# What Is an X.509 Certificate?

**X.509** is a standard format for **public key certificates**, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

First introduced in 1988 alongside the X.500 standards for electronic directory services, X.509 has been adapted for internet use by the IETF’s Public-Key Infrastructure (X.509) (PKIX) working group. [RFC 5280](https://tools.ietf.org/html/rfc5280) profiles the X.509 v3 certificate, the X.509 v2 certificate revocation list (CRL), and describes an algorithm for X.509 certificate path validation.

Common applications of X.509 certificates include:

* [SSL/TLS](https://www.ssl.com/faqs/faq-what-is-ssl/) and [HTTPS](https://www.ssl.com/faqs/what-is-https/) for authenticated and encrypted web browsing
* Signed and encrypted email via the [S/MIME](https://www.ssl.com/article/sending-secure-email-with-s-mime/) protocol
* [Code signing](https://www.ssl.com/faqs/what-is-code-signing/)
* [Document signing](https://www.ssl.com/s-mime-client-and-document-signing-certificates/)
* [Client authentication](https://www.ssl.com/s-mime-client-and-document-signing-certificates/)
* [Government-issued electronic ID](https://www.ssl.com/article/pki-and-digital-certificates-for-government/)

## **1. Key Pairs and Signature**

No matter its intended application(s), each X.509 certificate includes a **public key**, **digital signature**, and information about both the identity associated with the certificate and its issuing **certificate authority (CA)**:

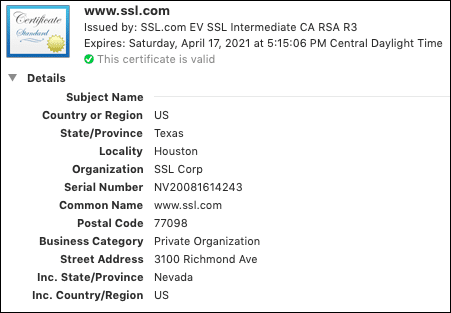
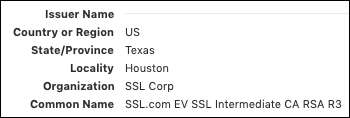
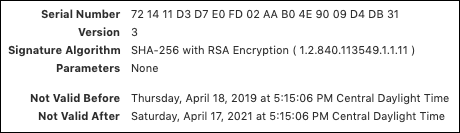
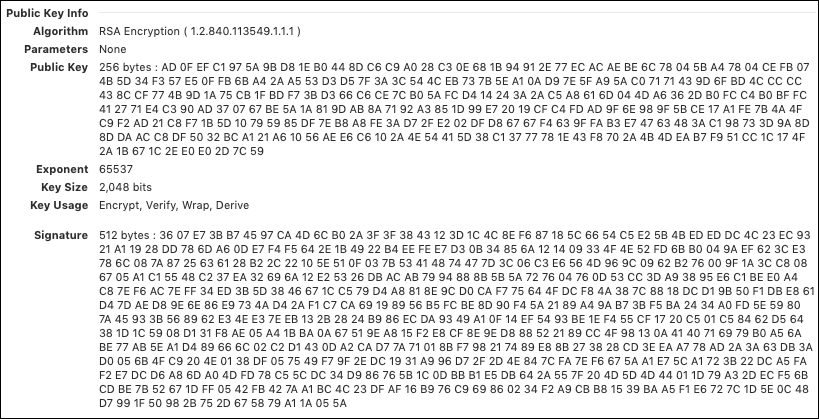
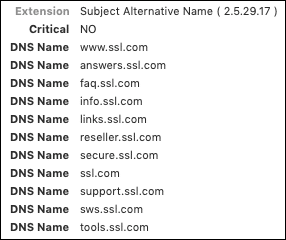
* The **public key** is part of a **key pair** that also includes a **private key**. The private key is kept secure, and the public key is included in the certificate. This public/private key pair:
  + Allows the owner of the private key to digitally sign documents; these signatures can be verified by anyone with the corresponding public key.
  + Allows third parties to send messages encrypted with the public key that only the owner of the private key can decrypt.
* A **digital signature** is an encoded hash (fixed-length digest) of a document that has been encrypted with a private key. When an X.509 certificate is signed by a **publicly trusted CA**, such as SSL.com, the certificate can be used by a third party to verify the identity of the entity presenting it.

