Digital Certificate - Implementing SSL for your website

INFORMATION ASSURANCE AND SECURITY 1

GODWIN S. MONSERATE

What is a Digital Certificate?

- A **Digital Certificate** is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI).
- **Digital Certificate** is also known as a public key **certificate** or identity **certificate**.

What is a Digital Certificate?

- A digital certificate (DC) is a digital file that certifies the identity of an individual or that certifies the identity of an individual or institution, or even a router seeking institution, or even a router seeking access to computer- based information.
- It access to computer- based information. It is issued by a Certification Authority, and serves the same purpose as a driver’s and serves the same purpose as a driver’s license or a passport

What is a Digital Certificate?

- The Certification Authority (CA) signs the certificate with their own private key. An SSL/Digital Certificate typically contains the following information:
  - Owner's public key
  - Owner's name
  - Expiration date of the public key
  - Name of the issuer (the Certifying Authority that issued the Digital Certificate)
  - Serial number of the Digital Certificate
  - Digital signature of the issuer

Certification Authorities

- CA’s are the digital world’s equivalent to passport offices.
- They issue digital equivalent to passport offices.
- They issue digital certificates and validate holders’ and validate holders’ identity and authority.
- They embed an individual or institution’s public key along with other identifying information into each digital certificate and then cryptographically sign it as a tamper-proof seal verifying the integrity of the data within it and validating its use.

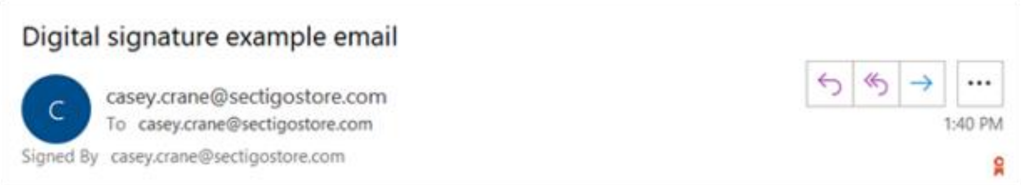
What does it do?

- Digital Certificates can be used for a variety of electronic transactions including e-mail, electronic commerce, groupware and electronic funds transfers.
- If you are running an online e-commerce website, an electronic banking website or any other electronic services website then customers may abandon your website due to concerns about privacy and security.
- You will hence need to provide secure access to your website visitors via **https** protocol.
- To do this you will need to setup your website on a dedicated IP address and install a valid digital certificate on your hosting server.

What does it do?

- Digital Certificates, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information.
- A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys to impersonate other users.
- Used in conjunction with encryption, Digital Certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction.
- A digital certificate also is known as public key certificate allows exchanging data securely over the internet using public key infrastructure

