Extended Validation (EV) SSL Certificates

Key to Online Success for you and your customers

COMODO
Creating Trust Online®

Extended Validation (EV) SSL Certificates
Key to Online Success for you and your customers

COMODO
Creating Trust Online®

- EV SSL certificates are a new industry standard for identity assurance and authentication
- A green trust indicator in the web browser illustrates that this website has been validated against the highest standards
- Extended validation certificates allow you to offer a premium SSL service to your customers

EV SSL certificates are more then a revenue opportunity – they are an opportunity to Create Trust Online™.

EV SSL Certificates - a solid foundation for Online Business

The aim of EV certificates is to reduce the amount of online fraud

High Assurance SSL certificates in general protect users from doing business with unauthenticated web merchants. EV SSL certificates are the new type of High Assurance SSL certificate that provide rigorous and standardized authentication for a business' identity. This Extended Validation (EV) will only be given to online businesses that can be verified through secure authentication processes that meet the extended validation guidelines established by the CA/Browser Forum. The validation process includes, for example, rigorous vetting procedures for:

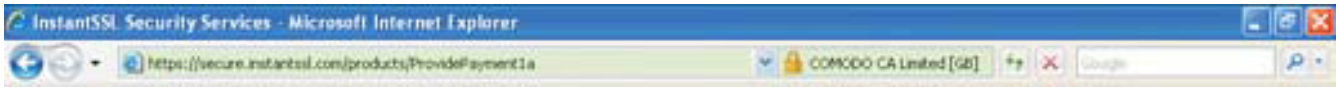
- Government registration
- Trading name
- Type of business
- Place of business - full address
- Management Contacts

In addition to confirming domain name ownership, the process includes authenticating the authority of the contact person requesting the certificate, verification of the businesswith government or third party business registries, and other methods to assure the legal and physical existence of the business.

What's new about these EV SSL certificates?

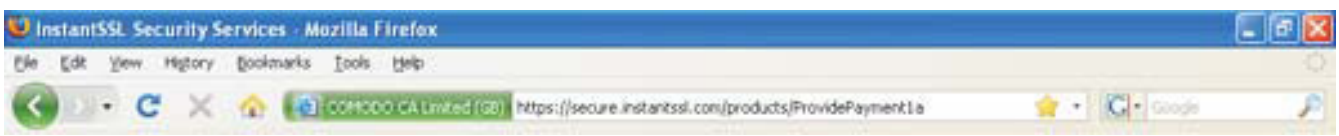
To indicate websites that have undertaken this strict examination of business identity, most major browsers will give these sites a prominent visual display, such as turning the address bar green.

Microsoft IE 7.0 address bar for a site with an EV SSL (showing the identity of the site from the SSL Certificate)



*phishing filter needs to be turned on

Mozilla Firefox 3.0 address bar for a site with an EV SSL



Opera 9.5 address bar for a site with an EV SSL

If a business identity on a website can be verified (and a competitor cannot) customers are likely to trust this site more. 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 you win your customer trust, you win their business.

Why EV SSL Certificates have become necessary

Cheap domain only validated certificates provide no authentication and without authentication a fraudster can easily mock a website identity

Online trust has eroded significantly in the past two years according to analyst reports, with threats of phishing and pharming growing each day. In fact, a Gartner study recently reported that 20% of all consumers will not do business online at all. To date, security responses to online fraud have been ineffective, reactive and based on old tools which are becoming more vulnerable.

The most common way e-commerce sites and consumers protect themselves against fraud is to rely on server certificates (SSL or Secure Socket Layer certificates) issued by public certification authorities (CAs). These Certificates verify the organization's existence, the organization's right to use the domain name included in the certificate, and the authority of the requester to obtain a certificate on behalf of the organization. Such certificates used to afford a satisfactory level of assurance by enabling three security services - confidentiality, authentication, and integrity.

However, with the rise of a new business model for SSL certificate issuance, some CAs have started to issue server certificates without authenticating the subscriber, thereby providing only two of the three security services - confidentiality and integrity. Further using current browser technology, it is very difficult for an internet user to distinguish between higher- and lower-assurance server certificates.

Comodo identified this breakdown in online authentication and two years ago Comodo called for the creation of the CA/B Forum, a consortium of leading certification authorities and browser providers including Microsoft, Comodo, Mozilla, Opera and VeriSign to develop next generation solutions to address emerging trust threats on the internet. The creation of EV SSL certificates is currently the first result of that effort and they were created to protect users from doing business with unauthenticated web merchants. Through rigorous guidelines, specifications are being created that standardize online identity verification process among CA's so that consumers can now easily know who they are doing business with.

Extended Validation (EV) SSL Certificates

Who owns www.abc-company.com? and who owns www.abccompany.com? Only improved identity vetting can tell.

