What is Domain, Organization & Extended Validation Certification?

Ioanna Anifanti - 2022-11-18 - SSL Πιστοποιητικά

What is a certification?

Certification authorities shall issue certificates bearing:

- A public key and

- the identity of the owner for whom the SSL is being issued.

When a user visits a site with a certificate, the browser produces a unique session key that is encrypted with the SSL public key and then encrypts the user's communication with the page. Depending on the browser, the user may see a key icon or a padlock, which indicates that the communication is secure.

The issuing authority has the obligation to certify the SSL requested entity details, while the final version is a confirmation from the authority that the public key included in the certificate belongs to that entity.

Depending on the steps taken by the authority to verify the identity of the entity, three different types of certification are emerging: Domain, Organization, and Extended Validation.

What is the difference between certification types?

Domain Validation

Domain validation guarantees that when using SSL, the exchange of information with this domain will be encrypted and secure. It provides certification at a basic level, and for its

issuance it is sufficient to confirm that the domain name is valid and that it belongs to the entity that requested the certificate. This certification does not require the filing of a document, and just a simple click on the verification link that the publishing authority sends to the domain name owner via mail. For this reason, the certificate is issued and activated immediately.

Its use is for entities (natural persons, businesses, etc.) who need an SSL directly without corporate documents, and is suitable for pages requiring information exchange in encrypted form eg. For login pages, pages that implement small-scale transactions, email servers, etc.

Organization Validation

With Organization Validation, in addition to ownership of the domain name, additional information is provided for the organization or business that has requested SSL. This information includes the name of the entity, the city, the county and the country where it is based. The issuing authority searches on bank or local government sources and databases. In the event of non-confirmation, payment of documents proving the identity of the applicant and the organization is required.

Organization validated certificates are suitable for businesses that, in addition to encrypting information on their page, want to provide page visitors with certification for their corporate identity and corporate identity. It is recommended to independent businesses that require the highest level of security in order to gain the maximum confidence from their customers and maintain their competitiveness. In some browsers, the address bar for pages with Organization Validated certificate becomes blue.

Extended Validation

Extended Validated SSLs are the ones that are accompanied by the tightest audit procedure to confirm the identity of the organization. Organization certificates are differentiated from the certification process, as EVSL is dictated by the Certification Authority Browser Forum and includes 7 levels that require submission of documents for: exclusive ownership of the domain name, headquarters, physical and legal Its functioning, the confirmation that the organization itself has requested the issuance of the SSL and the natural and legal existence of the legal representative.

It's an ideal SSL for companies and organizations that want to show that they have gone through the tightest evaluation test to gain instant customer confidence. It is recommended to large businesses with online and e-commerce services who wish to maintain their competitiveness and immediately notify the customer that they are on a secure page with their personal data and transactions protected.