



DEFINITION

certificate authority (CA)

By [Rahul Awati](#) | [Peter Loshin](#), Former Senior Technology Editor

What is a certificate authority (CA)?

A certificate authority (CA) is a trusted entity that issues [Secure Sockets Layer \(SSL\) certificates](#). These [digital certificates](#) are data files used to cryptographically link an entity with a [public key](#). Web browsers use them to authenticate content sent from web servers, ensuring trust in content delivered online.

As providers of these certificates, CAs are a reliable and critical trust anchor of the internet's public key infrastructure ([PKI](#)). They help secure the internet for both organizations and users.

The main goal of a CA is to verify the authenticity and trustworthiness of a website, domain and organization so users know exactly who they're communicating with online and whether that entity can be trusted with their data.

When a CA issues a digital certificate for a website, users know they are connected with an official website, not a fake or spoofed website created by a hacker to steal their information or money.

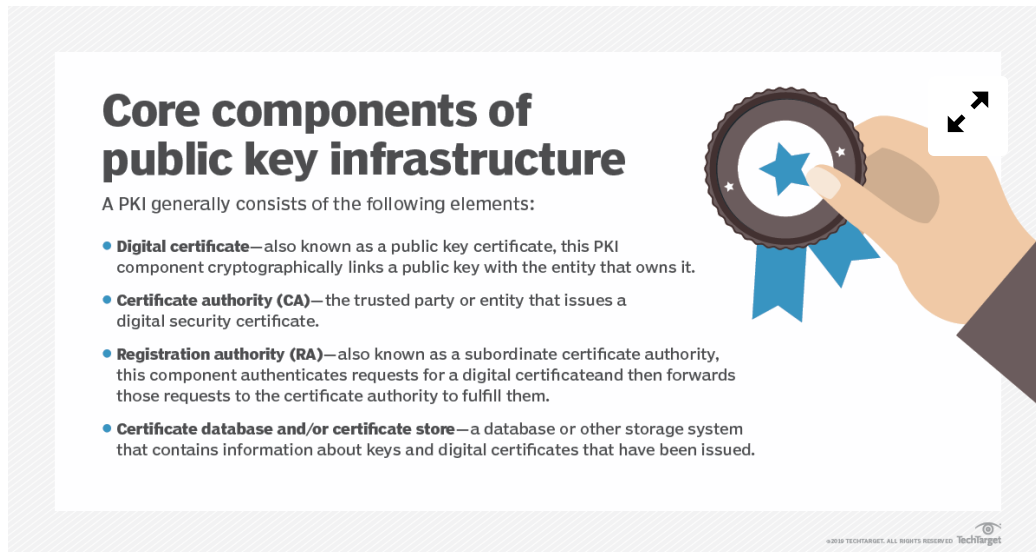
Key roles of a certificate authority

As an integral part of PKI, a CA plays multiple crucial roles:

- issues digital certificates;
- helps establish trust between communicating entities over the internet;

- verifies domain names and organizations to validate their identities; and
- maintains [certificate revocation lists](#).

Every CA charges a small fee to complete the verification process and issue a digital certificate following the process explained below.



The basic elements of a public key infrastructure

How a digital certificate works

A digital certificate primarily acts as a credential to validate the identity of the entity it is issued to. It also encrypts and secures communication over the internet and maintains the integrity of documents signed with it, ensuring third parties cannot alter the documents while they are in transit.

A digital certificate contains information about the entity to which it has been issued. Typically, that includes its name, contact information, organization, domain name, public key, certificate issue and expiry date, and more. The name of the issuing CA and its [digital signature](#) are also normally included in the digital certificate.

In the digital certificate, the digital signature proves that a trusted CA issued the certificate and it was not modified by any other party.

How SSL/TLS certificates work

The Transport Layer Security ([TLS](#)) protocol uses SSL certificates to encrypt and authenticate data streams for Hypertext Transfer Protocol Secure ([HTTPS](#)). The SSL cryptographic protocol facilitates secure encrypted connections over the internet via web browsers that connect to websites. SSL works on top of HTTP to create an HTTPS connection.

SSL certificates are sometimes called *SSL/TLS certificates* or simply *TLS certificates*. TLS is an upgraded version of SSL.

Similar to SSL, HTTP is layered on top of TLS to create HTTPS. It encrypts otherwise readable data to provide enhanced protection for applications and websites requiring higher privacy and security, such as those involving banking, taxation and e-commerce. TLS also provides privacy between the endpoints of a data transmission and boosts data integrity so hackers cannot intercept or compromise private data.