Sample Digital Certificate



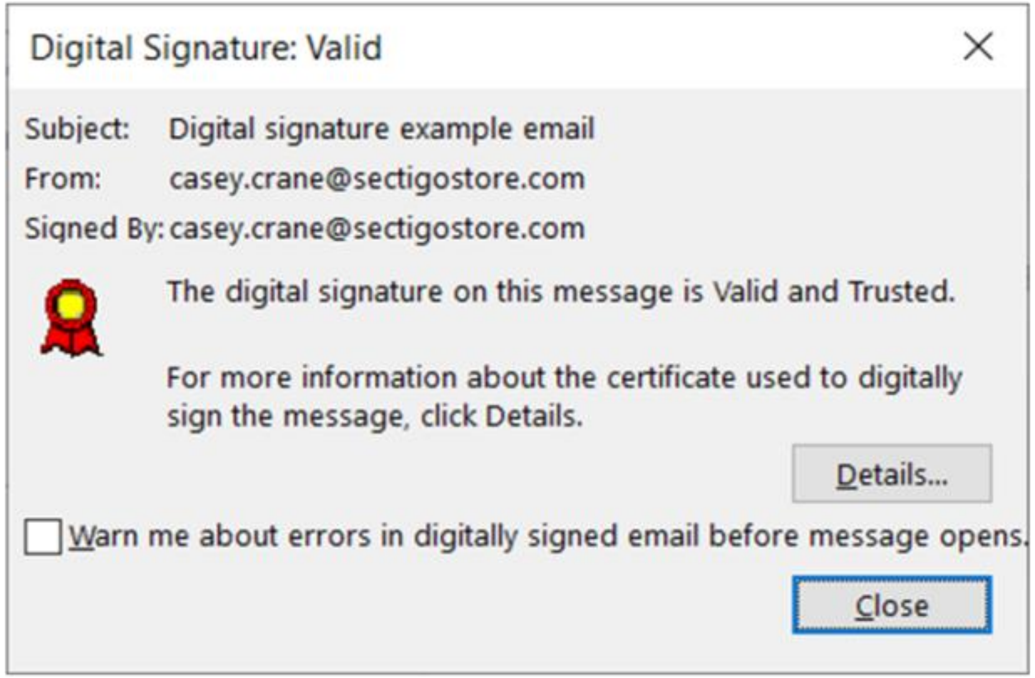
Digital signature example email

casey.crane@sectigostore.com

To casey.crane@sectigostore.com

Signed By casey.crane@sectigostore.com

1:40 PM



Digital Signature: Valid

Subject: Digital signature example email

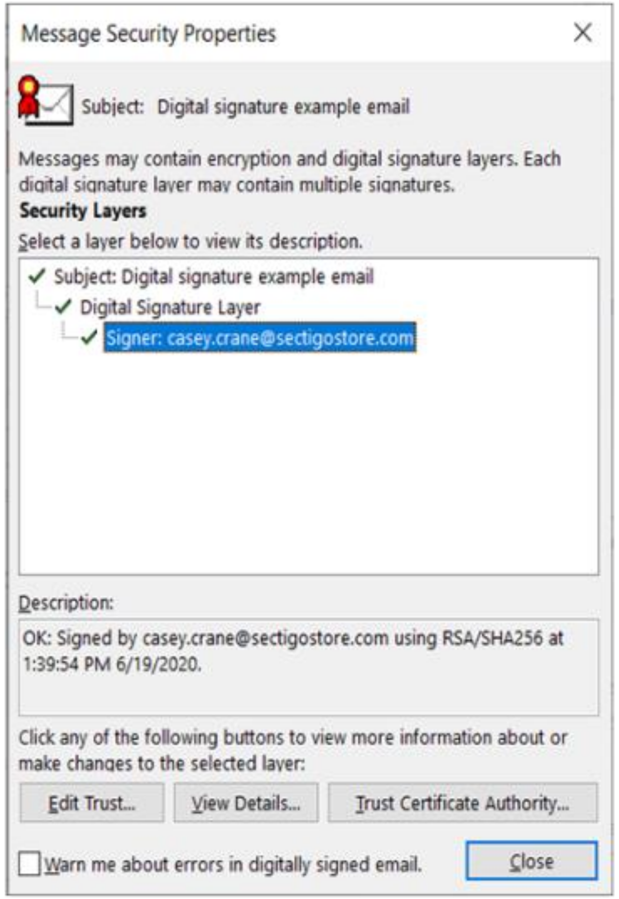
From: casey.crane@sectigostore.com

Signed By: casey.crane@sectigostore.com

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

□ Warn me about errors in digitally signed email before message opens.



Message Security Properties

Subject: Digital signature example email

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

- ✓ Subject: Digital signature example email
  - ✓ Digital Signature Layer
    - ✓ Signer: casey.crane@sectigostore.com

Description:

OK: Signed by casey.crane@sectigostore.com using RSA/SHA256 at 1:39:54 PM 6/19/2020.

Click any of the following buttons to view more information about or make changes to the selected layer:

□ Warn me about errors in digitally signed email.

Types of Digital Certificates

- There are 4 main types of Digital Certificates

1. Server Certificates or /TLS/SSL Certificate
2. Personal Certificates
3. Organizational Certificates or Client Certificate
4. Developer’s Certificates or Code Signing Certificate

Types of Digital Certificates

- Server Certificates
  - Allows visitors to exchange personal information such as credit card numbers, free from the threat of interception or tampering.
  - Server Certificates are a must for building and designing e-commerce sites as confidential information is shared between clients, customers and vendors.
  - TLS/SSL (Transport Layer Security/Secure Socket Layer) Certificates are installed on the server. The purpose of these certificates is to ensure that all communication between the client and the server is private and encrypted.
  - The server could be a web server, app server, mail server, LDAP server, or any other type of server that requires authentication to send or receive encrypted information. The address of a website with a TLS/SSL certificate will start with “https://” instead of “http://”, where the “s” stands for “secure.”

