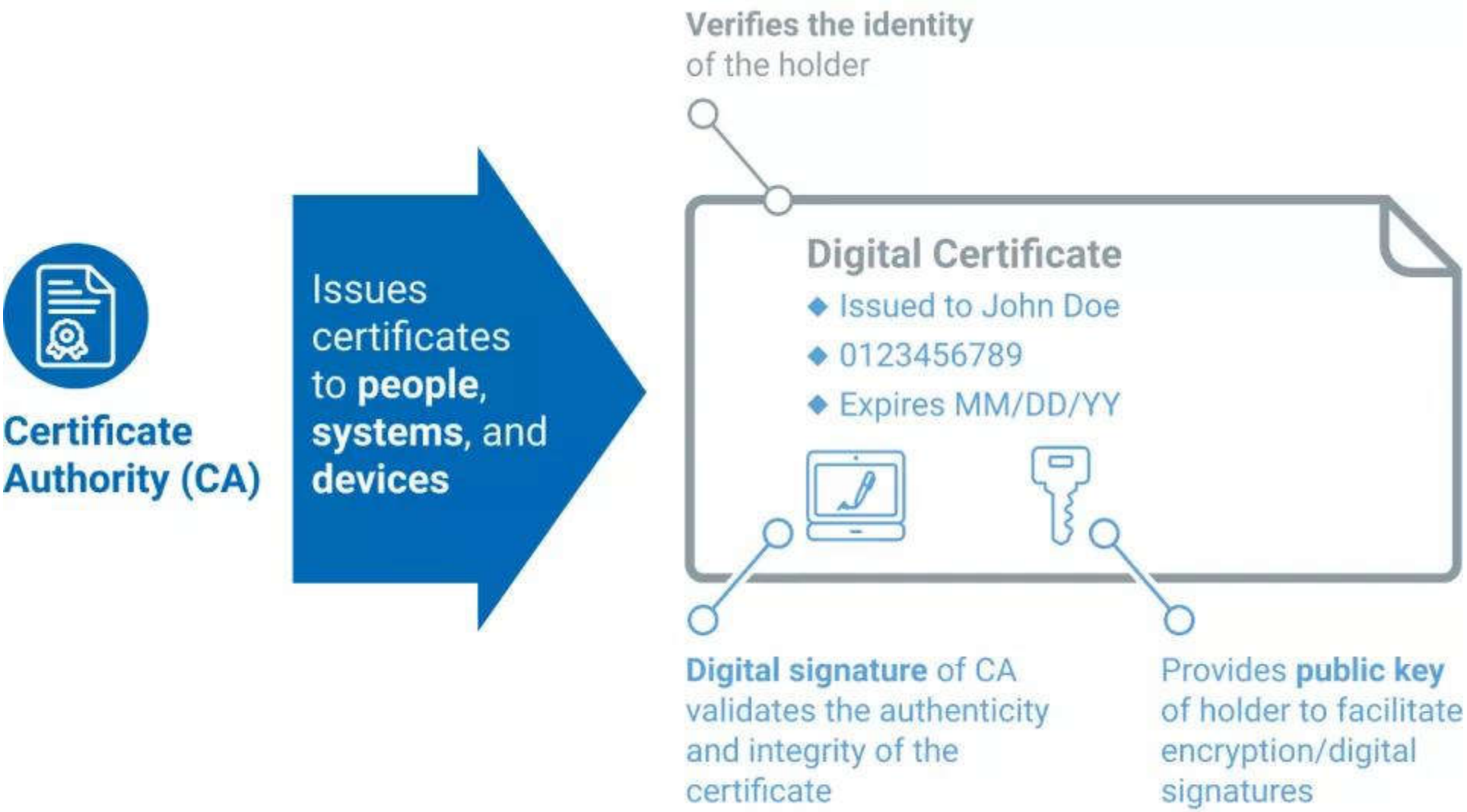
Digital Certificates

- A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).

- Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks.

- A common use of digital certificates is to confirm the authenticity of a website to a web browser, which is also known as a secure sockets layer or SSL certificate.

Digital Certificates



Types of Digital Certificates

- There are three different types of public key certificates.

- A transport layer security (TLS)/SSL certificate.
- A code signing certificate.
- A client certificate.

TLS/SSL Certificate

- A TLS/SSL certificate sits on a server— such as an application, mail, or web server—to ensure communication with its clients is private and encrypted.

- The certificate provides authentication for the server to send and receive encrypted messages to clients.

- The existence of a TLS/SSL certificate is signified by the Hypertext Transfer Protocol Secure (HTTPS) designation at the start of a Uniform Resource Locator (URL) or web address.

Code Signing Certificate

- A code signing certificate is used to confirm the authenticity of software or files downloaded through the internet.

- The developer or publisher signs the software to confirm that it is genuine to users that download it.

- This is useful for software providers that make their programs available on third-party sites to prove that files have not been tampered with.

Client Certificate

- A client certificate is a digital ID that identifies an individual user to another user or machine, or one machine to another.

- A common example of this is email, where a sender signs a communication digitally and its signature is verified by the recipient.

- Client certificates can also be used to help users access protected databases.

Who Can Issue a Digital Certificate?

- Digital certificates are issued by CAs, which sign a certificate to prove the authenticity of the individual or organization that issued the request.
- A CA is responsible for managing domain control verification and verifying that the public key attached to the certificate belongs to the user or organization that requested it.
- They play an important part in the PKI process and keeping internet traffic secure.

Benefits of Digital Certificates

- **Security:** Digital certificates can keep internal and external communications confidential and protect the integrity of the data. It can also provide access control, ensuring only the intended recipient receives and can access the data.

- **Authentication:** With a digital certificate, users can be sure that the entity or person they are communicating with is who they say they are and makes sure that communications reach only the intended recipient.

Benefits of Digital Certificates

- **Scalability:** Digital certificates can be used across a variety of platforms for individuals and large and small businesses alike. They can be issued, renewed, and revoked in a matter of seconds.
- **Reliability:** A digital certificate can only be issued by a publicly trusted and rigorously vetted CA, meaning that they cannot be easily tricked or faked.
- **Public Trust:** The use of a digital certificate proves authenticity of a website, documents, or emails. It can assure users and clients that the company or individual is genuine and respects privacy and values security.

Benefits of Digital Certificates

- **Scalability:** Digital certificates can be used across a variety of platforms for individuals and large and small businesses alike. They can be issued, renewed, and revoked in a matter of seconds.
- **Reliability:** A digital certificate can only be issued by a publicly trusted and rigorously vetted CA, meaning that they cannot be easily tricked or faked.
- **Public Trust:** The use of a digital certificate proves authenticity of a website, documents, or emails. It can assure users and clients that the company or individual is genuine and respects privacy and values security.

Digital Signatures vs. Digital Certificates

- The digital signature is utilized to identify the document's owner. In contrast, a digital certificate is a document that verifies the organization's identification.

- DSS (Digital Signature Standard) is used to generate a digital signature. On the other hand, digital certificates are based on the concepts of public-key cryptography standards.

- When message encryption is required, a digital signature employs the RSA algorithm. In contrast, a digital certificate is a proof that data will be transmitted securely and encrypted.

Digital Signatures vs. Digital Certificates

- A mathematical function (Hashing function) is used in the digital signature. On the other hand, a digital certificate contains personal information that may be used to track down the owner.

- The digital signature is formed by the signer's private key and validated by the signer's public key. In contrast, a digital certificate is provided by a third party and may be validated and authenticated by the end user.

- Digital signatures are utilized to validate the supplied data. In contrast, digital certificates are utilized to confirm the sender's identity.