**Note:** Not all applications of X.509 certificates require public trust. For example, a company can issue its own privately-trusted certificates for internal use. For more information, please read our article on [Private vs. Public PKI](https://www.ssl.com/article/private-vs-public-pki-building-an-effective-plan/).

* Each X.509 certificate includes fields specifying the **subject**, **issuing CA**, and other required information such as the certificate’s **version**and **validity period**. In addition, v3 certificates contain a set of **extensions** that define properties such as acceptable key usages and additional identities to bind a key pair to.

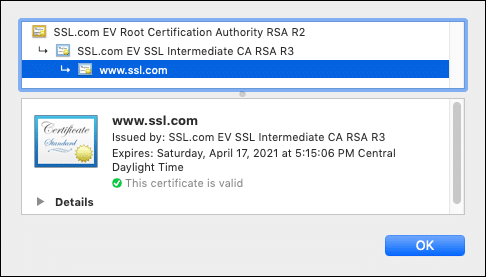
## **2. Certificate Fields and Extensions**

To review the contents of a typical X.509 certificate in the wild, we will examine www.ssl.com’s SSL/TLS certificate, as shown in Google Chrome. (You can check all of this in your own browser for any HTTPS website by clicking the lock on the left side of the address bar.)

* [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-01.png?x71269)The first group of details includes information about the **Subject**, including the name and address of the company and the **Common Name** (or Fully Qualified Domain Name) of the website that the certificate is intended to protect. (**Note:** the **Serial Number** shown in this subject field is a Nevada business identification number, not the serial number of the certificate itself.)
* [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-02a.png?x71269)Scrolling down, we encounter information about the **Issuer**. Not coincidentally, in this case, the **Organization** is “SSL Corp” for both subject and issuer, but the issuer’s **Common Name** is the name of the issuing CA certificate rather than a URL.
* Below the Issuer, we see the certificate’s **Serial Number** (a positive integer uniquely identifying the certificate), **X.509 Version** (3), the **Signature Algorithm**, and dates specifying the certificate’s **Validity Period**.  
  [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-02b.png?x71269)
* [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-04.png?x71269)Next, we arrive at the **Public Key**, **Signature**, and associated information.
* [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-05b.png?x71269)In addition to the fields above, X.509 v3 certificates include a group of **Extensions** that offer additional flexibility in certificate use. For example, the **Subject Alternative Name** extension allows the certificate to be bound to multiple identities. (For this reason, multiple-domain certificates are sometimes referred to as [**SAN certificates**](https://www.ssl.com/faqs/what-is-a-san-certificate/)). In the example below, we can see that the certificate actually covers eleven different SSL.com subdomains:
* [](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-06.png?x71269)The **Fingerprints** shown below the certificate information in Chrome are not part of the certificate itself, but are independently-calculated hashes that can be used to uniquely identify a certificate.

## **3. Certificate Chains**

For both administrative and security-related reasons, X.509 certificates are typically combined into **chains** for validation. As shown in the screenshot from Google Chrome below, the SSL/TLS certificate for www.ssl.com is signed by one of SSL.com’s intermediate certificates, SSL.com EV SSL Intermediate CA RSA R3. In turn, the intermediate certificate is signed by SSL.com’s EV RSA root:

[](https://cdn.ssl.com/app/uploads/2019/09/faq-x.509-07.png?x71269)

For publicly trusted websites, the web server will provide its own **end-entity** certificate, plus any intermediates required for validation. The root CA certificate with its public key will be included in the end user’s operating system and/or browser application, resulting in a complete [**chain of trust**](https://www.ssl.com/faqs/what-is-a-chain-of-trust/).

## **4. Revocation**

X.509 certificates that must be invalidated before their **Not Valid After** date may be **revoked**. As mentioned above, [RFC 5280](https://tools.ietf.org/html/rfc5280) profiles certificate revocation lists (CRLs), time-stamped lists of revoked certificates that can be queried by browsers and other client software.