SSL certificates are a critical building block for securing electronic commerce and one of the ubiquitous uses of public key infrastructure (PKI). SSL certificates provide three security services-confidentiality, authentication, and integrity so that users can:

- Securely communicate with a Website so that information provided by the internet user cannot be intercepted in transit (confidentiality)
- Or altered without detection (integrity)
- Verify that the internet user is actually at the company's Website and not an impostor's site (authentication).

This latter point is fundamental to understand the need for EV SSL Certificates. With the proliferation of low assurance, domain only verified SSL certificates, there was no assurance that a certificate that could verify organization "ABC Company, Inc.". The user has no means to find out that ABC Company, Inc. is the legitimate owner of an Website named www.abc-company.com or come to the conclusion that the site: www.abc-company.com is just a fake. Without this authentication security, phishing can emerge and phishers trick unsuspecting Web surfers into doing business with someone pretending to be ABC Company, Inc.

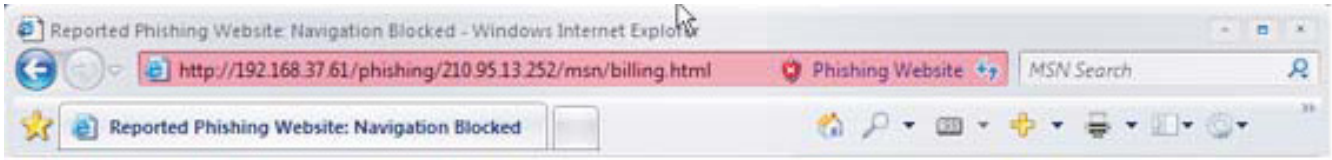
EV guidelines will provide better consumer protection and better trust credentials

With EV certificates your customers can achieve the same visible trust level as big online merchants

Untill now, because of the way SSL sessions have been displayed in browsers, phishers could potentially apply a padlock onto fraud sites through easily procured Low Assurance SSL Certificates. To close this security gap, Certificate Authorities (CA's) and browser vendors have taken action by giving consumers the means to distinguish between businesses validated High Assurance Certificates and domain only validated Low Assurance Certificates.

For example, in Microsoft Internet Explorer 7.0*, Mozilla Firefox 3.0 or Opera 9.5 browsers, users will immediately see the address bar turn green when they visit a Web site secured with an EV SSL. A display next to the URL will toggle between the organization name and the certificate and the Certificate Authority that issued the SSL Certificate. The green bar means that a third party has validated the legitimacy of the business, the business' right to use the domain name, and the High-Assurance SSL Certificate was legitimately obtained.

Microsoft IE 7.0 address bar for a known phishing website detected by the Phishing Filter.



Microsoft IE7 address bar for a site with a high-assurance SSL certificate
(showing the identity of the site from the SSL certificate)

*phishing filter needs to be turned on

Firefox 3.0 address bar for a site with an EV SSL

Extended Validation (EV) SSL Certificates
Key to Online Success for you and your customers

COMODO
Creating Trust Online®

Opera 9.5 address bar for a site with an EV SSL

Why should your customers upgrade to EV SSL Certificates?

Is a Comodo High Assurance certificate not good enough?

SSL certificates in general will provide security by encryption to make sure that data being transferred between your website and the browser can not be intercepted. Current Comodo high assurance SSL certificates will continue to be viewed as an identity assurance certificate far superior to low assurance or domain only validated new certificates. However Web surfers will not see a green bar. This is reserved for certificates that have been issued based on the new industry wide EV standard.

Comodo customers can benefit from the previous High Assurance validation process and an upgrade to EV will be almost as cost effective as buying an additional trust seal for their sites but far more effective.

An Upgrade to EV is almost like **moving a shop from a back street to a high traffic street.** Now your customers can be as trusted as Amazon and ebay.

What's the benefit for you?

You will be the first to help your customers upgrade to EV SSL certificates - and you'll be ready with Comodo behind you.

Being able to sell EV is a quality indicator to your business, not all SSL resellers will qualify - only the ones that can prove that they have access to extended validation resources such as the background infrastructure that Comodo provides for you.

As our valued partner you will be among the first to be validated. If you want to become part of our EV campaign, Comodo will provide you with free* EV SSL certificate for your online shop so that your customers can see what they will get.

* Partner band 3 minimum deposit = $5000 within the last 6 month required/ To qualify legally you need to be incorporated .

Above this you can benefit from the high retail price for EV SSL certificates and strong wholesale margins. Selling EV certificates will significantly increase your revenue per customer.

3 Ways to make money - The Comodo's SSL Certificate Portfolio:

The Right SSL Portfolio For All Your Customers' Needs

Comodo, the World's 2nd largest Certification Authority, offers every type of SSL certificate so you have more opportunities to meet the needs of your customers. All at prices that are designed to give you the best opportunity to drive revenue and margins. Sell certificates equivalent to VeriSign - but buy them at a fraction of the price. Increase your competitiveness by cutting prices or simply enjoy higher profits.

