Protecting Your Brand & Customers

Business Value of Extended Validation SSL Certificates

Contents

Introduction

Deceptive e-mail and malicious web sites are increasingly responsible for compromising user's personal information, eroding their confidence in online transactions, impacting the businesses ability to communicate with its customers and conduct ecommerce. Based on an analysis by Microsoft completed in early 2008, 10-80% of email purporting to come from many Fortune 500 ecommerce sites is forged, often leading users to fraudulent web sites. These exploits not only impact user's privacy, but are increasingly a threat to corporate data, infrastructure, and often more visibly, their brand value. Domains owned by leading online financial services and commerce sites are increasingly being targeted by these online criminals.

Historically Web site security focused on protecting information in transit—helping to keep information safe from prying eyes. Companies conducting e-commerce and collecting personal data have adopted SSL certificates to help secure those communications. A Secure Sockets Layer (SSL) certificate allows the user to see who the site belongs to, and contains information about the certificate holder, the domain to which the certificate was issued along with and the country it was issued in. The certificate sits on a secure server and is used to encrypt the communications and identify the Web site. While SSL was designed to protect your customer's information from being accessed by 3rd parties, criminals have been able to obtain 'valid' SSL certificates for their deceptive sites, targeting domain misspellings or unregistered top level and country specific domains such .net or .de.

Unfortunately phishing sites have secured many popular and commonly misspelled domain names and have been exploiting user's mistakes for their own gain. Often those sites will obtain SSL certificates to further their deception, where users are unlikely to notice an extra character or wrong spelling in the address bar. While looking for that gold padlock icon continues to be important, without site identity information, users can end up sending personal information to the wrong Website, resulting in loss of financial and personal information.

Responding to these threats, the CA/B Forum has developed the Extended Validation (EV) SSL Certificate, to provide consumers with a higher level of trust. Working with key industry and business stakeholders, a standardized authentication process has been created that every CA must follow if it is to issue this new type of SSL certificate. The process not only helps to avoid issuing certificates to deceptive sites, but provides consistency, helping businesses protect their brand and users from being scammed with an added level of online differentiation.

Windows Internet Explorer 7 provides a visual trust indicator upon the presence of an EV certificate. Utilizing the well-understood traffic light paradigm with "green" inferring to proceed or "go", users are presented with a lock and green Address Bar that includes the name, the country of operation and address of the company that controls the site. EV SSL certificates are supported by Internet Explorer 7 on Windows XP SP2, Windows Server 2003 SP1 and Windows Vista.

EV SSL certificates are useful to any company and brand conducting online commerce who desires to protect their brand from deceptive exploits. According to the Netcraft Secure Server Survey, through December 2007 EV SSL certificates were deployed on nearly 4,000 consumer and ecommerce sites owned by Alaska Airlines, AutoZone, British Airways, eBay, FedEx, PayPal, Microsoft, Royal Doulton, The Body Shop UK, and Travelocity. In addition, leading financial services who are realizing the benefits of EV SSL certificates include the Banque National du Canada, Charles Schwab, Deutsche Bank, SunLife, Sovereign Bank, UBS, and Vanguard.[1]

This guide is designed to help businesses understand the value of EV SSL certificates, and offers a review of the steps required to obtain one. For technical implementation information, visit http://download.microsoft.com/download/b/d/9/bd9ab0f2-35b7-4e03-86df-ddb710fa7abc/IE7%20EV%20implementation%20guide%20v1.doc.

Threats to Online Safety

Data and identity theft represent a continuing threat for online users and businesses. From the consumer perspective, the issue is finding ways to help prevent the unintentional disclosure of personal data. Businesses are faced with phishing attacks that prey on their customers and attack their brand reputation. Internet Explorer 7 provides several optional solutions to these challenges through the Microsoft Phishing Filter and support for EV SSL certificates.

The Microsoft Phishing Filter provides protection against sites trying to trick users into entering their personal information. The Phishing Filter combines local heuristic page analysis with an online URL reputation service. As users navigate online, the Phishing Filter is able to warn against suspicious pages – or entirely block known Phishing sites. Today, on a weekly basis, this technology blocks nearly 1 million attempts to visit confirmed phishing sites, protecting over 200 million users of Windows® Internet Explorer® 7, for Microsoft Windows® XP Service SP 2 and Windows Vista™.

The Microsoft Phishing Filter is an opt-in service that operates in the background and provides a warning to users of both suspicious web sites that could be engaging in identity and data theft, as well as those confirmed to be phishing sites. It relies on browser-based heuristics to analyze Web pages in real time and warn users about suspicious characteristics as they browse. This client-side technology is combined with centrally managed and dynamically updated information to help keep users safe from known phishing sites, while maintaining privacy controls on all PII transmitted. Microsoft works with a network of third-party data-provider partners and a community of users who provide information on potential and confirmed phishing sites to constantly populate the back-end data service. More information can be found at www.microsoft.com/safety/antiphishing

[1] Netcraft Secure Server Survey www.netcraft.com. A listing of leading brands who have adopted EV SSL is published at www.aotalliance.org/resources/ev

Business Value of EV Certificates

Online businesses have long benefited from the security protection of SSL certificates. While SSL certificates help protect data in transit between browser and server, up to now there has not been a consistent process or procedure by which CAs validate the endpoint. Some traditional SSL certificates contain information about the server to which it is issued, but CAs lack consistent processes for validating the organization's identity.

