THE BUSINESS VALUE OF EXTENDED VALIDATION

How Internet Browsers Support
EV and Display Trusted Websites

Table of contents

Introduction

Extended Validation (EV) certificates were launched in January 2007. EV certificates are an effort to define a standard for a high assurance SSL/TLS certificate and create a **new trust foundation**. The EV Guidelines are managed by the leading browsers and certification authorities (CAs) through the **CA/Browser Forum**, and have been since launch.

This paper will discuss:

- What the objectives are for the implementation of EV certificates
- How the EV Guidelines set the standard for SSL/TLS certificate issuance
- How the browsers support EV certificates and display trusted sites to browser users
- How EV certificates mitigate phishing, Man-in-the-Middle (MITM) attacks, provide site acceptance and increase secure transactions

There are now over 130,000 websites protected with EV certificates as indicated by Netcraft in July 2015. EV is growing at a rate of 20 percent year over year. While some may think this growth is small and the number of websites employing EV certificates consists of a very small portion of the Internet, the year over year growth is increasing and indicates a change in mindset as several of the most frequently visited and globally trusted brands (i.e. American Airlines, Apple, Citibank, Fidelity, PayPal and Twitter) have adopted and deployed EV.

Objectives

The CA/Browser Forum defined primary and secondary objectives of EV Certificates.

Primary

The primary objectives of EV certificates are to:

1. Identify the legal entity that controls a web site by providing reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by the specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
2. Enable encrypted communications with a website by facilitating the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a web site.

Secondary

The secondary objectives (which are derived from the primary) help establish the legitimacy of an entity claiming to operate a website, and provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the entity, EV SSL Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using certificates;
2. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
3. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including, where appropriate, contacting, investigating or taking legal action against the entity.

Excluded Purposes

Please note the focus of EV certificates is to identify the subject of the certificate and the authorization to issue the certificate. The EV process does not represent that the subject is actively engaged in doing business, complies with the applicable laws or that they are trustworthy, honest or reputable in their business dealings. The EV process does not indicate that it is safe to do business with the subject named in the EV certificate.

CA/Browser Forum Focus

The focus of the CA/Browser Forum is to implement standards and practices which fulfil the primary and secondary EV objectives. These practices provide verification principles and would be auditable to confirm compliance.

It is important to note and state the excluded purposes. Fundamentally, there are no verification processes which verify the reputation of the certificate applicant. Even if there was, it would be impractical to track that rating through the life of the certificate. As such, browser users must make this judgement themselves, in a similar way as they would when visiting the brick-and-mortar site of the applicant.

How to bring trust

Through multiple proposals and eighteen months of work, the CA/Browser Forum developed **Extended Validation and the EV Guidelines**. The EV Guidelines raised the level of applicant identification, authorization to issue, validation requirements, high risk mitigation, technical leadership and annual compliance audits.

Identification

For domain validated (DV) certificates, there is no requirement to determine or publish the identity of the certificate subscriber. For organization validated (OV) certificates, the identity is determined. For EV, the verified legal identity is determined in a very rigorous way and only certain types of identities are eligible to purchase EV certificates.

EV verification includes determination of legal identity, physical existence and operational existence. It also verifies the type of organization, registration number and the jurisdiction of registration.

The identity is restricted to entities which have been registered with a government agency or to an actual government agency. If the entity has not been registered, then they cannot apply for an EV certificate.

Accumulation and verification of identity information drives attackers away from EV. With this type of data, it becomes easier to track attackers down. In addition, this data also reduces the likelihood that the owner of the website will perform fraudulent activities since the CA is always in a position to provide identity and verification data to law enforcement.