When a web browser initiates a secure connection over HTTPS, the SSL/TLS digital certificate is sent to the web browser. The browser checks the information in the certificate and authenticates it against its own root certificate store. This is how the certificate ensures secure, encrypted connections between a user's browser and the

organization's web server or a website's web server.

When this feature is working, users will not see warning messages in their browser, such as "not sure" or "your connection is not private." Those are displayed for insecure websites.

All major browsers, including those provided by Microsoft (Internet Explorer, Edge), Google (Chrome), Apple (Safari) and Mozilla ([Firefox](#)) all maintain their own web browser root certificate stores. This is where they post the root certificates of CAs the publishers have decided their browser will trust.

How a certificate authority issues a digital certificate

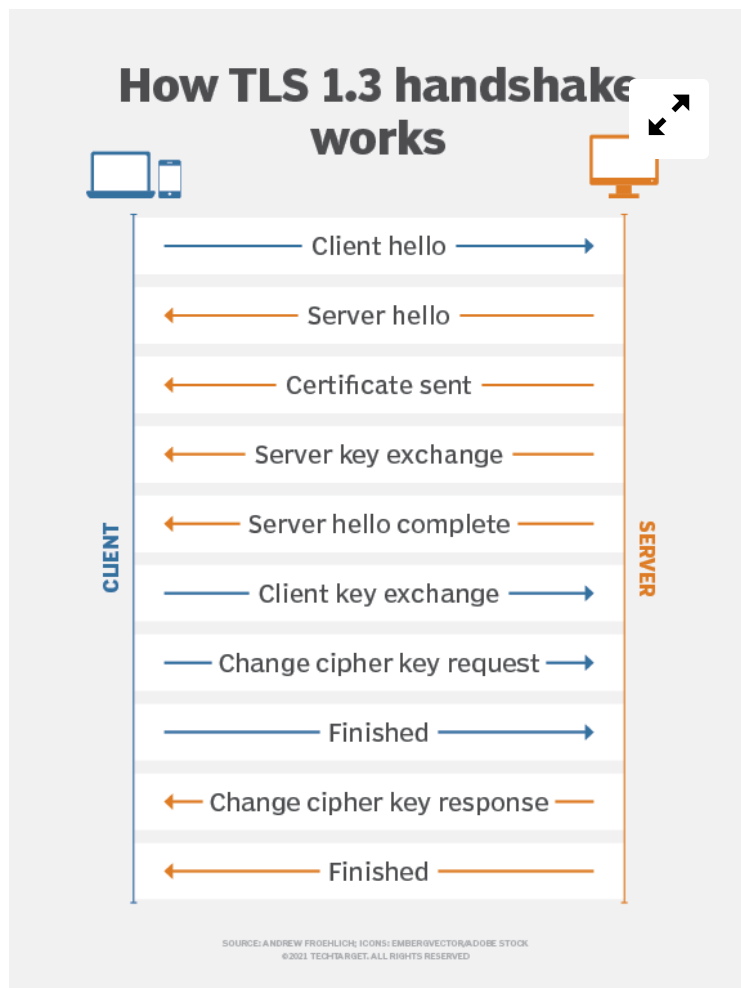
SSL/TLS certificates authenticate and secure websites and facilitate secure, encrypted connections. They let users know they are visiting a genuine website by displaying a padlock icon in the web browser.

As important components of PKI, SSL/TLS certificates require a digital certificate to work. This is where the CA comes in.

An entity -- organization or person -- can request a digital certificate from a CA. First, it generates a key pair, which consists of the following:

- private key, which is always kept a secret and should never be shown to anyone, including the CA; and
- public key, which is mentioned in the digital certificate the CA issues -- the applicant also generates a certificate signing request (CSR), an encoded text file that specifies the information that will be included in the certificate, such as the following:
 - domain name;
 - additional or alternative domain names, including subdomains;
 - organization; and
 - contact details, e.g., email address.

The information included in the CSR depends on the intended use of the certificate and its validation level. Both of the above processes are usually done on the server -- or workstation -- where the certificate is to be installed.



TLS ensures authenticity using a client-server handshake via an encrypted and secure connection.

The applicant then sends the CSR to the CA, which verifies the information in the CSR and the applicant's identity. Then, the CA generates a digital certificate, digitally signs it with its private key and sends the certificate to the applicant.

At this point, this digital certificate can be authenticated -- by a web browser, for example -- using the CA's public key. The browser can also use the certificate to confirm that the digitally signed content was sent by a legitimate entity that holds

the corresponding private key and that this information has not been altered since it was signed by that entity.

