

The New EV\* SSL Certificates -  
Improve revenue and profits.

Let us show you how.

**Identity & Trust Assurance in a changing  
standards environment.**

\*(Extended Validation)

# Introduction

Today, online commerce is worth an estimated US \$1 trillion and continues to grow at a substantial rate. SSL Certificates have become a cornerstone of this e-commerce engine because they help establish trust when doing business online. SSL Certificates help consumers assess whether:

- a site is safe to shop from
- they are at risk for identity theft
- a merchant is trusted to take payments
- this is the company it claims to be

Therefore, while SSLs provide the security infrastructure upon which much of online commerce rests ... it is important to understand how SSL Certificates are changing and what it means for your business. Comodo can help secure your business today while protecting your SSL investment for tomorrow.

## Putting trust back in online commerce.

The growing use of the Internet for commerce, communication and collaboration has significantly increased the need for online security. Certification Authorities (CA) like Comodo and VeriSign provide a key link in the Internet security chain since a Certification Authority acts as a trusted third party whose purpose is to securely sign Certificates for entities it has authenticated using secure means.

CAs require highly evolved infrastructure and business processes to manage complex and variable environments including PKI services, validation processes, customer support, evolving security threats, database management and monitoring, user authentication and vulnerability identification and remedy. Further, these systems must support diverse stakeholder groups - consumers, enterprises, ISP's, browser providers and government agencies. Therefore, CAs like Comodo are a key advocate for consumer security and safety.

However not all CAs provide SSL certificates with identity assurance. It is for this reason that Comodo initiated the creation of a "trust" consortium comprising of leading browser providers (such as Microsoft) and other CAs. The purpose of this consortium, the CAB Forum (Certification Authorities and Browsers) is to identify and remedy current and emerging threats. The first and most urgent task this working group addressed is the difficulty of establishing identities in online interactions.

## The commercial dangers of weak validation

Establishing trust online is first about establishing identities – user to the site and vice versa. A user, presumably, can verify the site's identity by looking for the gold padlock on a website. But today all padlocks look the same despite the fact that there are two types of Certificates providing significantly differing levels of trust associated with the lack of identity authentication.

The first type of SSL Certificate is called a High Assurance SSL Certificate. This Certificate requires at a minimum of two step validation process:

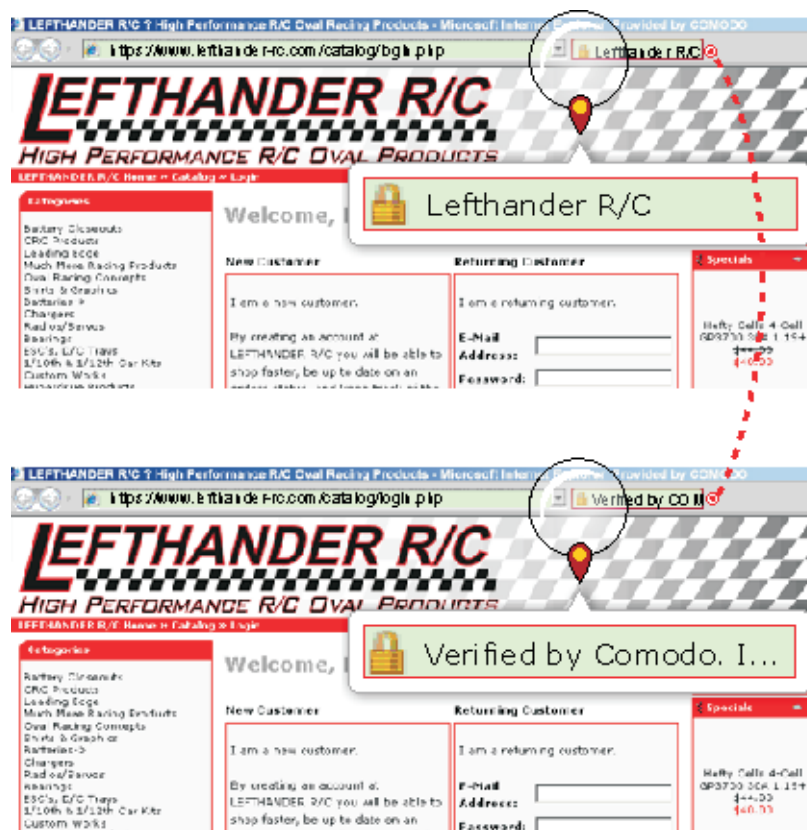
**Step 1:** Verify that the applicant owns, or has legal right to use, the domain name featured in the application.