On the Web, CRLs have proven ineffective in practice and have been superseded by other solutions for revocation checking, including the OCSP protocol (published in [RFC 2560](https://tools.ietf.org/html/rfc2560)), OCSP Stapling (published in [RFC 6066, section 8](https://tools.ietf.org/html/rfc6066#section-8), as “Certificate Status Request”), and an assortment of vendor-specific solutions implemented in various web browsers. For more information on the thorny history of revocation checking and how current bowsers check the revocation status of certificates, please read our articles, [**Page Load Optimization: OCSP Stapling**](https://www.ssl.com/article/page-load-optimization-ocsp-stapling/), and [**How Do Browsers Handle Revoked SSL/TLS Certificates?**](https://www.ssl.com/article/how-do-browsers-handle-revoked-ssl-tls-certificates/)

**Introduction To SSL/TLS X.509 Certificates And Keys**

**Summary:**

**What is an SSL/TLS x.509 Certificate?**

An SSL Certificate is a **digital computer file** that has two specific functions:

1. **Authentication and Verification**: The SSL Certificate has information about the authenticity of details around the identity of a host or site. When you click on the padlock displayed or check the trust mark the certificate chain details prove where the certificate is generated from.
2. **Data Encryption**: The SSL Certificate enables encryption, which means that the sensitive information exchanged via the web site cannot be intercepted and read by anyone other than the intended recipient.

An SSL Certificate is most reliable when issued by a trusted Certificate Authority (CA). The CA has to follow very strict rules and policies about who may or may not receive an SSL Certificate. So, when you have a valid SSL Certificate from a trusted CA, there is a higher degree of trust.

**More Information:**

**How do I check a site for a valid secure connection?**

1. A standard web site without SSL security displays “HTTP” at the beginning of the web site address in the browser address bar. This stands for “Hypertext Transfer Protocol,” and is the conventional way to transmit information over the Internet. However, a web site that is secured with an SSL Certificate will have “HTTPS” before the address. This stands for “Hypertext Transfer Protocol Secure”.
2. You will also see a padlock symbol on the top or bottom of the Internet browser.
3. You may also notice a trust mark displayed on the web site. This will display details of the certificate with all of the company information as verified and authenticated by the CA.
4. By clicking the closed padlock in the browser window, or certain SSL trust marks, you can see the authenticated organization name. In high-security browsers, the authenticated organization name is prominently displayed and the address bar turns green when an Extended Validation (EV) SSL Certificate is detected. If the information does not match, or the certificate has expired, the browser displays an error message or warning.

**What Is an SSL/TLS X.509 Certificate?**

An SSL/TLS X.509 certificate is a digital file that's usable for Secure Sockets Layer (SSL) or Transport Layer Security (TLS). The certificate fulfills two functions. **First**, the certificate can assist with authenticating and verifying the identity of a host or site. **Second**, it enables the encryption of information exchanged via a website.