Phishers have taken advantage of this deficiency and have been able to obtain 'valid' SSL certificates for their bogus sites. Users have become trained to rely on sites with SSL connections, and phishers rely on users not to look too hard when the gold padlock icon is presented.

Extended Validation (EV) refers to a new set of business process standards for validating the identity of a business and the authority of the individual requesting a certificate before issuing. The benefits to the adopting business include;

- Demonstrating that the site is highly authenticated and the identity of the domain is validated.
- Enhancing and increasing user confidence in online commercial transactions
- Reducing the risk and threat of phishing attacks.
- Demonstrating commitment to online security of customers
- Differentiating the domain and brands from other sites and online "copycats"

The CA/B Forum, a consortium of certification authorities, browser vendors and audit professionals have developed formal guidelines to mandate uniform business practices in issuing EV certificates. This process helps to ensure that the certificate subject is who it claims to be. Certification authorities that issue EV certificates have agreed to perform a consistent and rigorous set of steps to validate and verify the information provided by the business entity making the request for a certificate. CAs are audited annually by independent WebTrust auditors. Through this audit process, certificate integrity can be assured on every EV SSL certificate issued.

Like familiar SSL certificates, EV SSL Certificates are digitally signed, preventing usage if they have been modified. To help protect against the possibility of a certificate holder no longer meeting the criteria or being erroneously issued an EV certificate, CAs are required to provide certificate status information online. In addition, if a CA systematically fails to meet the EV guidelines, WebTrust and browser vendors may remove the CA from the certificate store at any time. Such action would disable the green address bar and all other visual trust indicators for their certificate.

Based on a review of these checks and balances, EV Certificates are endorsed by leading non-profit organizations focused on online trust. These include the Authentication & Online Trust Alliance www.aotalliance.org and the Merchant Risk Council www.merchantriskcouncil.org.

Primary Purposes of EV SSL certificates:

1. Identify the legal entity that controls a web site.
2. Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a 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
3. Facilitate 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 website.

Secondary Purposes

To help establish the legitimacy of a business claiming to operate a website and to provide a vehicle to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

1. Make it more difficult to mount phishing and other online identity fraud attacks using SSL 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 and their legitimate websites to users; and
3. Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the imposter.

Limitations

EV Certificates focus only on the identity of the company named in the Certificate, and do not assert to the business practices or reputation of the company including but not limited to:

1. Whether the site is actively engaged in doing business;
2. Whether it complies with applicable laws;
3. Whether it is trustworthy, or reputable in its business dealings; or
4. Whether it is “safe” to do business with the site.

How Internet Explorer & EV certificates work

EV certificates address security issues by enforcing certificate process enhancements. For web site and domain holders, EV certificates require just a small time investment to implement and deploy. For users of Windows Vista no client changes are required. EV certificates represent no increase in encryption strength or additional key length, nor make it harder to crack the content of an SSL transaction. As such they do not require more server processing time,

additional SSL accelerators or user PC resources. For users of Windows XP, users must enable the Microsoft Phishing Filter or the server Certificate Revocation Check.[2]

IE7 will display a number of *EV indicators* when a valid EV certificate is provided by the website, (see Figure 1). Specifically:

1. The background of the address bar changes to Green
2. This SSL padlock is displayed in the new Security status bar, located in the right portion of the address bar.
3. The Security status bar alternates between two different displays:
    a. The name of the legal entity which controls this website, along with the name of the country identified as their place of business in the EV SSL Certificate.
    b. The identity of the CA issuing the EV SSL Certificate.

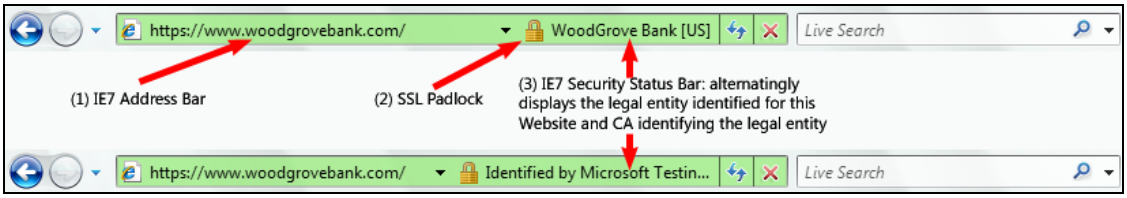

Figure 1 Internet Explorer 7 Address and Security status bar

The Security status bar also provides an easy way for users to view more information (see Figure 2). Hovering the cursor over the Security status bar highlights the area and a pop-up is displayed with more information about the EV SSL Certificate. Clicking on the Security status bar will bring up the security report window containing more detailed information from the certificate.

