**What is an EV SSL Certificate?** [**https://www.ssl2buy.com/wiki/what-is-an-ev-ssl-certificate**](https://www.ssl2buy.com/wiki/what-is-an-ev-ssl-certificate)

Primary Keyword: EV SSL Certificate

Secondary Keyword: TLS/SSL certificate, Extended Validation, extended validation process, validation, EV certificate

* Introduction
  + Brief overview of SSL certificates:
  + Importance of SSL certificates in securing online communications.
* Definition of EV SSL Certificate
  + Explanation of Extended Validation (EV) SSL certificates.
  + How EV SSL certificates differ from other types of SSL certificates (DV and OV).
* Validation Process
  + Detailed description of the rigorous validation process for obtaining an EV SSL certificate.
  + Steps involved in the validation process (e.g., verifying the legal, physical, and operational existence of the entity).
* Benefits of EV SSL Certificates
  + Increased customer trust and confidence.
  + Protection against phishing attacks.
  + Improved website security and data encryption.
  + Positive impact on SEO and website ranking.
* Use Cases
  + Ideal scenarios for using EV SSL certificates (e.g., e-commerce websites, financial institutions, and other high-security environments).
* How to Obtain an EV SSL Certificate
  + Steps to purchase and install an EV SSL certificate.
  + Tips for choosing a reputable Certificate Authority (CA).
* Conclusion
  + Recap of the importance and benefits of EV SSL certificates.
  + Encouragement to consider EV SSL certificates for enhanced website security.

-=-===========================================================

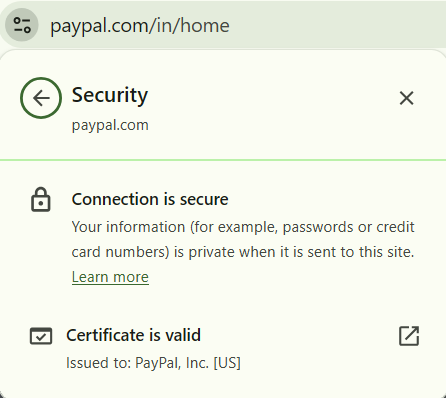
**Introduction:**

SSL (Secure Socket Layer) certificates, also called TLS/SSL certificates used to verify websites' identity with a strong backup of SSL encryption. An SSL certificate protects communication that takes place between a web server and the user's browser. An SSL certificate means that if you share a login credential, credit card numbers or personal data on the site, no eavesdroppers can steal or sniff it.

SSL certificate falls in different validation types including domain validation, organization validation and extended validation. In this short piece of information, we will cover Extended Validation and its important information.

**Definition of EV SSL Certificate:**

Extended Validation (EV) is a type of TLS/SSL certificate that confirms that the SSL certificate holder has gone through the most rigorous identity background checks and vetting to guarantee that the website to which the extension is attached is truly legitimate.



EV SSL certificate is crucial for the users' trust, for the protection of information, rules of the data protection laws. EV SSL certificate is used by organizations having plenty of security concerns, such as financial institutions, selling businesses online and government departments.

**How EV SSL certificates is different:**

EV SSL certificates or Extended Validation SSL certificates are advanced certificates that authenticate the owner of a website more than any other SSL certificates do. The key differences between EV SSL certificates and different types of SSL certificates are:

**Higher Validation**: EV SSL certificates entail a much more strict validation process, which also includes checks of the background, legal status, physical existence, and operational existence of an organization.

**Verified Identity**: EV SSL certificates are thus presented with the most comprehensive trust display details such as the organization name, country of the organization and the padlock icon in a browser once a user clicks on a padlock. It is a way of establishing confidence with users visiting the specific website after seeing a verified identity.

**Time to Issue**: Since the verification process is extended, EV SSL certificates normally take more time to be issued (approx. 4-5 days) than any other type of SSL certificate.

**Higher Cost**: EV SSL certificates cost more than other SSL certificates, but the added level of validation and trust bring its cost higher.

Overall, the use of EV SSL certificates empowers the authentication and garnering confidence of website visitors as well, which makes them good for securing the websites.

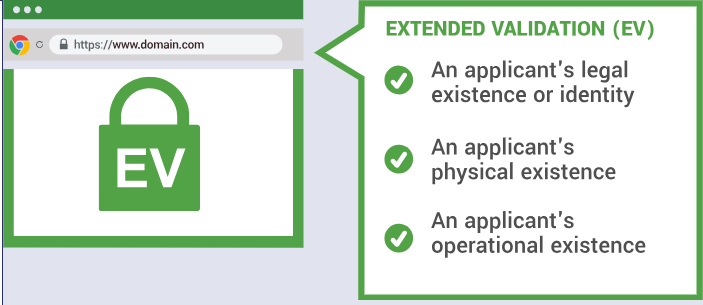
**How Extended Validation validates an Organization?**

EV SSL Certificate verification involves the owner of the website going through a standard identity verification process, which confirms that the domain belongs to an exclusive right holder; as well, the certificate authority checks that an entity carries legal, operational and physical existence.

