EV VERIFICATION GUIDE

EV Verification Guide

Extended Validation (EV) SSL certificates have a unique issuance and management process which guarantees that internet browsers qualify quickly and trust your web site. When an applicant applies for an EV certificate, they are submitting to a pre-approved Certificate Authority (CA) that will perform rigorous verification steps to ensure the EV certificate is issued to an authorized applicant.

HOW TO APPLY FOR AN EV CERTIFICATE

1. Only certificate authorities (CAs) which pass an independent, qualified audit review may issue EV certificates. CAs must follow rigorous steps before issuing an EV SSL certificate.
2. The authorized CA evaluates the organization applying for the certificate to verify their identity and check that they should receive an EV SSL certificate.
3. The authorized CA confirms the organization's registered legal name, registration number, registered address, physical business address and any assumed business names.
4. The authorized CA verifies the applicant organization's right to use the domain name.
5. The authorized CA substantiates that the applying organization has approved the issuance of an SSL certificate with EV.
6. The authorized CA makes sure the organization applying for an EV certificate is not located in a country on government prohibited lists.
7. Only when everything checks out does the CA issue the EV Certificate.

Source: CA Security Council **https://casecurity.org/**

Step 1: EV Certification Authorities

EV Certification Authorities (CA) must first ensure they meet the requirements of the CA/Browser Forum EV Guidelines. This is done with a pre-issuance audit to ensure that the CA knows and employs the processes and procedures needed to issue EV certificates to their full requirements.

Annually, the EV CAs must show compliance to their issuance guidelines. This requires three audits which include WebTrust for CA, SSL Baseline Requirements, and WebTrust for EV. Audit results must be publicly posted and provided to the browsers within three months from the end of the audit period. CAs which are unaudited or have not posted a qualified audit may be subject to removal from the browser or operating system.

Step 2: Organization Validation

The identity of the organization applying for an EV certificate must be verified with their registration authority. During verification, the registration authority checks with the government agency that originally registered the entity. The registration authority never verifies with a commercial data business, such as Dunn and Bradstreet. The exact business name that is discovered during verification and was used during registration with the government is included in the certificate and used by the browser to show who the trusted company is that operates the website.

Step 3: Organization Registration

The certificate will also include what type of entity the business is—whether they are private, government or non-commercial. The jurisdiction information is included in the certificate indicating which state, province or country the entity was registered in. The registration number or date of registration is included in the certificate. The physical business address is verified and included in the certificate. Also, if the company wants to use a doing-business-as name, this is verified and is included as part of the organization name.

With all of this verification, the owner of the website is well established and provides the browser user additional information to decide whether to trust the website owner. It also provides law enforcement with more data to reach out to a website owner if required. This level of verification is not attractive to an attacker, discouraging them from applying for an EV certificate.

Step 4: Domain Name Validation

Domain names, in the context of EV verification, are restricted to fully qualified domain names only. No IP addresses, reserved or unregistered domain names are allowed.

Determining domain name ownership or control is done similarly to the process performed for domain validated or organization validated certificates. The substantial improvement is that no certificate is allowed to be issued for a domain name because you have established control of the domain name. The owner of the domain name must also approve the issuance of the certificate. This avoids an attacker from obtaining control of a website and establishing his own certificate for fraudulent use.

Step 5: Certificate Issuance Authorization

EV authorization requires access to contacts across multiple roles within the certificate acquiring organization. The issuance process requires a Contract Signer, Certificate Approver and a Certificate Requester to be identified.

The Contract Signer must accept the terms of the certificate subscriber agreement. The Certificate Approver must approve all requests from a Certificate Requester. Authorization of the Contract Signer and the Certificate Approver must be established through a means such as a verified professional letter, a corporate resolution, through contract or by an independent confirmation.

Step 6: Risk Mitigation

Certificate issuance risk mitigation is performed by the CA. The CA must not issue certificates to countries which are not allowed in the jurisdiction where the CA is operating. The CA must also respect any denied lists or legal blacklists supported by their country of jurisdiction. This helps to avoid certificates being issued to currently known harmful applicants.