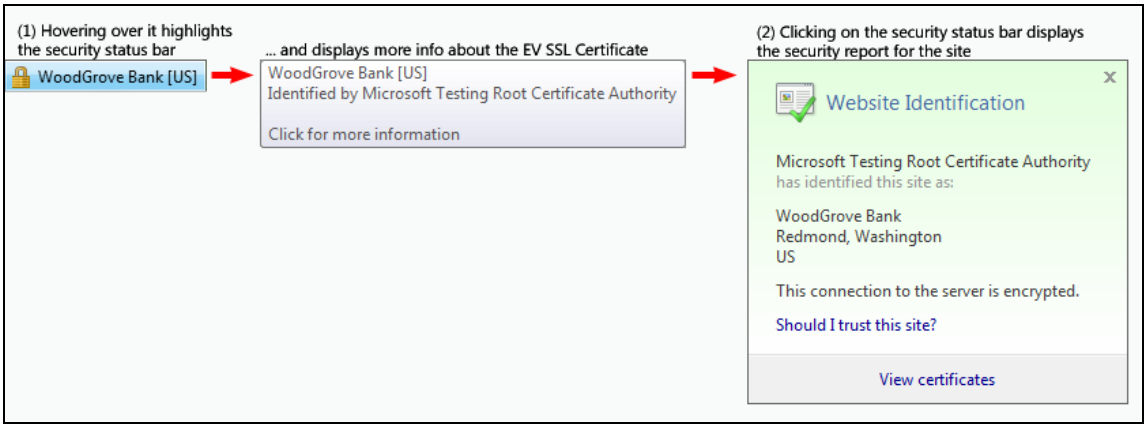

Figure 2 Security status bar and security report

[2] Microsoft has created a deployment guide to help ensure all Windows users are able to properly display your EV certificate http://download.microsoft.com/download/b/d/9/bd9ab0f2-35b7-4e03-86df-ddb710fa7abc/IE7%20EV%20implementation%20guide%20v1.doc.

Getting started with EV

The first step to getting up and running with EV certificates is to apply for one from an issuing CA. Today nearly 30 CAs worldwide are actively selling EV certificates. While standard domain-validated SSL certificates may be obtained within hours, businesses should plan for a minimum of 5-10 business days to obtain an EV certificate.

The process for obtaining an EV certificate should be similar from one CA to another with some variations based on business entity type and jurisdiction of incorporation. Applicants need to complete additional steps in the paperwork process such as providing details about the corporate structure, incorporating locale, corporate officers and other entity related details. In addition, administrators will need to create a certificate request, following the same process used for SSL certificates. Once the validation process has been completed and the CA has verified the information, it will sign the certificate request using the CA EV root certificate.

Organizations which may qualify for EV Certs include privately held and public business, non-profits and governmental organizations. In applying for your EV certificate, some or all of the following may be required by your CA for verification:

1. Proof of business incorporation / certificate of incorporation including
    a. Applicant's jurisdiction of Incorporation.
    b. Proof of legal existence
    c. Phone number of business
    d. Verified physical address, phone of business presence, (PO boxes are not accepted)
2. Notarized documents including governmental issued personal identification of Principal.
3. Third party validation of all documents
4. Verification of Applicant's control of domain name(s), via the Internet Corporation for Assigned Names (ICANN) and data in the public "Who Is" data base, showing the physical address and name of the administrative contact for the organization.
5. Corporate officer or business Principal must confirm claims made in EV application.
6. Verification that the Applicant and contract signer are authorized agents of the Applicant, including a legal opinion, accountant letter and or corporate resolution.

For a comprehensive list of EV Cert criteria, contact your CA or visit the CA/B Forum web site at www.cabforum.org. EV Certificate guidelines may be found at www.cabforum.org/EV_Certificate_Guidelines.pdf

Summary

EV certificates are designed to provide solutions to help both consumers and businesses combat online threats. An EV certificate contains verified information about the legal entity behind a website, allowing users to make better trust decisions about whom they are transacting with on the internet. Because the entity verification process is uniform across all issuing CAs, users should become more comfortable trusting a site that displays the Internet Explorer 7 EV indicators or similar indicators in other browsers.

Business and users are encouraged to deploy Internet Explorer to maximize online safety including dynamic anti-phishing protection via the Microsoft Phishing Filter, support for EV Certificates, product support and other privacy and security enhancements.

Resources

Internet Explorer 7	www.microsoft.com/ie
Microsoft Online Safety Strategy	www.microsoft.com/safety
Microsoft Windows Vista	www.microsoft.com/vista
Consumer Advice	www.microsoft.com/protect
Microsoft Phishing Filter	www.microsoft.com/safety/phishing
Sender ID Framework	www.microsoft.com/senderid
Microsoft Security Resources	www.microsoft.com/technet/security/tools www.microsoft.com/security
Anti-Phishing Working Group (APWG)	www.antiphishing.org
Authentication & Online Trust Alliance (AOTA)	www.aotalliance.org/resources/ev
CA/B Forum	www.cabforum.org
Merchant Risk Council (MRC)	www.merchantriskcouncil.org

R1-16