Types of Digital Certificates

- Personal Certificates
  - Personal Certificates allow one to authenticate a visitor’s identity and restrict access to specified content to particular visitors.
  - Personal Certificates are perfect for business to business communications such as offering suppliers and partners controlled access to special web sites for updating product availability, shipping dates and inventory management.

Types of Digital Certificates

- Organization Certificates
  - are used by corporate entities to identify employees for secure e-mail and web-based transaction.
  - Client Certificates or Digital IDs are used to identify one user to another, a user to a machine, or a machine to another machine.
  - One common example is emails, where the sender digitally signs the communication, and the recipient verifies the signature.
  - Client certificates authenticate the sender and the recipient.
  - Client certificates also take the form of two-factor authentication when the user needs to access a protected database or arrives at the gateway to a payment portal, where they’ll be expected to enter their passwords and be subjected to further verification.

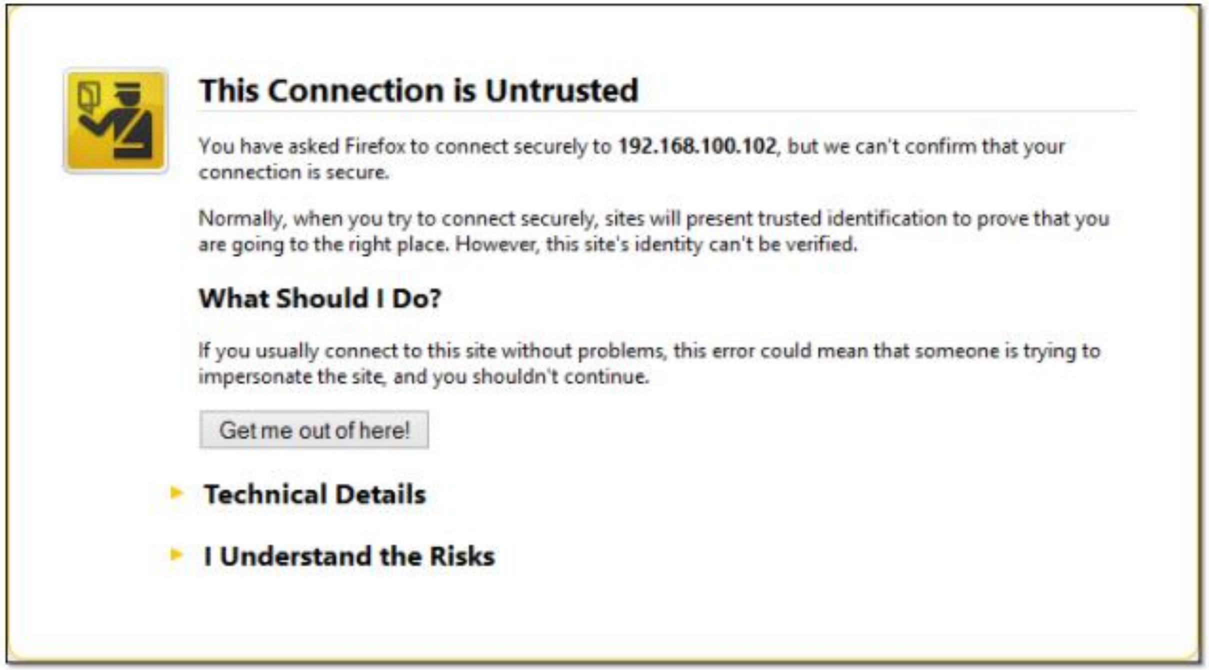
Types of Digital Certificates

- Developer Certificates
  - Prove authorship and retain integrity of distributed software programs e.g. installing a software on a computer system in most instances requires what is called a “serial key”
  - Used to sign software or files that are downloaded over the internet. They’re signed by the developer/publisher of the software.
  - Their purpose is to guarantee that the software or file is genuine and comes from the publisher it claims to belong. They’re especially useful for publishers who distribute their software for download through third-party sites. Code signing certificates also act as a proof that the file hasn’t been tampered with since download.