**Steps involved in the validation process**

The extended Validation process includes a few steps that an SSL applicant needs to follow in order to get a certificate.

* Domain Control Validation
* EV Enrollment
* Verification of Documents
* Confirmation of Legal Existence
* Confirmation of Physical Existence
* Phone Number Verification



https://www.thesslstore.nl/extended-validation-ssl-certificates.aspx

**Domain Control Validation**: An SSL applicant needs to complete the Domain Control Validation (DCV) process before proceeding further with EV certificate issuance. DCV is the first part of an extended validation process. A DCV process can be done via domain-related generic email, CNAME record, and file validation methods. You can find generic emails like:

* admin@abc.com
* administrator@abc.com
* postmaster@abc.com
* webmaster@abc.com
* hostmaster@abc.com

**EV Enrollment:** The certificate Authority ask your organization to submit the EV Enrollment form to ensure the organization is authorized to get an EV SSL Certificate. It is a digital form. If needed, the user must download the form, fill it out manually, and send the scanned version to the certificate authority.

**Confirmation of Legal Existence:** The certificate authority verifies the documents of an organization by checking its legal registered status with the government. The CA will validate the organization's registration information, and the registration status of the organization should be financially active in a government database. If the certificate authority does not find the organization's name, the authority may ask for a document of Article of Incorporation, certificate of formation or any other registered document**.**

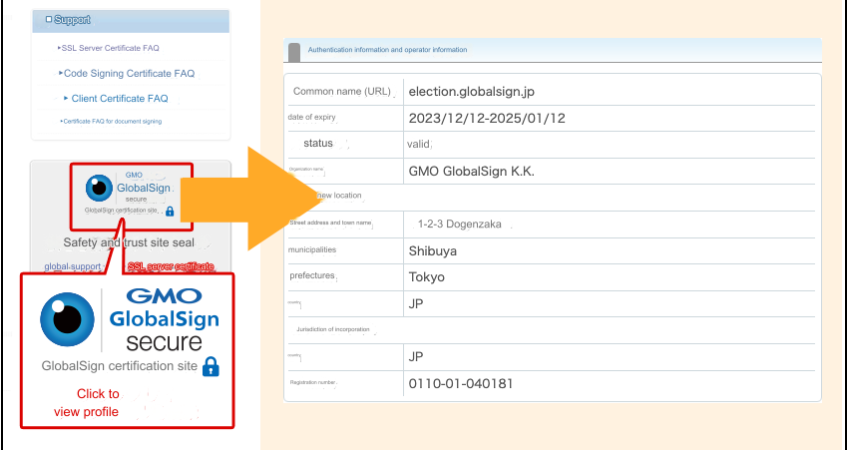
**Confirmation of Physical Existence:** The certificate authority, after the confirmation of legal status, confirms the physical existence of an organization. The authority verifies the physical address (like country or state) of an organization. The address will be shown in the body of an SSL certificate.

**Phone Number Verification:** The final step in EV SSL issuance is phone verification and it should be done to avoid fraud attempts. The authority should call to active verified phone number listed in govt., third party like Dun & Bradstreet, Hoovers, and Bloomberg. A contacted person should be mentioned in the EV Enrollment form.

After the above steps, the EV SSL order will be moved for final approval before the issuance of an EV SSL certificate.

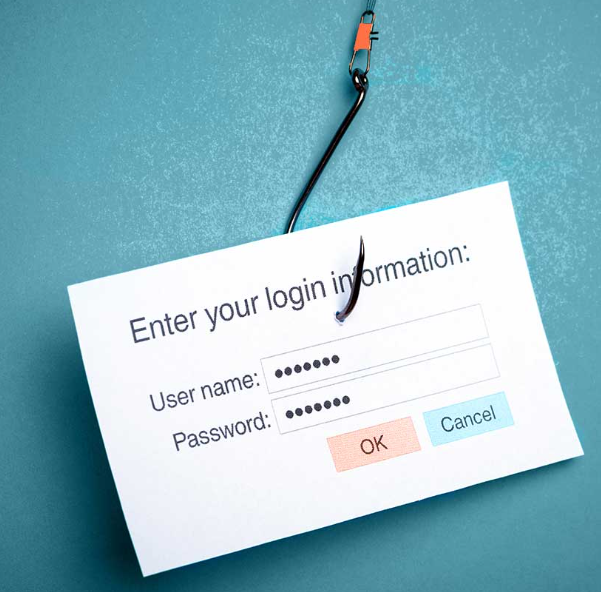
**Benefits of EV SSL Certificate:**

**Trust Logo:** According to the case study, there are 61% of shoppers leave their shopping cart due to the unavailability of a trusted logo. EV SSL certificate allows a secure site seal that can be placed on any webpage for higher assurance. A single click on a site seal can give you a real-time certificate status report.



https://support.globalsign.com/ssl/ssl-certificates-installation/secure-site-seal-overview-installation

**Phishing Protection:** The certificate authority follows a strict validation process that eliminates the chances of phishing websites. Cyber culprits find it difficult to obtain EV SSL due to the systematic validation process**.**



https://cheapsslsecurity.com/blog/what-is-phishing-a-3-minute-phishing-definition-explanation/

**Compliance Requirement:** The EV SSL certificate is bound by PCI-DSS and HIPAA rules and regulations regarding the data protection of customers. When the website has an EV SSL certificate, it indicates that an organization is committed to such laws and regulations.