**Step 2:** Verify that the applicant is a validly existing and legally accountable entity.

The second type of SSL certificate skips the second step, e.g. business identity validation step. These SSL Certificates are considered Low Assurance and do not authenticate identities nor protect consumers against phishing attacks. These “weak” validation Certificates rely only on the Domain Name Registrar details to validate ownership of a domain, which can be purchased by “who knows who”. Companies using weakly validated certificates risk losing the trust of customers who rely on SSL certificates to reassure them that the company behind the site is who it purports to be. Without such reassurance, customers will go elsewhere to conduct their business.

## But new standards will provide better consumer protection.

Until now, because of browser protocols, phishers could apply a padlock onto fraud sites through easily procured Low Assurance SSL Certificates. To close this security gap, Certificate Authorities (CAs) and browser vendors are fighting back by giving consumers the means to distinguish between EV Certificates and domain only validated Low Assurance Certificates. Importantly, in web browsers such as Microsoft Internet Explorer 7.0, Firefox 3.0 or Opera 9.5 users will see the address bar turn green when they visit a website secured with a high assurance EV SSL Certificate.. A display next to the URL will toggle between the organization name and the Certificate Authority that issued the SSL Certificate. The green bar means that a third party has validated the existence of the business, the business's right to use the domain name, and the EV SSL Certificate was appropriately obtained. All other major browsers will be also adopting similar green visuals to enable visitors to distinguish between EV SSL certificates and all other SSL certificates.



# Extended Verification (EV) Certificates:

## Increased Protection = Increased Trust = Increased Revenue

Study after study confirms that trust is the differentiator between profits or losses ...

- 70% of online shoppers have abandoned an online purchase because they didn't get a sense of security during payment part of process
- 90% of those shoppers report that they would have completed the transaction had trust been established through a trustlogo

(Source: TNS Research, April 2005).

## Extended Validation (EV) SSL Certificates A new standard to achieve a new level of trust

SSL certificates are a critical building block for secure electronic commerce and one of the ubiquitous uses of public key infrastructure (PKI). SSL certificates provide four security functions:

- Authentication: SSL certificates verify that the business or organization with whom the user is communicating really is who it says it is, and not an impostor. EV SSL Certificates create a greater level of confidence than any other type of SSL certificate.
- Confidentiality: SSL certificates enable secure sessions with a web site so that information provided over the Internet by the user cannot be intercepted in transit.
- Integrity: SSL certificates ensure that messages are not altered without detection.
- Non-repudiation: SSL certificates ensure that the sender and recipient of an electronic message or transaction cannot deny sending or receiving the message or engaging in the transaction.

## EV Certificates in action

If your site's identity authentication can be prominently displayed while a competitor's site cannot, you will be more trusted. This competitive advantage translates into reduced visitor abandonment rates, improved conversions, higher revenue per transaction and higher lifetime customer value. In the world of e-commerce, establishing trust is mission critical because, when consumers trust you, they can confidently transact with you online.

# The New EV SSL Certificate

## Here are the facts:

You must have an SSL certificate on your website to enable your customers to securely conduct business transactions with you online.

- The new class certificates, EV (Extended Validation) SSL certificates has been introduced to the market, ..and web browsers such as Microsoft IE 7.0, Opera 9.5 and Mozilla Firefox 3.0 will provide consumers with this new color-coded user interface. This highly visible green trust indicator will show to consumers that your business and your data encryption capabilities have been authenticated according to the new EV guidelines.
- EV SSL certificates are base on an industry wide approved standard of validation so that web browsers can let consumers instantly tell the difference between a website whose identity has been fully authenticated and other types of SSL certificates.

When your site is secured with a new EV SSL certificate, the IE 7.0, Firefox 3.0 or Opera 9.5 address bar will visibly turn green when consumers visit your web site. So start earning the trust of your customers right away.

To learn more about EV SSL certificates please visit [www.evsslcertificate.com](http://www.evsslcertificate.com).

# FAQ for EV reference website

## **Q:What is SSL?**

**A:** Secure Sockets Layer (SSL) is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

When you choose to activate SSL on your webserver you will be prompted to complete a number of questions about the identity of your website (e.g. your website's URL) and your company (e.g. your company's name and location). Your webserver then creates two cryptographic keys - a Private Key and a Public Key. Your Private Key is so called for a reason - it must remain private and secure. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file also containing your details.