CAs often accept requests from applicants directly. Sometimes, they delegate the task of authenticating applicants to registration authorities ([RAs](#)). The RA collects and authenticates digital certificate requests and then submits those requests to the CA, which then issues the certificate to be passed through the RA to the applicant.

The RA may also be used for marketing and customer support. The CA is required

to limit the RA to registering certificates within the domain namespace assigned to the RA.

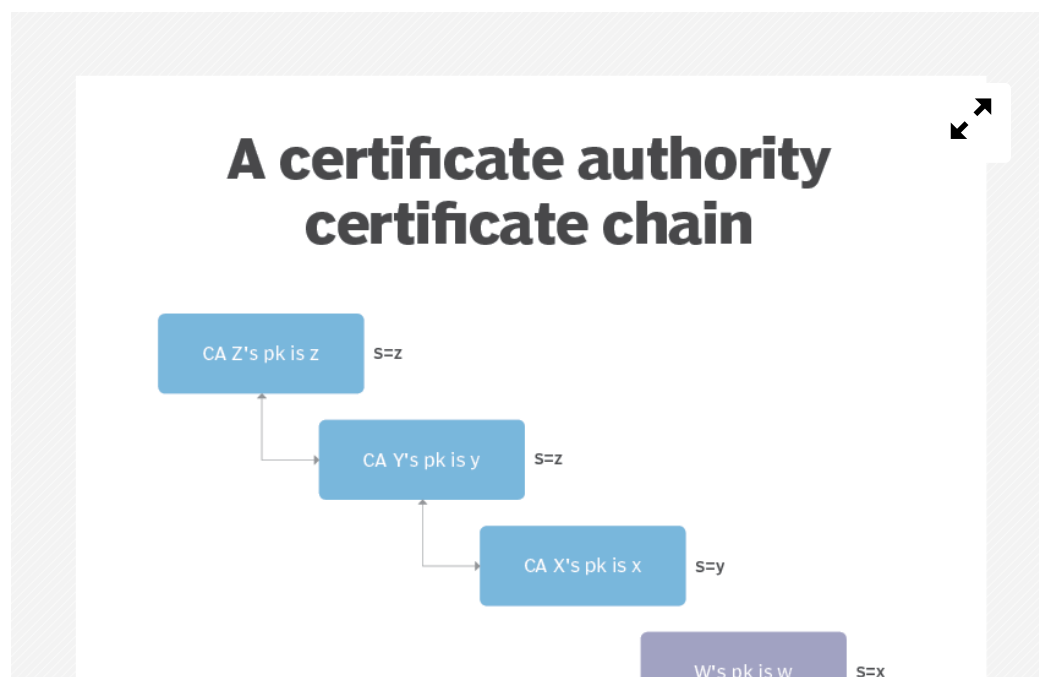
Root certificates and intermediate certificates

The CA plays a vital role in the chain of trust, a hierarchical trust model that consists of root certificates, intermediate certificates and SSL certificates. Its activities start with a root certificate, which is used as the ultimate basis for trust in all certificates the authority issues.

The root certificate -- along with the private key associated with that certificate -- is treated with the highest level of security and is usually stored offline in a protected facility. It may also be stored on a device that is unpowered except when the certificate is needed.

The CA will use that root certificate to create intermediate certificates, i.e., the certificates used to sign the digital certificates issued by the authority. The root certificate should never be used directly for signing digital certificates. Different intermediate certificates support different purposes.

This enables the public to trust the issued certificates, while also protecting the root when an intermediate certificate expires or is revoked. RAs may also issue digital certificates using intermediate certificates.