Signed vs Self-signed certificates

- In theory, certificate authorities are supposed to exercise due diligence before signing digital certificates submitted to them through Certificate Signing Request or CSRs.
- They need to verify first whether the information placed on the digital certificates are in fact true. This is important because their attestation would later on serve as the sole basis that certain websites who are able to present certs signed by them can really be trusted.
- It would be safe to assume that signed certificates are more reliable and trustworthy than self-signed certificates. In fact, when a user attempts to connect to your site and your site only has a self-signed certificate, the user's browser will display something like this:

Signed vs Self-signed certificates



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.100.102**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

- Self-signed certificates are relatively safe to use internally, i.e., within your organization, where you have more control over the servers that operate in the network.
- So, for instance, you can use it to add security to a web file transfer that takes place behind your corporate firewall.

Implementing SSL in Website

What is an SSL?

- SSL stands for **Secure Sockets Layer**, a now-deprecated cryptographic protocol that has kept only its name in common use. All SSL certificates are technically TLS certificates, TLS being the successor of the SSL technology.
- TLS or **Transport Layer Security** is a more advanced and secure protocol, that’s been now the standard encryption technology for more than a decade.

What is an SSL Certificate

- **SSL Certificate** is a digitally signed Certificate which is built of complex hashing functions and algorithm that keeps user's information encrypted during the data transmission form Client to Server and server to client.
- So, here both term SSL Certificate and Digital Certificate comes up different meaning and definition.

What is an SSL Certificate

- Also known as **SSL Certificate** is a digitally signed certification by an established authority to confirm the identity of your website/business and uses encryption to send/receive data between your website and its visitors.
- SSL certificate authenticates the connection between web server and browsers by encrypting communication between the website and its users.
- It is issued for a domain by a trusted authority referred as Certificate Authority (CA). Example CAs are Comodo and Thawte.

What does it do?

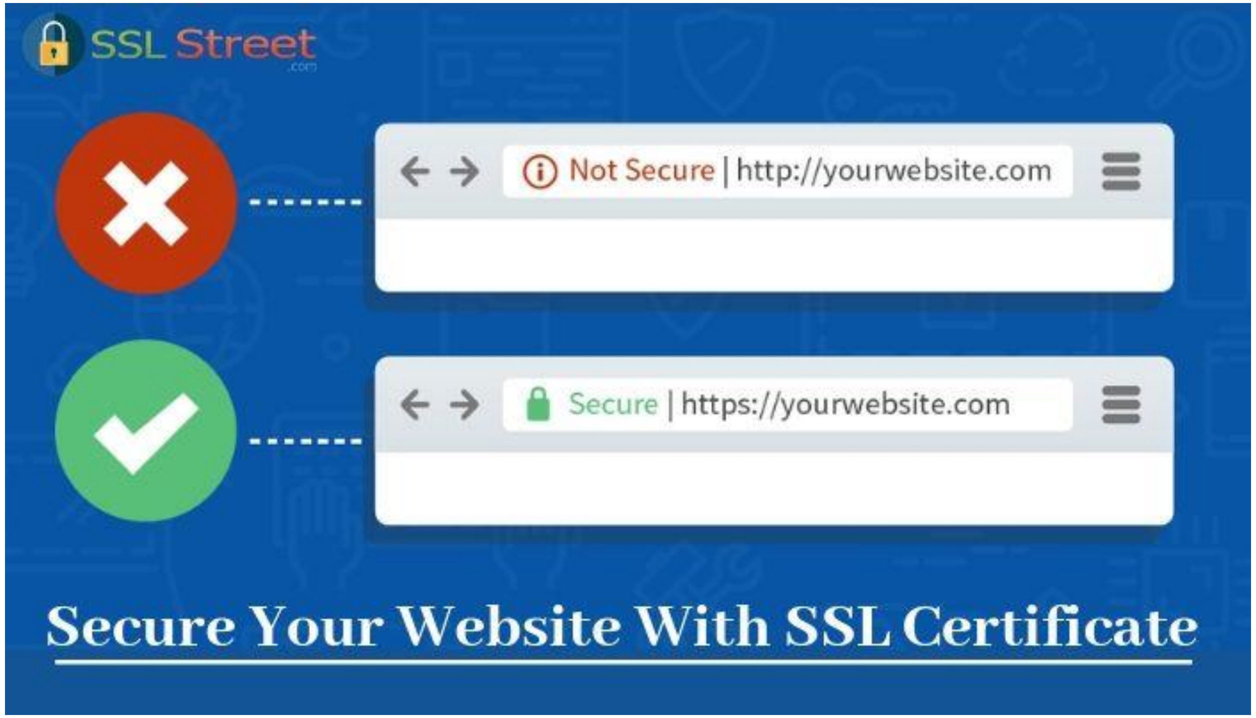
- An SSL certificate allows you to establish your credentials when doing business or other transactions on the Web.
- It is generally used when a website wants to accept sensitive information like passwords, credit card details and other sensitive information.
- The SSL Certificate protects your customer's personal data including passwords, credit cards and identity information. Thus, getting an SSL certificate for your website is the easiest way to increase your customer's confidence in your online business.