Your webserver will match your issued SSL Certificate to your Private Key. Your webserver will then be able to establish an encrypted link between the website and your customer's web browser.

In this context, SSL can be thought of as the security "platform" for e-commerce.

## **Q:Why are High Assurance SSL certificates the Standard for establishing Trust in e-business?**

**A:** Safety on the net is essential, but most consumers don't know how to tell a secure site from one that is not. They do, however, know to look for a padlock, which is the sign of the site being SSL-secured. A site that does not show an SSL Certificate is not likely to do much e-commerce business.

## **Q:What is an EV (Extended Validation) SSL certificate?**

**A:** Extended Validation (EV) SSL certificates are the next generation SSL certificate because they work with high security Web browsers to clearly identify a Web site's organizational identity. For example, if you use Internet Explorer 7.0, Firefox 3.0 or Opera 9.5 the address bar will turn green to identify this site as having an EV SSL certificate. It will also display the padlock as an icon of trust. However, the address bar will not turn green if the website does not have an EV SSL certificate.

## **Q:Is Extended Validation a new Standard?**

**A:** Yes, it has been introduced to protect your website against phishing and other fraudulent activities in the online world. Since most Internet crimes rely on false identity, EV certificates require that organizations go through a rigorous validation process that meets the Extended Validation guidelines established by the CA/Browser Forum to combat these threats. In addition to confirming domain name ownership, the process includes authenticating the authority of the contact person requesting the certificate, verification of the business with government or third party business registries, and other methods to assure the legal and physical existence of the business.

## **Q:What kind of information does the EV SSL certificate display?**

**A:** Identity confirming company information will include, but is not limited to: company name, domain name, government business registration number, business address.

## **Q: Why has this become necessary?**

**A:** Unfortunately, not all SSL certificates are equal. Until now, consumers could not easily tell the difference between SSL certificates that provide extensive identity authentication from certificates that provide only domain validation with virtually no identity verification. It became necessary to give consumers the means to do intelligent risk assessment about with which online merchants they will transact business. Consumers need to verify the identity of online businesses, not just their domain names.

EV SSL certificates are the most technologically advanced SSL certificates from Comodo for allowing your customers to verify your identity. Comodo has positioned itself to help e-merchants become trusted by their customers through Comodo's EV SSL certificates.

## **Q: Who is defining the new guidelines for these Extended Validation SSL Certificates?**

**A:** The guidelines for the new EV SSL certificates are being defined in an industry-wide association called the CA Browser Forum. Comodo saw the upcoming need for defining an industry wide standard and initiated the CAB Forum in May 2004. Forum members are browser companies including Microsoft, Mozilla, Opera and Konqueror (KDE) in partnership with Certificate Authorities including Comodo, VeriSign, RSA, with participation from other organizations representing banking and lawyer associations.

## **Q: Terms like “High Assurance”, “Extended Validation”, “Domain only”, “Low Assurance” and “Enhanced Validation” are all being used in describing different types of SSL certificates. What's the difference between these SSL certificates?**

**A:** The main difference between all these certificates is the level of identity verification as follows:

- “Domain only” certificates, also known as “low assurance” certificates, only verify domain ownership. These are certificates most often sold by GeoTrust and GoDaddy. Unfortunately, these certificates provide virtually no identity assurance whatsoever since domain purchasing requires no identity verification.
- “High Assurance” certificates refer to certificates that include identity validation from a Certification Authority using currently established and accepted vetting processes. These SSL certificates are seen as significantly superior to domain only SSL certificates because users can trust that an objective third party a certification authority, has verified the identity of the website.
- “Extended Validation” (EV) SSL certificates are the newest option for eMerchants as these SSL certificates require the most stringent verification processes as outlined in the guidelines developed by CA/B Forum. The advantage of these the next generation high assurance SSL certificates is that these certificates work with the new security browsers to include a new visual indicator that confirm the site's identity.

## **Q: How will EV SSL certificates increase consumer confidence?**

**A:** High profile incidents of fraud and phishing scams have made Internet users very concerned about identity theft. Before they enter sensitive data, they want proof that the website can be trusted and their information will be encrypted. Without it, they might abandon their transaction and do business elsewhere. EV SSL Certificates provide third-party verification using a highly visual display that gives consumers confidence and builds trust in e-commerce.