The CA must perform extra due diligence for applicants who have been established as targets for phishing. The CA can use their own database of customers which have had applications rejected or certificates which have been revoked to help remove attackers.

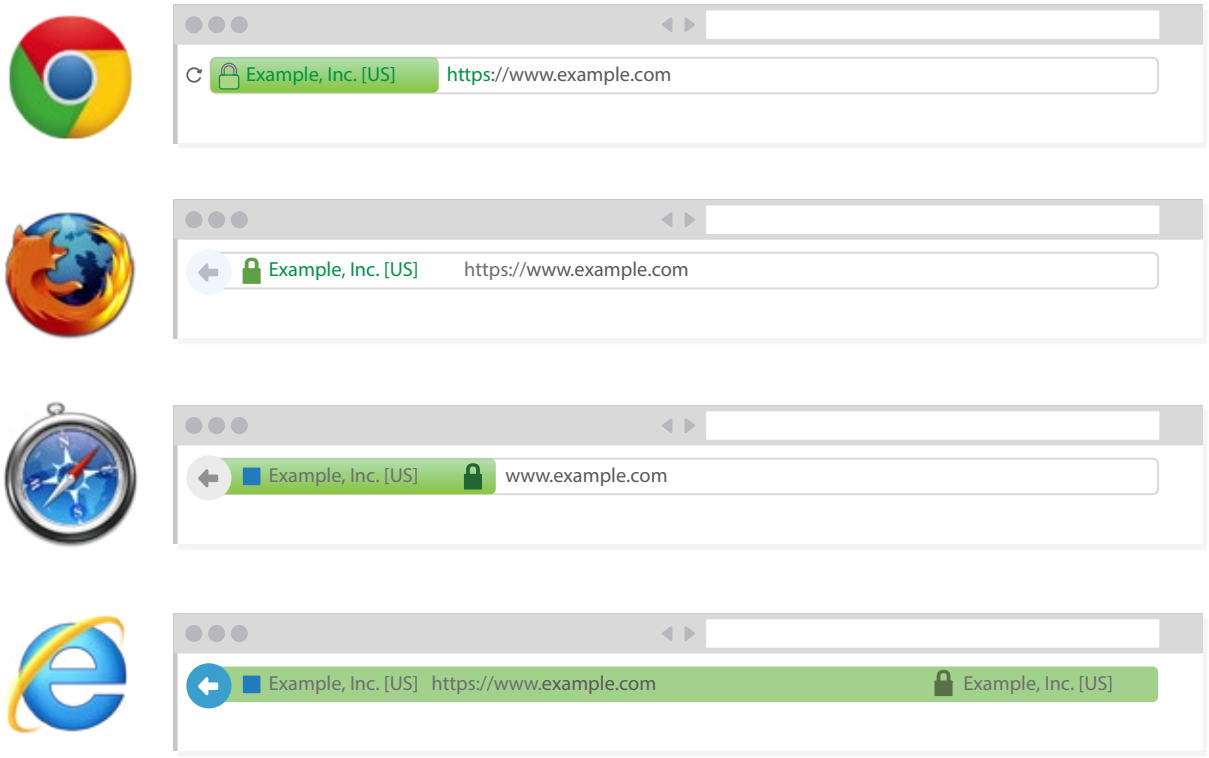
Finally, all verifications must be reviewed and approved for quality. The person performing verification qualification can reject certificate applications if they do not receive a satisfactory explanation from the applicant to issues that arise during the verification process in a reasonable period of time.

EV Certificate Issuance

Once all certificate validation is performed, then the CA can issue the certificate.

EV certificates not only provide security and privacy, but they also provide trust. The issuance of the EV certificate has been authorized by an entity which has been physically established. The issuance has been authorized. And finally, the information in the EV certificate is display to the browser user showing a green “go” color and the name of the website owner.

EV certificates reduce phishing and man-in-the-middle attacks, bring trust, reduce shopping cart abandonment, protect brand and provide support saving. Go green, go EV.



@EntrustDatacard /EntrustVideo /EntrustSecurity +entrust datacard-group RSS

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™

30126-1-0116