When do you require an SSL/Digital Certificate?

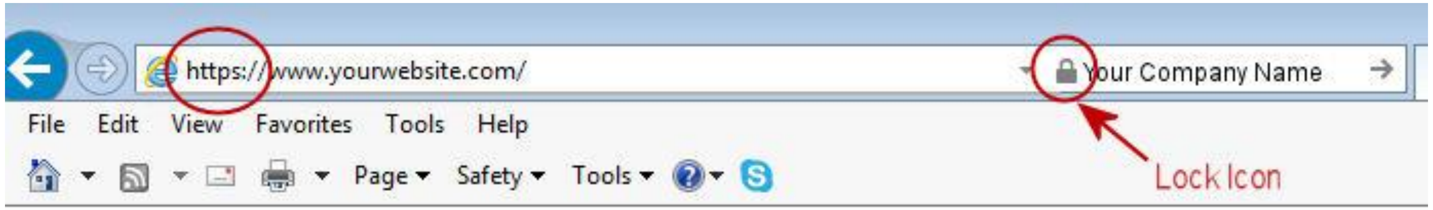
- An SSL Certificate does 2 things:
  a. Encrypt the information sent from your website visitor's browser to your website
  b. Authenticate your website's identity.
- By doing these 2 things, an SSL Certificate protects your customers and in turn increases their trust in your online business.
- This is especially important if your website requires users to login using passwords or enter sensitive information such as credit card details.
- Many customers actively look for the SSL lock icon before handing over sensitive data.

How do you know you have a digital certificate?

- If you come across a website whose URL begins with **https://**, you can view the website's SSL Certificate by clicking on the lock icon in the address bar of your browser.


SSL Street
.com
Not Secure | http://yourwebsite.com
Secure | https://yourwebsite.com

Secure Your Website With SSL Certificate


https://www.yourwebsite.com/

Your Company Name

Lock Icon

Types of SSL Certificates

- Certifying authorities provide SSL certificates in a few variety of branded names, each serving a specific purpose.
- For example, Comodo sells a basic SSL certificate in the name of *Positive SSL* while Thawte sells an equivalent certificate named as *SSL123 Certificate*.
- Likewise, a wildcard SSL certificate is named as *Positive SSL Wildcard* by Comodo and *Wildcard Server Certificate* by Thawte.

Types of SSL Certificates

- Broadly there are two types of SSL certificates:

1. **Basic SSL certificate:** allows you to secure one sub-domain. For example, if your e-commerce website is store.yourwebsitename.com, a basic SSL will secure only this sub domain and hence people will be able to access your website as https://store.yourwebsitename.com. If you want to also secure www.yourwebsitename.com, you may need to purchase a second separate certificate for this second sub-domain. A basic SSL certificate is quite well suited for small websites and blogs.
2. **Wildcard SSL certificate:** allows you to secure your primary domain name as well as all its sub-domains. Thus one certificate will secure both www.yourwebsitename.com and store.yourwebsitename.com, and any other sub domains such as support.yourwebsitename.com, webmail.yourwebsitename.com, etc. A Wildcard SSL is best suited for large e-commerce websites.