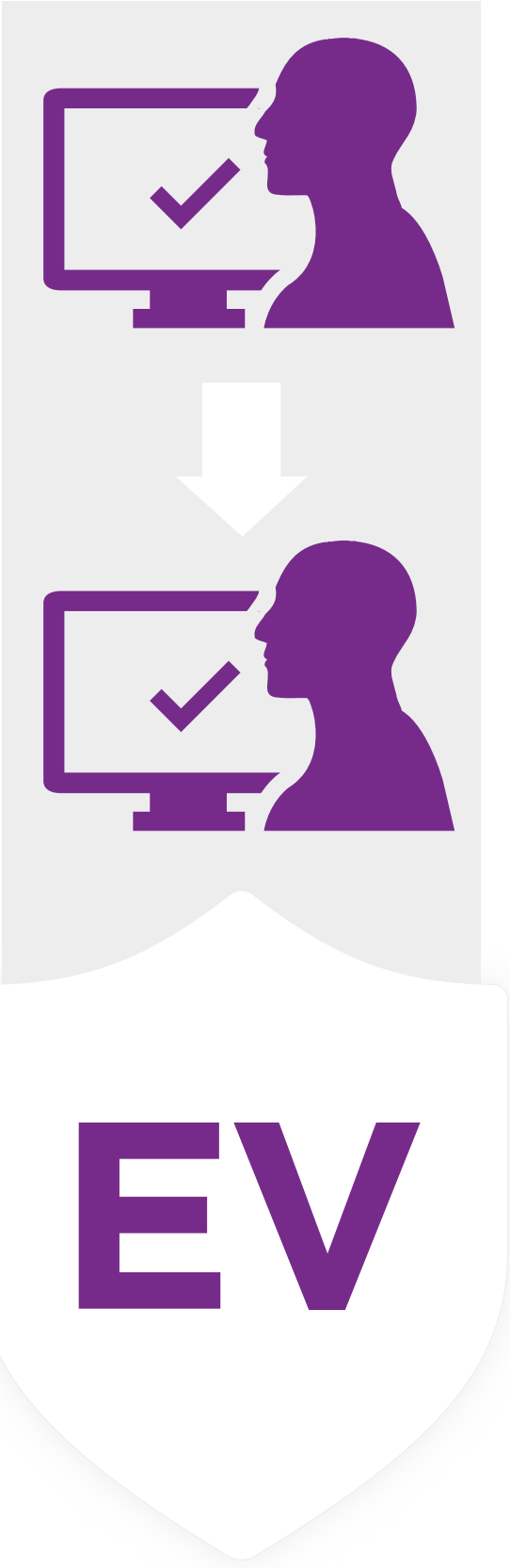
Authorization

No authorization is required to issue a DV certificate as the CA needs only to determine that the requester owns or controls the domain. For OV certificates, the CA must contact the applicant through a reliable method of communication to confirm the authenticity of a certificate request. For EV certificate requests, authenticity and authorization are also confirmed but in a more rigorous way.

EV has three roles which must be identified and authorized; the Certificate Requester, Certificate Approver and Contract Signer.

Authorization comes from a hierarchical model. The contract signer and certificate approver must authorized through a method such as a professional letter from a lawyer or accountant. It can also be done by an authority verified to be with the identity, a corporate resolution, a new or prior contract, or though information from a government database. Once this is accomplished, the CA will have a source to accept the subscriber agreement and have all certificate requesters approved.

Exposure of all parties involved with authentication and authorization helps discourage attackers from requesting EV certificates.



Validation

Unlike DV certificates, EV validation is not automated and requires a validation specialist to perform verification. The EV guidelines set the bar by defining the security requirements, training and testing of a validation specialist.

Once the validation specialist has completed verification, a second party must review the validation to ensure the processes have been completed in a proper manner. This mitigates false verification by having quality assurance performed before the certificate is issued.

Manual verification will also mitigate the risk of a fraudulent certificate request. In automated verification, a requester can submit requests multiple times. Their goal is to game the system and look for faults which can be used for a fraudulent request. Manual verification makes this tactic obsolete.

In addition, an EV certificate can only be issued using information which was verified in the last thirteen months. This requires the validation team to keep the information updated on a regular basis and will mitigate issues where domain name ownership changes or there is a company name change.

High Risk Mitigation

As EV SSL certificates are issued to help mitigate phishing, the EV guidelines implemented requires for the CA to perform additional scrutiny for domain names with a high risk for phishing or other types of fraudulent usage.

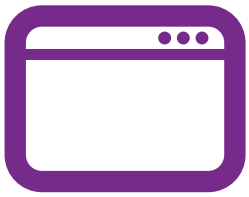
CAs are also required to maintain criteria or a database which covers information such as names contained in either previous rejected certificate requests, revoked certificates, and more (i.e. the Miller Smiles phishing list or the Google Safe Browsing list). With this information the CA verification team can raise the level of due diligence to determine whether a certificate requested will be approved.

EV high risk verification also requires the CA to use denied lists or other legal black lists which are available in the CAs jurisdiction. If the certificate requesting entity, contract signer or certificate approver or place of business is on the list, then the CA is not allowed to issue the certificate.

Technical Leadership

In addition to raising the bar in certificate validation, the EV guidelines set minimum requirements for technical and crypto data.