**Verified Company Details:** End users can click on a padlock icon in a browser to verify the company's details. Thus, they can get assurance about the website's authenticity and data integrity.

**Enhanced Trust**: EV certificates offer trustworthy security in building trust and ensuring an encouraging environment for online shoppers. If shoppers feel safe with their personal and financial information, there will be more checkout in the end.

**Use Cases:**

Extended validation in EV certificate means the certificate applicant has completed verification of details like domain, organization's legal status, physical existence, and operational existence.

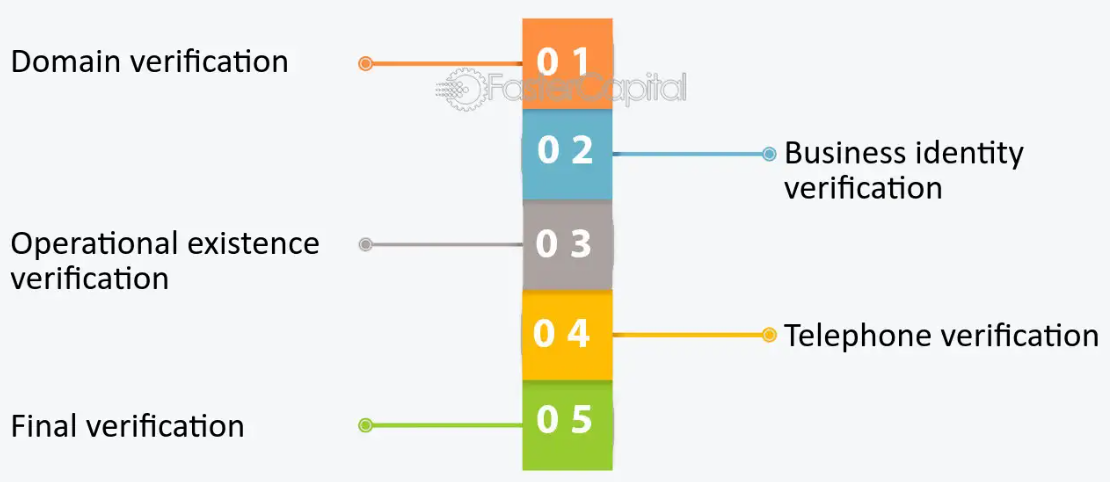
EV SSL certificate is used by below entities and organizations.

* E-commerce websites
* Financial Institutions
* Banks
* Fortune 500 companies
* Healthcare and Insurance companies

Users enter their financial information on such sites; hence, it requires strict validation and strong encryption standards.

**How to Obtain an EV SSL Certificate**

EV SSL certificate, as we discussed, requires a systematic and strict validation process, which includes a few steps as discussed under in order to obtain an EV SSL certificate. An organization must prove legal company name, location, and domain name ownership to get this type of SSL/TLS certificate.



https://fastercapital.com/content/Extended-Validation--EV--trust-certificate--Elevating-Trust-in-E-commerce.html

* First, you need to open an account with your SSL provider and select EV SSL certificate.
* After paying the price, you need to start generating CSR (Certificate Signing Request) from the server on which you wish to install the certificate.
* You need to submit the CSR to the SSL provider and start the configuration process, where you need to provide basic information.
* After that, you need to complete the domain verification process by approving the generic email (admin@, administrator@, hostmaster@, postmaster, webmaster@) you receive. The domain control verification process (DCV) can also be completed with the file base and CNAME method.
* Once the DCV process is completed, you will be asked to provide business registration documents for further verification.
* The certificate authority will verify the organization's physical, operational and legal existence before the issuance of a certificate.
* Here, the authority checks the organization's status with the registration agency. The company's name should be verifiable and registered.
* The authority checks that the company is able to do business operations.
* After that, the vetting department arranges a telephone call to confirm the order and employment binding with the Subscriber Agreement.
* Finally, the certificate authority issues an EV SSL certificate after verification of all required documents and domain ownership.
* You need to install the EV SSL certificate on the server on which the CSR was generated.

**Conclusion:**

Overall, an EV SSL certificate is the most secure and trustworthy kind of certificate for the website. It undergoes a thorough process of validation to confirm that the website is being run by an organization you can trust and stand in confidence with. An EV SSL certificate is an essential investment in online security and customer trust for businesses that handle sensitive transactions and must achieve a high level of trust between their customer and themselves.