How to get an SSL Certificate for your website?

- To be issued an SSL Certificate, you need to purchase one from a web service provider and then go through a process that entails the following:
- **Step 1: Purchasing SSL**
  - As a first step you place an order for an ssl certificate with the web service provider. While placing order, you will need to specify the exact domain name for which you require the ssl certificate.
  - For example, if you need to secure *store.yourwebsitename.com*, you should specify *store.yourwebsitename.com* while placing order and not *www.yourwebsitename.com*.
  - Once your order has been executed by the service provider, you will be provided with a control panel from where you can apply for your certificate.

How to get an SSL Certificate for your website?

- **Step 2: Private Key and CSR Generation**
  - Prior to applying/enrolling for a Certificate with the CA, you must generate a minimum of 2048-bit Private Key and CSR pair from your hosting server.
  - Digital IDs make use of a technology called *Public Key Cryptography*, which uses Public and Private Key files.
  - The *Public Key*, also known as a *Certificate Signature Request (CSR)*, is the key that will be sent to the CA.
  - The Public Key is generated on your server and validates the computer-specific information about your web server and Organization when you request a Certificate from a CA.

How to get an SSL Certificate for your website?

- **Step 2: Private Key and CSR Generation**
  - The *Private Key* will remain on your hosting server and should never be released into the public. Even the Certifying Authority will *not* have access to your Private Key.
  - It is generated locally on your server and is *never* transmitted to the CA or any browser visiting your website. The integrity of your Digital ID depends on your Private Key being controlled exclusively by you.
  - A CSR *cannot* be generated without generating a Private Key file. Similarly the Private Key file *cannot* be generated without generating a CSR file.
  - In certain web server software platforms like Microsoft IIS, both are generated simultaneously through the Wizard on the web server.

How to get an SSL Certificate for your website?

- ## Step 2: Private Key and CSR Generation
  - Most hosting service providers provide you with a hosting management control panel which has an *SSL/TLS Manager* interface using which you can generate your CSR - private key pair.
  - You will be required to enter certain relevant details about your organization while generating the CSR.
  - On completion of this process, your hosting server will generate an encoded file, viz. your CSR. This CSR can now be used to submit your SSL Certificate application to the Certificate Authority.

How to get an SSL Certificate for your website?

- **Step 3: Enrollment**
  - After you have generated a minimum of 2048-bit Private Key and CSR pair from your web hosting server, the next step is to submit your Enrollment information to the CA for the CA to verify your information and issue the Digital certificate to you.
  - The enrollment is done from the interface that the web service provider will provide to you after you have purchased the SSL certificate.

How to get an SSL Certificate for your website?

