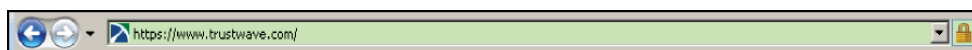


Extended Validation (EV) SSL Certificates



Trustwave Extended Validation (EV) SSL certificates institute and maintain consumer confidence in your organization and Web site via a rigorous validation process and the distinctive green Internet-address bar displayed by consumers' Web browsers.

Establish and maintain credibility to increase e-commerce conversions



The green Internet-address bar displayed in Internet Explorer by a Web site that presents an EV SSL Certificate

When a consumer adds an item to their online cart, but fails to convert their browsing to a purchase, an e-commerce merchant loses a sale. There is no single explanation for shopping cart abandonment, however, all e-commerce merchants know that it occurs every day and want to do all they can to alleviate the phenomenon's strain on their business.

A number of studies connect shopping cart abandonment with a lack of faith in a merchant's reputation and security practices. Consider the same concept in the brick-and-mortar world – a majority of consumers would prefer to purchase an item from an established electronics retailer rather than out of the trunk of a car.

Consumers need to know they can hold a merchant accountable for a purchase. A customer wants to know it's easy to contact a merchant in the event of a problem and that the merchant will take responsibility for the purchased product. Before a consumer makes a purchase, they also want to trust that a merchant handles personally identifiable information and payment card numbers in a secure, responsible manner. In the e-commerce realm, questionable merchant operations, phishing attacks (wherein a fraudulent Web site represents itself as a legitimate Web site to steal sensitive data) and data security breaches in general continue to shake consumers' confidence.

Trustwave Extended Validation (EV) SSL certificates protect a merchant's transactions with its customers by encrypting sensitive data, including payment card numbers, and establishing, without a doubt, the legitimacy of the business by displaying the trusted green Internet-address bar.

About Trustwave

Trustwave is a leading, global provider of information security and compliance management solutions to large and small businesses and the public sector. Trustwave offers and supports SSL certificates, proprietary security appliances, managed security services and compliance management solutions to help organizations simplify, accelerate and validate their compliance with industry standards and regulations such as PCI DSS, HIPAA, SAS-70, GLBA and ISO 27002 (formerly 17799) among others. Trustwave's clients include financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

www.trustwave.com 1-888-878-7817



The New Standard in Internet Security: Trustwave Extended Validation (EV) SSL Certificates

Certificate Authorities (CAs), entities such as Trustwave that issue security certificates, and Web browser software vendors worldwide collaborated to institute the EV SSL Certificate Standard and provide for a more secure Internet. The continued evolution of Web-based exploits, phishing scams and other fraudulent online activity made it necessary to develop a mandate for the authentication of Web sites and their owners. EV SSL certificates transcend traditional SSL certificates because of the stringent validation criteria required for their issuance:

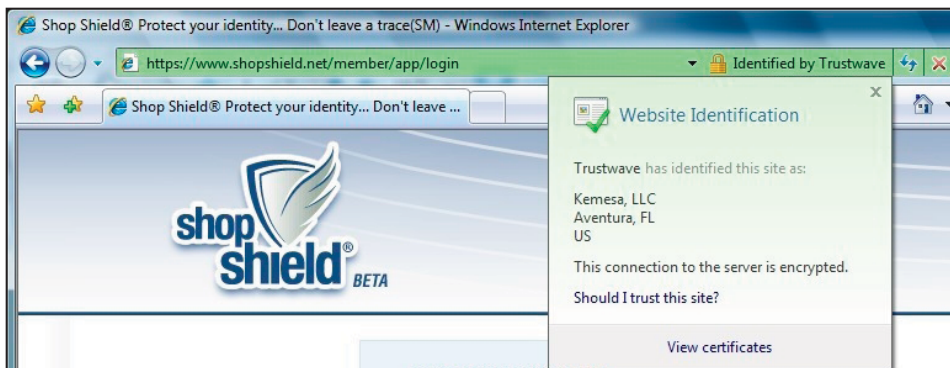
- **Legal Existence and Identity** – Verification of an organization's legal existence and identity via government records and verification of an organization's Doing Business As (DBA) name via government records or a letter from a registered lawyer or a Certified Public Accountant (CPA)
- **Physical Existence** – Verification that an organization conducts business operations at the physical address provided by the organization via corroboration with business registry databases, a letter from a registered lawyer or a CPA or a visit to the site
- **Operational Existence** – Verification of an organization's ability to do business via validation of the organization being incorporated for three years, verification from a regulated financial institution or a letter from a registered lawyer or a CPA
- **Domain Name** – Verification of an organization's exclusive control of applicable domain names via public records, documents from an approved domain registrar or a letter from a registered lawyer
- **Authorization** – Verification of name, title, agency-status and authority of an organization's agents that request and approve the EV SSL certificate on behalf of the organization via confirmation with the applying organization's human resources department or a letter from a registered lawyer or a CPA

Source: CA/Browser Forum's EV SSL Certificate Guidelines Version 1.1 effective April 10, 2008

As evidenced above, an organization subjected to EV SSL certificate validation undergoes a thorough review. The meticulous verification process of an EV SSL certificate ensures that the certificate and green Internet-address bar exude a higher level of credibility, security and trust. An EV SSL certificate promotes the fact that a qualified authority has validated a merchant's existence, adding trust to the purchase process.

The Green Internet-Address Bar: Greater Security Visibility

To reinforce trust in the Web site authenticated with an EV SSL certificate, the Internet-address bar in a site visitor's Web browser shades green to differentiate it from other Web sites. Among others, Mozilla, Microsoft, Opera, KDE and Apple browsers all support EV SSL certificates. In the Internet Explorer Web browser for example, the green Internet-address bar helps customers immediately distinguish a Web site with a valid EV SSL certificate from suspicious or fraudulent Web sites or Web sites that use traditional SSL certificates.



EV SSL certificate's green Internet-Address bar and Web site identification information displayed in Internet Explorer

Trusted CommerceSM Web Site Security

Trustwave's Trusted Commerce program protects a merchant against data security breaches and fraud. The Trusted Commerce program includes Payment Card Industry Data Security Standard (PCI DSS) compliance services, SSL certificates and the Trusted Commerce Web site security seal.

The Trusted Commerce seal denotes credibility. A Web site that displays the Trusted Commerce seal handles sensitive information in a secure, responsible manner. When an organization uses Trustwave SSL, PCI DSS compliance services and promotes that fact with a Trusted Commerce Web site seal, a shopper can rest assured that payment card information and other sensitive data provided to the organization's Web site will not fall into the hands of malicious individuals seeking to profit from stolen consumer data.

While ideal, layered protection includes both PCI DSS compliance services and SSL certificates from Trustwave, users of either solution can display the Trusted Commerce seal on their Web site.

Millions of consumers view the Trusted Commerce seal daily on merchant Web sites across numerous industries.

