What is a Certificate Authority? What is CA?

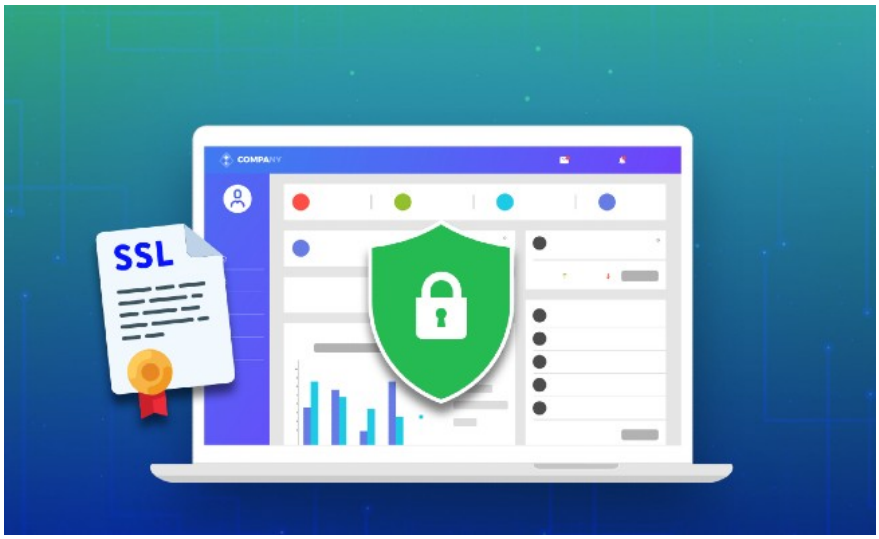
Certificate Authority, also known as CA, can be interpreted as a provider of digital certificates to verify the transparency of websites, servers, source code and software.

Certificate Authority or CA plays an important role in ensuring safety and transparency for the internet. So what is a Certificate Authority? Invite you to find out.

What is a Certificate Authority? What is CA?

The Certificate Authority (CA) is a trusted authority responsible for issuing digital certificates. CAs are an important part of the internet's PKI public key infrastructure because they provide Secure Sockets Layer (SSL) certificates to websites so that they authenticate content sent from the web server.

SSL is the standard of security technology, encrypted communication between Web server and browser. All major browsers use the web server's SSL certificates to authenticate the reliability of the content. Meanwhile, SSL combines with the Transport Layer Security protocol (TLS) to encrypt and authenticate data streams for the HTTPS protocol.



The most common role of CA is to issue SSL certificates
Digital certificates contain certified entity data, including the entity's public key, the certificate's expiry date, the entity name, contact information, etc., along with that, in the certificate. There is also cryptographic data used to verify the identity of the entity.

Web servers will transmit these certificates when the browser initiates a secure connection via HTTPS. Upon receipt, the browser will compare the web server's certificate with its root certificate. Big browser development companies like Google, Microsoft, Apple and Mozilla all have their own root certificate store.

An individual or business may, when necessary, request a CA digital certificate. After authenticating the identity of the applicant, the CA will issue them a digital certificate with a digital signature linking that certificate to the CA's private key. The digital certificate can then be verified by the public key of the CA.

The role of CA bodies

The most common role of CA is to issue SSL certificates to entities that want to publish content on the web. There are three levels of SSL certificates that CA agencies can issue, corresponding to different levels of trust. The higher the degree of trust, the more stringent the CA authority is in certification.

However, currently CA agencies have expanded their operations, granting more types of certificates at the request of the market
The three levels of SSL certificates include Extended Validation (EV), Organization Validated (OV) and Domain Validdated (DV). In particular, EV is the highest level certificate.

In addition to SSL, CA can also issue digital certificates for other purposes such as:

1. Code signature certificates are used by software developers and programmers to sign the software they distribute.
2. Email certificates allow entities to sign, encrypt and authenticate email using the S / MIME (Secure Multipurpose Internet Mail Extension) protocol to ensure secure access to attachments.
3. Device certificates are issued to IoT devices to enable the safe management and authentication of firmware or software updates.
4. Object certificates can be used to sign and authenticate any software object.
5. User or customer certificates, used by individuals for various authentication purposes and sometimes collectively referred to as digital signatures.

Recently, CA agencies are shifting their focus from issuing SSL certificates to web domains to providing a range of other certificate services. This is a general development trend, to ensure a safe internet environment as well as increase revenue for CA.