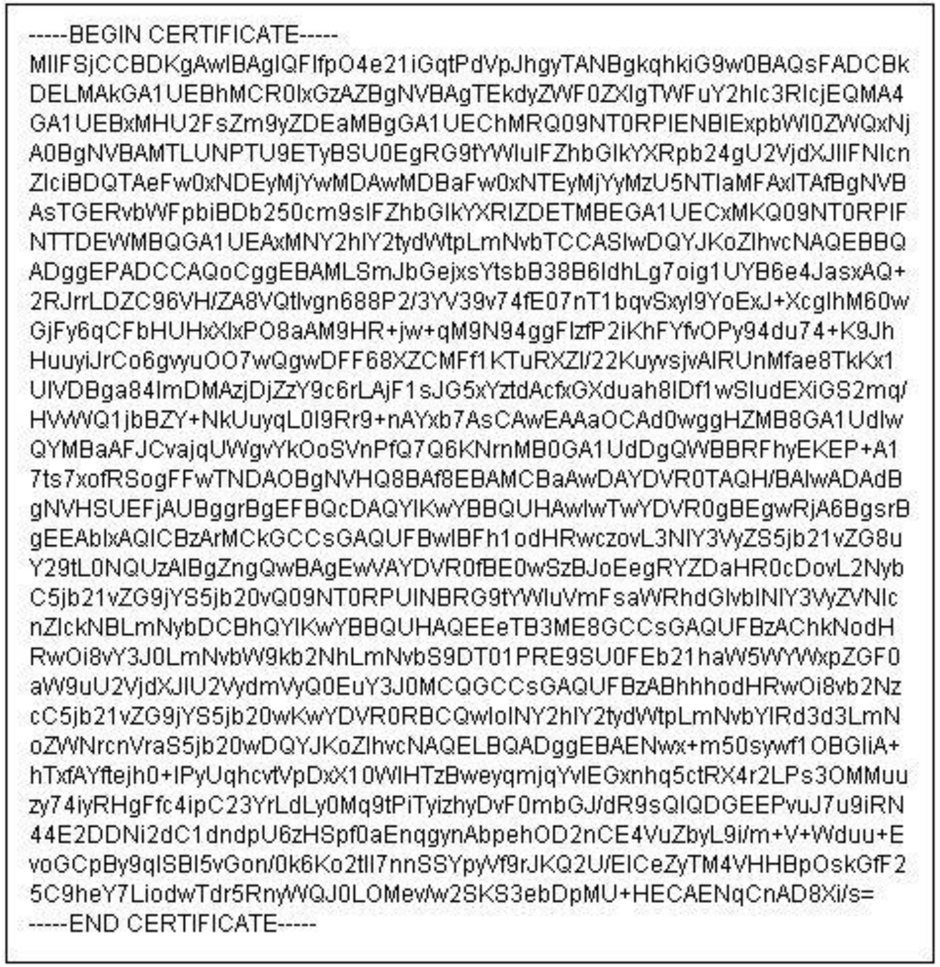
- **Step 3: Enrollment**
  - Enrollment essentially requires you to submit a form wherein you provide relevant details about your organization such as Organization name, Contact details, Admin email address, Approver Email Address, etc.
  - The contact details that you provide here must match with the ones available in your domain's whois lookup.
  - Also, you must ensure that prior to enrollment, your domain is not privacy protected and that it's whois information is publicly visible.
  - Subsequently, after the certificate is issued to you, you may re-enable your domain's privacy protection.

How to get an SSL Certificate for your website?

- ## Step 4: Verification Process & Certificate Issue
  - After you have submitted the enrollment form, the Certifying Authority will now carry out a verification of your organization and the information you have submitted. If required, they may call you at your specified phone number for additional verification of your business.
  - This process is much faster and usually automatic when you apply for a basic ssl certificate. Subsequently, after the CA is satisfied with the verification, you will receive an email from the CA to approve the issue of ssl certificate.
  - After you have done the approval, you will receive an email from the CA informing you that your certificate has been issued. The email will also contain information on how you can retrieve the issued certificate.

How to get an SSL Certificate for your website?