## **Q: How is a consumer expected to distinguish between the different type of SSL certificates?**

**A:** The presence of a verifiable High Assurance SSL certificates provides reassurance to consumers. Low assurance certificates, by contrast, are not inherently trusted by browsers and will cause some browsers to display “warning messages” informing the user that the certificate has not been issued to a verifiable entity. Loss of trust equals loss of sales whereas increased trust results in increased sales.

### **Q:What are the benefits of EV SSL certificates to Web site owners?**

**A:** An EV SSL Certificate helps visitors complete secure transactions with confidence because your site has the “green bar” in IE 7.0, Firefox 3.0 or Opera 9.5 whereas your competitor's site does not. You appear to be more trusted and more legitimate. That's a competitive advantage that translates into higher conversion and more revenue. And it's why you are in business.

### **Q:Why do I need an EV Certificate on my site?"**

**A:** Today's fastest growing threat is phishing, where a fraudulent web site impersonates a legitimate business to attract unsuspecting visitors into divulging personal information. The increasing awareness to this problem has caused consumers to not trust buying online.

To stem this erosion of trust, EV SSL certificates, for the first time, let customers visibly see that they are doing business with an identity verified business. Using an EV SSL certificate will assure them that your website really is who it claims to be. (Now verifiable directly by the browser)

### **Q:Why does the whole high or low assurance matter to my customers?**

**A:** Online businesses need a way to make customers feel as comfortable buying online as they would if they were making a purchase in a store. With the release of web browsers such as Internet Explorer 7.0, Opera 9.5 and Firefox 3.0 that displays a green address bar of a EV SSL secured site, a visitor can easily verify your identity. Be sure your site does not lose sales because of the new browser displays.

### **Q:Will I be able to upgrade my existing Comodo High Assurance SSL certificate to get a green bar in the Browser?**

**A:** Sure. Comodo can offer you a quick migration path from your existing High Assurance SSL certificate. To learn more go to <http://www.instantssl.com/ssl-certificate-products/ssl/ssl-certificate-evssl.html> or call + 1.800.758.1669.

### **Q:Are EV SSL Certificates available for purchase now?**

**A:** Not yet but very soon. That's why Comodo is helping you get ready now so these new EV SSL certificates can start helping you make more money when they do become available early next year.

### **Q:Is my existing High Assurance SSL certificate still sufficient for protecting online transactions?**

**A:** SSL certificates will continue to provide security encryption to make sure that data being transferred between your website and the browser can not be stolen And, your current high assurance SSL certificate will continue to be viewed as an identity assurance certificate far superior to low assurance or domain only validated certificates. What varies is the level of identity assurance that comes with these SSL certificates The new EV certificates provide a browser based confirmation only to users who have the new browsers. However, today and in the future, your high assurance SSL certificate still provides excellent identity assurance to users who do not have the "EV enabled" browsers yet.

To learn more about EV SSL certificates, please call + 1.800.758.1669 or visit [www.evsslcertificate.com](http://www.evsslcertificate.com) .

# About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. With global offices in the US, UK, Ukraine and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital ecommerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo - Creating Trust Online™

## **Comodo Credentials Serving and securing over 200,000 customers worldwide including:**

- 7 of the top 10 Fortune 1000
- 5 of the top 7 leading U.S. universities
- Top 2 U.S. automotive manufacturers
- Top 2 global software providers
- Top 3 global wireless providers
- Top 2 U.S. military manufacturers
- Leading multi-national companies such as NASA, Xerox, SONY Europe, GE, Kaiser Permanente, BASF, Deutsche Bank AG and U-Haul
- Portfolio of 10 Public root certificates under direct ownership
- Fully automated process for certificate issuance with unlimited re-issuance policy
- Virtually universal browser ubiquity (99+%) with 128/256 bit industry standard encryption and up to \$1million USD warranty
- SGC (Server Gated Cryptography) certificates to enable older system to achieve 128-bit equivalent encryption
- First to market with Multi-Domain SSL certificates specifically addressing the multi-domain needs of the enterprise
- A fully WebTrust compliant CA the highest globally recognized standard and a member of the Microsoft Root Certificate program

### **Comodo**

525 Washington Blvd.,  
Jersey City, NJ 07310  
Tel : +1.888.COMODO.1  
email : sales@comodo.com

[www.comodo.com](http://www.comodo.com)

### **Comodo Group**

3rd Floor, 26 Office Village,  
Exchange Quay, Trafford Road,  
Salford, Manchester M5 3EQ,  
United Kingdom.  
Tel Sales: +44 (0) 161 874 7070  
Fax Sales: +44 (0) 161 877 1767