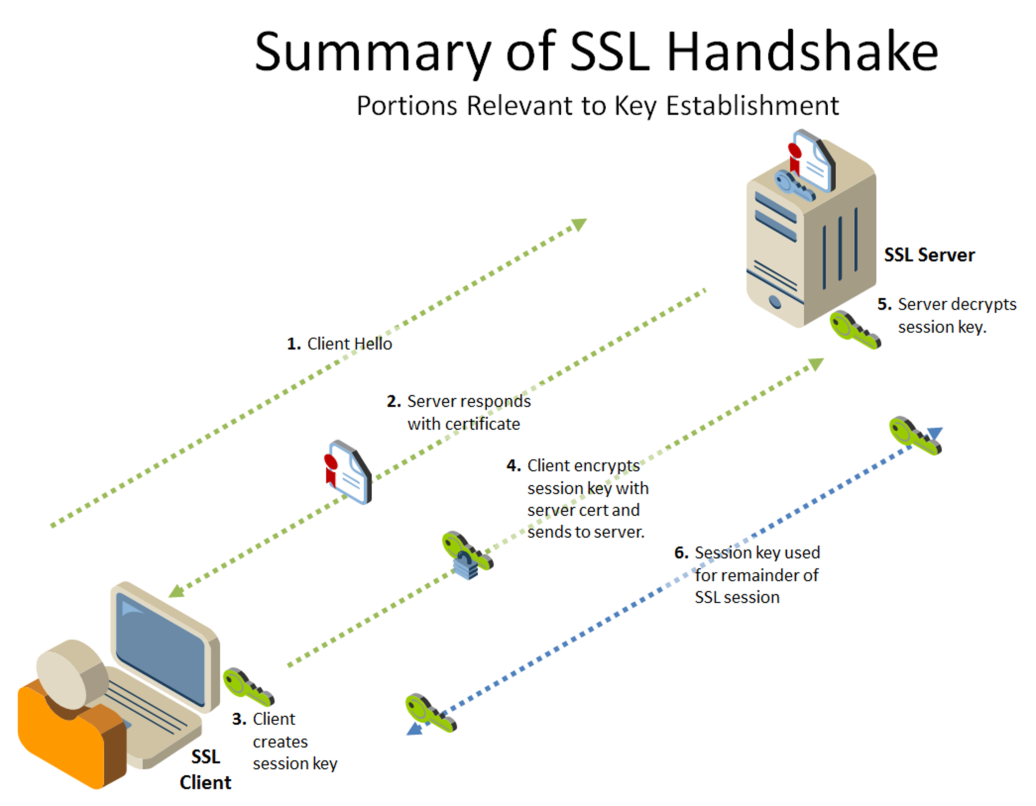
An SSL/TLS certificate is one of the most popular types of [X.509 certificates](https://www.ietf.org/rfc/rfc2459.txt), or a type of public key certificate which uses the X.509 standard. X.509 certificates contain a public key and the identity of a hostname, organization, or individual. Some of these certificates are self-signed. When a certificate authority (CA) signs them or another entity validates them, the owner of that certificate can leverage the public key to establish secure connections with another party or validate documents someone digitally signed using the corresponding private key.

SSL/TLS certificates are X.509 certificates with Extended Key Usage: Server Authentication (1.3.6.1.5.5.7.3.1). The "[Extended Key Usage](https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_8.0.1/com.ibm.help.domino.admin.doc/DOC/H_KEY_USAGE_EXTENSIONS_FOR_INTERNET_CERTIFICATES_1521_OVER.html)" extension lists the "roles" for the entity that uses the certificate. In other words, an entity must use SSL/TLS certificates only for server authentication and nothing else. Otherwise, that entity risks violating the issuing CA's policies.

There are also other common types of X.509 certificates, like Client Authentication (1.3.6.1.5.5.7.3.2) and Code Signing (1.3.6.1.5.5.7.3.3). These files form the basis of encryption and authentication schemes.

As SSL/TLS certificates enable encryption, they are integral to Hyper Text Transfer Protocol Secure (HTTPS), a protocol which encrypts all communication exchanged between a website and your browser.

1. HTTPS starts when a browser requests a secure page.
2. The web server responds with its public key and its certificate.
3. The browser then verifies a trusted authority or CA issued this digital file.
4. Assuming that's the case, the browser uses the web server's public key to encrypt a random symmetric encryption key and sends it to the server with an encrypted URL and other encrypted HTTP data.
5. If the public key is valid, the web server uses its private key to decrypt the symmetric encryption key, URL, and HTTP data before sending over the HTML document and HTTP data now encrypted with the symmetric key.
6. This symmetric key, in turn, allows the browser to decrypt the HTTP data and display it to the user.



You can check that a website you're visiting is using HTTPS by looking for "HTTPS" in the address bar. There should also be a padlock symbol next to the website's address. If you click on that symbol, your web browser should display the name of the organization that owns the SSL/TLS certificate. That symbol turns green when your web browser detects an Extended Validation (EV) SSL certificate.

If the certificate has expired, the web browser will display an error message or warning. These alerts could lead a visitor to navigate away from a website. To prevent this from happening, organizations that own websites and use HTTPS need to manage their certificates and make sure the ones they want to keep don't expire. [Are all your certificates up to-date?](https://www.venafi.com/solutions/encryption-and-authorization/outages)