- Image shows how your issued ssl certificate will look:



```
-----BEGIN CERTIFICATE-----
MIIFSjCCBDKgAwIBAgIQFIfpO4e21iGqtPdVpJhgyTANBgkqhkiG9w0BAQsFADCBk
DELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4
GA1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxNj
A0BgNVBAMTLUNPTU9ETyBSU0EgRG9tYWluIFZhbGlkYXRpb24gU2VjdXJlIFNlcn
ZlciBDQTAeFw0xNDEyMjYwMDAwMDBaFw0xNTEyMjYyMzU5NTlaMFAxITAfBgNVB
AsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDETMBEGA1UECxMKQ09NT0RPIF
NTTDEWMBQGA1UEAxMNY2hlY2tydWtpLmNvbTCCASIwDQYJKoZIhvcNAQEBBQ
ADggEPADCCAQoCggEBAMLSmJbGejxsYtsbB38B6ldhLg7oig1UYB6e4JasxAQ+
2RJrrLDZC96VH/ZA8VQtlvgn688P2/3YV39v74fE07nT1bqvSxyl9YoExJ+XcgIhM60w
GjFy6qCFbHUHxXlxPO8aAM9HR+jw+qM9N94ggFlzfP2iKhFYfvOPy94du74+K9Jh
HuuyiJrCo6gvyuOO7wQgwDFF68XZCMFf1KTuRXZl/22KuyvsjvAIRUnMfae8TkKx1
UlVDBga84ImDMAzjDjZzY9c6rLAjF1sJG5xYztdAcfxGXduah8IDf1wSludEXiGS2mq/
HWWQ1jbBZY+NkUuyqL0I9Rr9+nAYxb7AsCAwEAAaOCAd0wggHZMB8GA1UdIw
QYMBaAFJCvajqUWgvYkOoSVnPfQ7Q6KNrnMB0GA1UdDgQWBBRFhyEKEP+A1
7ts7xofRSogFFwTNDAOBgNVHQ8BAf8EBAMCBaAwDAYDVR0TAQH/BAIwADAdB
gNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwTwYDVR0gBEgwRjA6BgsrB
gEEAbIxAQICBzArMCkGCCsGAQUFBwIBFh1odHRwczovL3NlY3VyZS5jb21vZG8u
Y29tL0NQUzAIBgZngQwBAgEwWAYDVR0fBE0wSzBJoEegRYZDaHR0cDovL2Nyb
C5jb21vZG9jYS5jb20vQ09NT0RPUlNBRG9tYWluVmFsaWRhdGlvblNlY3VyZVNlc
nZlckNBLmNybDCBhQYIKwYBBQUHAQEEeTB3ME8GCCsGAQUFBzAChkNodH
RwOi8vY3J0LmNvbW9kb2NhLmNvbS9DT01PRE9SU0FEb21haW5WYWxpZGF0
aW9uU2VjdXJlU2VydmVyQ0EuY3J0MCQGCCsGAQUFBzABhhhodHRwOi8vb2Nz
cC5jb21vZG9jYS5jb20wKwYDVR0RBCQwIoINY2hlY2tydWtpLmNvbYIRd3d3LmN
oZWNrcnVraS5jb20wDQYJKoZIhvcNAQELBQADggEBAENwx+m50sywf1OBGIiA+
hTxfAYftejh0+IPyUqhcvtVpDxX10WIHTzBweyqmjqYvlEGxnhq5ctRX4r2LPs3OMMuu
zy74iyRHgFfc4ipC23YrLdLy0Mq9tPiTyizhyDvF0mbGJ/dR9sQIQDGEEPvuJ7u9iRN
44E2DDNi2dC1dndpU6zHSpf0aEnqgynAbpehOD2nCE4VuZbyL9i/m+V+Wduu+E
voGCpBy9qISBI5vGon/0k6Ko2tIl7nnSSYpyVf9rJKQ2U/EICeZyTM4VHHBpOskGfF2
5C9heY7LiodwTdr5RnyWQJ0LOMev/w2SKS3ebDpMU+HECAENqCnAD8Xi/s=
-----END CERTIFICATE-----
```

How to get an SSL Certificate for your website?

- **Step 5: Certificate Installation**
- This is the final step wherein you need to install the issued certificate on your hosting server.
- Additionally, you will also need to install the SSL Certificate of the Certificate Authority (known as the CA bundle).
- The CA bundle contains root and intermediate certificates of the CA and is available for download from the website of the CA.
- Depending upon the web server where you intend to install your SSL Certificate, you need to refer to the appropriate instructions provided by your hosting service provider.
- Once successfully installed, your website will become accessible via **https://....**

Difference between Digital Certificate and SSL Certificate

- **Digital Certificate:**
  - A Digital Certificate is a digital "password" which permits an individual, organization to exchange information securely across the Web utilizing the public key infrastructure (PKI).
  - Digital Certificate can be referred to as a public key certification or identity certification.

- **SSL Certificate:**
  - SSL Certificates are small data files which bind a cryptographic key to a company's particulars. Once installed on an internet server, then it activates the padlock along with the https protocol also enables safe connections from a web server to a browser.
  - Normally, SSL is used to secure credit card transactions, information transport and logins, and much more lately has become the standard when procuring browsing of social networking websites.