The EV guidelines were developed in 2007, just before the industry increased the bits of encryption required to secure data and transactions. The National Institute of Standards and Technology recommended that 1024-bit RSA keys and SHA-1 hash algorithm not be used after 2010. As such, the EV guidelines also mandated that 1024-bit RSA keys could not be used after 2010 and that the new baseline key size would become 2048-bit RSA.



Due to backwards compatibility issues with browsers and operating systems, the CA/Browser Forum was not able to mandate the move from SHA-1 to SHA-2 hashing algorithm in the same time frame. Please note that for DV and OV certificates, it took until the end of 2013 to migrate away from 1024-bit RSA keys.

Certificate status is provided through certificate revocation lists (CRLs) and online certificate status protocol (OCSP). Timeframes for CRL and OCSP responses are set to seven and four days respectively, with validity periods of seven and ten days. Shorter validity periods help mitigate attacks with a compromised or fraudulent certificate.

The EV guidelines confirm how root CA and subordinate CA private keys must be protected on a hardware security module (HSM) and which standard and level the HSM must meet. The guidelines also define how a CA private key should be generated. This requirement supports trust in a CA key from the day it is generated, and provides evidence to auditors that confirms this fact.

A root certificate cannot support EV certificates unless the CA entity has been approved by the browser or operating system vendor. Each vendor has a different policy which the CA must work its way through. Once the CA has been accepted, then the browser associates the root through metadata with a CA designated EV certificate policy object identifier (OID). All CAs have different policy OIDs, so if a root is compromised and a policy OID is untrusted, rejection of the OID will impact only one CA entity.

Validity periods of EV certificates were capped at 27 months. This would allow two-year EV certificates to be issued with an overlap of three months to validate and move to a renewed certificate. Of course with the validation rule of only using data which was validated in the last thirteen months, a two year certificate must be revalidated upon renewal.

EV certificates can only be issued to a domain name or IP address which has been registered. As such **attacks using non-registered internal domain names**, reserved names and reserved IP addresses are mitigated. This same requirement is being pushed down to DV and OV certificates as well, but will not be fully implemented until the fall of 2016.

Wildcard certificates are not permitted for extended validation. For example, if a subscriber owned **example.com** and wanted a certificate to support all sub-domains, they could not ask for ***.example.com**.

Wildcard certificates work differently. Wildcard subscribers can use multiple sub-domains related to their root domain name. By excluding wildcard certificates from the extended validation process, wildcard subscribers are not able to support an EV validated website with a suspect name such as facebook.example.com.

If an EV subscriber does want to support sub-domains, then they are permitted to request that each sub-domain be added to the subject alternative name (SAN) object identifier. By requesting each individual sub-domain, the CA can review and reject any sub-domain which could confuse a browser user.

Compliance Audits

The addition of the EV guidelines meant there was more criteria for a CAs to implement to show conformance. Before EV, all CAs would be annually audited based on standard criteria established by the WebTrust and the ETSI compliance programs. Once the EV guidelines were released, the audit community prepared additional audit criteria. As such, on an annual basis an EV CA must meet both the standard audit criteria and the EV criteria.

The EV guidelines also established the now current practice of requiring all new CA entities to have a pre-issuance readiness audit, and all CAs in production to have a self-audit performed every three months. Also note, the EV Guidelines set the standard for the SSL Baseline Requirements which have also provided another audit criterion for all EV CAs to meet.

Browser support

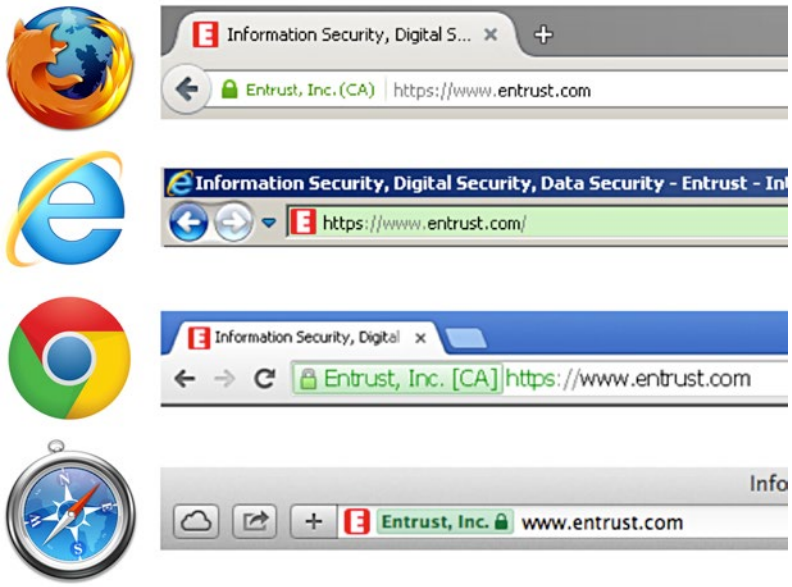
So how does EV show security to a website visitor? How can a subscriber know if an EV certificate has fraudulently been issued to their domain name?