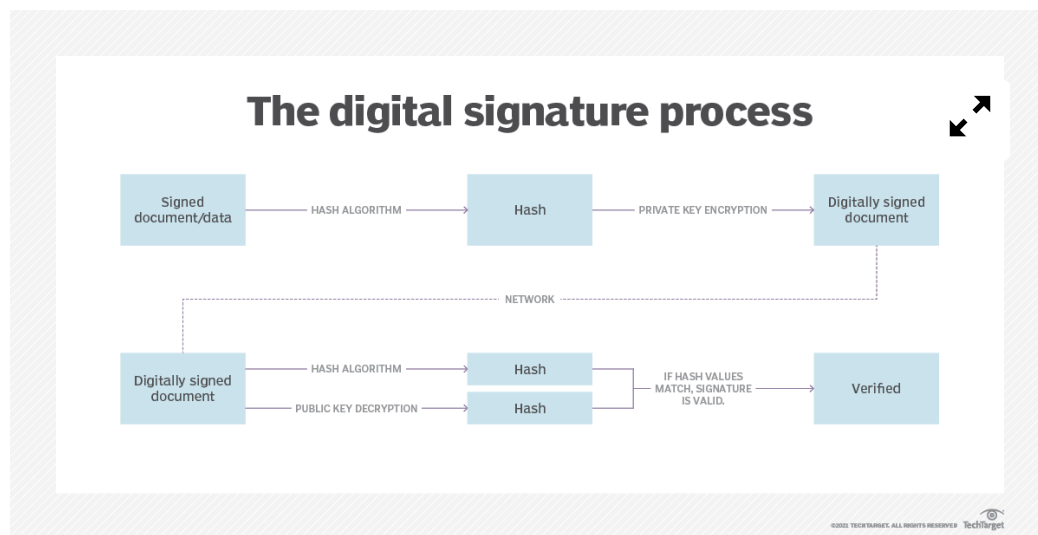


Certificates from a certificate authority usually form certificate chains. Rectangles represent certificates, while the note to the right of each specifies keys used to sign certificate at issue.

Types of digital certificates

CAs don't just issue SSL/TLS certificates. They can issue other types of certificates for different use cases, including the following:

- **Code signing certificates** are used by software publishers and developers to sign their software distributions. End users can then use them to authenticate and validate software downloads from the vendor or developer.
- **Email signing certificates** let entities sign, encrypt and authenticate email using the Secure/Multipurpose Internet Mail Extensions protocol for secure email attachments.
- **Object signing certificates** accommodate signing and authenticating any type of software object.
- **User/client signing certificates**, or signature verification certificates, help individuals handle a variety of authentication needs.



A digital signature is created with a private key that encrypts the signature while h:

is generated and encrypted simultaneously. Recipients use signers' public keys to the signatures.

What is the CA/Browser Forum?

The CA/Browser (CA/B) Forum [maintains guidelines](#) for all aspects of the creation, distribution and use of digital certificates, including policies for certificate expiration and revocation. Publicly trusted certificate authorities usually participate in this forum.

Most members are either CAs or web browser vendors. However, certificate consumer organizations also participate.

According to CA/B Forum rules, the CA must contractually require all RAs to comply and document their compliance with these rules. CAs are themselves also subject to extensive rules and operational audits.

Any infractions can prompt more audits and other consequences that could damage the CA's reputation and lower trust in its operations and reliability.

This was last updated in September 2021

➤ Continue Reading About certificate authority (CA)

- [PKI authentication explained: The basics for IT administrators](#)
- [How to get a digital certificate that works for your network](#)
- [Trusted? Certificate authority risks and how to manage them](#)
- [How to buy the best SSL for your enterprise](#)
- [How to detect fraudulent certificates that look real](#)

Related Terms

cryptography

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is... [See complete definition](#) ⓘ

identity provider

An identity provider (IdP) is a system component that provides an end user or internet-connected device with a single set of ... [See complete definition](#) ⓘ

phishing

Phishing is a fraudulent practice in which an attacker masquerades as a reputable entity or person in an email or other form of ... [See complete definition](#) ⓘ

➤ Dig Deeper on Identity and access management

Secure Sockets Layer certificate (SSL certificate)

By: Rahul Awati

3 types of PKI certificates and their use cases

By: Isabella Harford

X.509 certificate

By: Alexander Gillis

certificate revocation list (CRL)

By: Rahul Awati

Latest TechTarget
resources

NETWORKING



CIO

ENTERPRISE DESKTOP

CLOUD COMPUTING

COMPUTER WEEKLY

Networking



How cloud drives changes to network licensing

The cloud's effect on application management and licensing is expected to shift from end-user applications to SDN concepts. Say ...



How to avoid internet black holes for the network

Black holes in the network disrupt connectivity and compromise data integrity. Network monitoring, team collaboration and routing...

[About Us](#)

[Editorial Ethics Policy](#)

[Meet The Editors](#)

[Contact Us](#)

[Videos](#)

[Photo Stories](#)

[Definitions](#)

[Guides](#)

[Advertisers](#)

[Partner with Us](#)

[Media Kit](#)

[Corporate Site](#)

[Contributors](#)

[Reprints](#)

[Events](#)

[E-Products](#)

All Rights Reserved, [Copyright 2000 - 2024](#), TechTarget

[Privacy Policy](#)

[Do Not Sell or Share My Personal Information](#)