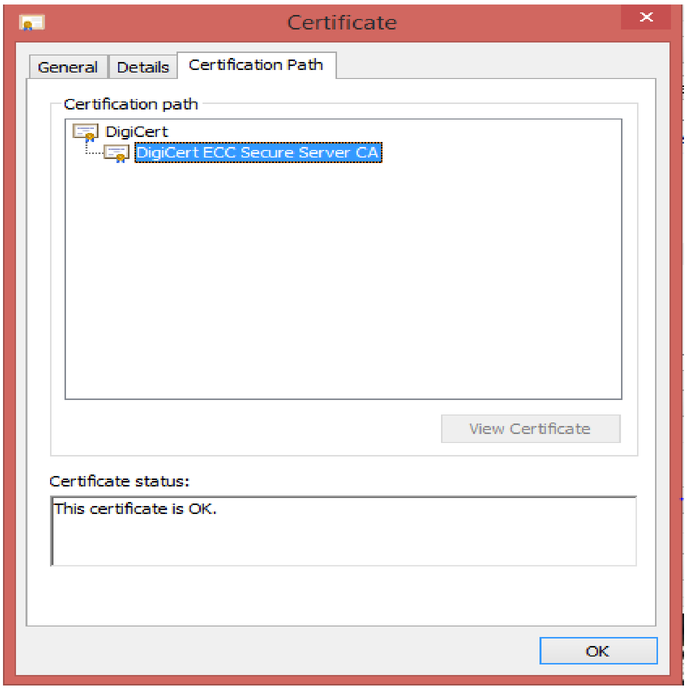
Figure 13: Digital Certificate Information



Show: <All>

| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 0a cb 28 ba 46 5e e5 39 08 76... |
| Signature algorithm | sha384RSA |
| Signature hash algorithm | sha384 |
| Issuer | DigiCert Global Root CA, www... |
| Valid from | Friday, March 8, 2013 7:00:00... |
| Valid to | Wednesday, March 8, 2023 7:... |
| Subject | DigiCert ECC Secure Server C |

Figure 14: Digital Certificate details



DigiCert
DigiCert ECC Secure Server CA

This certificate is OK.

Figure 15: Certification path

## 4 Advantages and Disadvantages

Advantages of using Digital Certificates in Public key Infrastructure:

1. Authentication: By using digital certificates the identity of the entity can be verified.

2. Secure: It assures that the public key belongs to the owner of the certificate an so a secure communication can established for confidential email, e-commerce and online transactions.

3. Integrity: Integrity is guaranteed a long as the CA's signature on the digital certificate can be verified.

4. It prevents man-in-the-middle attacks, where a malicious user pretends to be the web site that the user wants to connect with.

5. Non-Repudiation: The signature on the certificate guarantees that only the web site owner has the private key associated with the public key in the certificate.

6. The process of verification and authentication is transparent to the end user and the process of authentication takes only a few milliseconds.

7. Certificates are supported by many enterprise networks and applications.

Disadvantages are:

1. A browser does not give a warning when a web site changes the certificate.
2. A user has to blindly trust that the developer of the OS has installed genuine root certificates and not fraudulent certificates.
3. A fraudulent root certificate can be installed in the browser when a malicious user gains access to the personal computer. In this case the browser will not report any security warning while browsing sites that use the fraudulent certificate.

## 5 Conclusion

Public key infrastructure provides an effective authentication method through digital certificates. It ensures a secure communication that is necessary in today's world as majority of the transactions are online. It provides secure exchange of confidential information. Certificates are being used in various network applications and enterprises. Usage of certificates is not limited to personal computers, they are widely being used in smart phones, smart card and other devices as well.