Let's discuss the browser status bar and certificate transparency.

Status Bar

For DV and OV certificates, the browsers put a lock icon in the status bar. In older browsers, the lock icon was shown elsewhere in the browser chrome—the graphical framework and elements of the web browser window. The lock icon was so popular that website developers would put their version of the lock icon on their webpage. As such, a non-secured webpages looked trusted based on the well-placed lock.

A visitor to a website protected with an EV certificate could also be fooled. That's why newer browser versions have added other indicators to show website trust. Starting with the release of Internet Explorer 7 and Windows Vista, Microsoft indicated EV with a green lock. Internet Explorer also indicated the subscriber's organization name and the root CA name revolving in the browser status bar. As EV was subsequently adopted by Mozilla Firefox, Apple Safari and Google chrome, the green indication and the subscriber's name has become the clear indication to a user that the site is trusted and secure.



A similar type of EV representation has also been deployed in mobile browsers.

Please note that EV SSL certificates are supported on all current user operating systems and browsers.

Certificate Transparency

Google has also helped to extend trust to subscribers of EV certificates using certificate transparency. After the CA attacks in 2011, the industry wanted to be able to monitor which certificates were issued to which domains. Experts proposed systems including Sovereign Key, Convergence, Perspectives and Certificate Transparency (CT). CT is the option which the industry has chosen.

The idea regarding CT is, that all SSL/TLS certificates would be disclosed in many publicly available logs. The logs can be audited for reliability and monitored by domain owners.

Through 2014, logs were developed and EV CAs implemented certificate transparency for their EV certificate issuance. By the end of 2014, all currently valid EV certificates were provided to Google to be whitelisted for Chrome. As of January 2015, almost all EV CAs received signed certificate timestamps from distributed logs for their EV certificates.

Now the logs can be monitored by domain name owners or service providers to show all certificates which have been issued for an EV certified domain. If the domain owner indicates the certificate issuance was not authorized or was fraudulent, then the issuing CA can revoke the certificate to mitigate issues.

The EV advantage

EV Indication

Most of the items discussed so far happen behind the scenes, so an end user will never know what actions have been performed to bring trust to a website. Fortunately, the browsers support the EV green indication and the display of the subscriber name which has provided the impression of strong trust to many browser users.

The CA Security Council performed a trust survey which indicated 53 percent of respondents identify the padlock as increasing confidence in an e-commerce site. In addition, 42 percent associate the green bar and organization name in the status bar with greater safety. Greater safety means greater trust which keeps users on the website, reduces shopping cart abandonment and drives more sales and other transactions.

Microsoft stated "One of the indicators of diminished consumer confidence is the level of "shopping cart" abandonment a site encounters. Numerous studies indicate that by implementing EV Certificates, sites can lower the level of cart abandonment and increase site revenues. For example, Overstock.com reported an 8 percent reduction and Fitness Footwear reported a 13 percent reduction in cart abandonment. Canadadrug.com reported that after implementing EV Certificates 33 percent more of the purchases were completed with 27 percent higher sales per transaction."

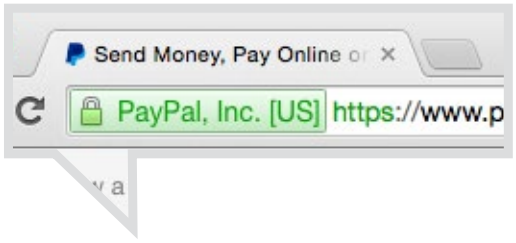
MITM Proof

In 2015, we saw a number of man-in-the-middle (MITM) vulnerabilities with incidents such as Superfish, PrivDog and a CNNIC issued subordinate CA certificate. In all cases a CA certificate was deployed between the browser user and their targeted site. In all cases an SSL/TLS session was enabled, but the session was open where it is possible to review or change data.

EV SSL is virtually MITM proof. Since then an EV Subordinate CA must be in the hierarchy of a root CA which has been designated by the browsers as EV, making it extremely hard for an attacker to issue an EV certificate.

Steve Gibson of Gibson Research Company advises that **EV SSL certificates are spoof proof** if you are using any browser other than Internet Explorer. This helps to mitigate MITM attack, because if you are expecting to see an EV indication and you don't, then perhaps a non-EV certificate is being used for MITM.

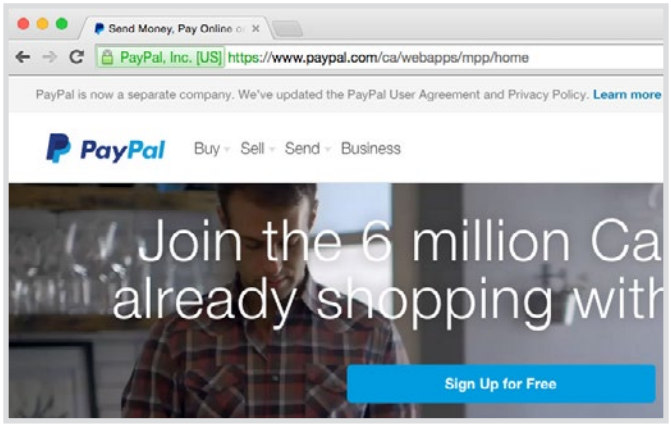
Please note that this only works if the user is expecting to see an EV indication, so it's best to promote to users how safe your site is, because you use EV.

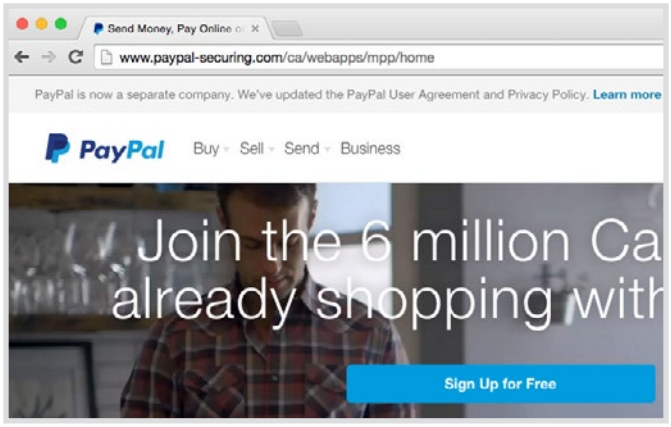


Phishing Proof

How about "Phishing proof"? In this case an attacker must have a site which represents your site but the attacker won't be able to get an EV certificate with your identification in it. As such, if your users expect to see an EV indication with your company's name, then they will not be fooled when they see a phishing site with no EV indication.

Here is an actual example of the real PayPal site and the phishing PayPal site.





Which is which? The green indicator shows you the answer.

When to use EV SSL

EV SSL certificates should be used when you want to indicate or develop trust with your brand's identity. EV is great for companies of all sizes, ranging from small-and-medium-sized businesses to Fortune 500 companies.

EV certificates are already deployed by many top financial institutions and e-commerce sites, but many more industries/websites can benefit from them. This is especially true if a site is used for transactions of any sort, or one that attracts new customers who may need some reassurance about the legitimacy of the business before transacting.

EV Certificates are proving to be a valuable tool for rebuilding consumer confidence and brand protection by communicating to the user with clear visual indicators the validity of the website's identity and the related security of the content being exchanged.

5 Key Takeaways

1. **Legal Identification and Exchange of Encryption Keys:** the EV validation process was designed by the CA/Browser Forum to identify the legal entity that controls a website, and enable encrypted communication of information over the Internet between the user of an Internet browser and a website.
2. **Inherent Trust:** web browsers inherently trust EV certificates more than others, and display them more prominently.
3. **Increased Customer Confidence and Decreased Abandon Rates:** the green bar helps browser users identify the website. Attackers cannot replicate the green indication, so confidence is assured and transaction conversions increase.
4. **Protection against Phishing and Attacks:** with increasing Phishing targeting e-commerce sites and financial institutions, EV SSL certificates give websites validity and protect against phishing and other malicious attacks with advanced encryption.
5. **Savings:** EV certificates prove the legitimacy of the website with branded protection and help reduce support costs and calls from browser users who have given their credentials to attackers.

As Microsoft further states, "By implementing EV Certificates, businesses can help remove one of the largest obstacles that prevent users from sharing personal information and completing online transactions."

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**.

Company Facts
Website: entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Twitter Facebook Youtube LinkedIn Google+ RSS