Your benefits are:

- Our product collateral makes it clear to end users why they should consider moving to higher priced certificate
- Comodo operates the entire backend issuance process including validation

Extended Validation (EV) SSL Certificates
Key to Online Success for you and your customers

COMODO
Creating Trust Online®

- Buy your certificates in volume and realize even greater profit margins
- Minimum buy price - maximum potential
- Easy upsell of customers
- No set up, no overhead, no hassle
- Huge discounts on volume purchases
- Easy provisioning

Comodo SSL Portfolio

Even though our SSL certificates offer the most popular features, they are the most cost effective in the market. Comodo offers the widest portfolio of SSLs for different client types - so you have something to offer all your customers.

Comodo is the second largest Certification Authority - **a name your customers can trust.**

Products	Description	Best used for	Ideal customer segment
Positive SSL	Provides data security quickly	Low volume E-commerce transactions. Ideal for securing Intranet/Extranet	Secure data storage and exchange; Websites with low value transactions
InstantSSL / Enterprise SSL	Provides transaction security and authentication	Leading E-commerce enabled websites conducting high volume / high value transactions	One product shops up to High Traffic websites
EV SSL Certificate	Provides high transaction security authentication and most compelling Identity assurance	Trustworthy E-commerce transaction protection from medium to high Volume	High profile websites and sites that benefit for visible authentication

Getting more into detail

What are the differences between the different SSL types?

SSL Type	Positive	Instant/Enterprise	EV
Max Duration	10 year	3 year	Max 2 years
Revalidation needed	When reissued	When reissued	When additional certs are issued 12 months after the initial EV cert was issued!!
Vetting process	Web only	Web + Fax + phone	Web + Fax + Phone Qualified 3rd Party source (databases) or legal letter or site visit in some cases Any step relies on 3rd party data or legal opinion
What needs to be validated	Domain Control - specifically the ability to *receive an email* at the chosen domain	Domain Ownership (Our high assurance validation involves humans looking at whois and matching this up with supplied documentation / databases. This is the differentiation between the terms 'ownership and control') Physical Address Legal existence as a business	Domain Ownership Physical address Legal existence as a business Identity of involved persons
Roles involved (all roles can be on person)	Requester	Requester and signer	Requesters Approver Signer
Documents needed	None	Business License Articles of Incorporation Major Utility Bill	EV Cert request Subscriber agreement Document that proves legal and physical existence All Information needs to be validated against a Qualified 3rd party source
Validation can be done by	Automatic	One person	Two people

SSL Type	Positive	Instant/Enterprise	EV
Certificate contains	Domain Name	Domain name Requesting company/individual Physical address (city/state/country)	Domain name organisation name Jurisdiction + registration Number Physical address (city/state/country) street optional
Minimum Cryptographic Requirements	40 bit encryption	40 bit encryption	SHA 1/ 128Bit or higher RSA 1024 (until Dec 2010)
Time to issue	Minutes	Hours	Days
Wildcards	Yes	Yes	No
Insurance	none	From $ 10,000- Up to 1,000,000	$1,000,000 + more

Questions your customers may ask

A) Why should I buy EV it is more expensive and does not give me more protection?

EV doesn't give you more protection it protects your customers better. Not only do customers know they are connected to a trustworthy website, but with EV SSL certificates, the new browsers will confirm it. If you compare the cost for the upgrade versus what you would have to pay for an Google ad, an EV SSL is money well spent as it increases conversion rate among first time customers.

B) Why not buy from Verisign?

Because in 2006, for the first time, Comodo exceeded all other CA as the "most sought after brand" according to recent search engine trend reports. How's that? Because now more than ever, consumers are using our desktop security products to protect their Pcs.

All this trust translates into greater trust in YOU when they see a Comodo site seal on YOUR site.

And Comodo has one of the most advanced processes in place to assure the highest standards in EV SSL issuance. Comodo has years of experience in identity vetting and we can guarantee you one of the most hassle free process in the industry.

Extended Validation (EV) SSL Certificates
Key to Online Success for you and your customers

COMODO
Creating Trust Online®

FAQ's

Q: What is an EV (ExtendedValidation) 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 Website'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 identity 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 SSL certificates a new standard for online identity assurance?

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 SSL 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 part of a portfolio of SSL certificates that 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 2005. Forum members are browser companies including Microsoft, Mozilla, Opera and Konqeurer (KDE) in partnership with Certificate Authorities including Comodo, VeriSign and RSA, with participation by 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 so that the identity of the owner of the domain is verified.

"Extended Validation" SSL certificates are the next generation of SSL certificate because these new certificates must comply with industry recognized guidelines for identity validation. E-merchants that pass this validation process will be issued an EV SSL certificate. Unlike all other SSL certificates, these certificates include a new visual indicator built into many new and forthcoming browser versions 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 visible display that gives consumers confidence and builds trust in e-commerce.

Q: What are the benefits of EV SSL certificates to Website owners?

A: An EV SSL Certificate helps visitor's complete secure transactions with confidence because your site has the "green bar" in IE 7 and 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.

Extended Validation (EV) SSL Certificates
Key to Online Success for you and your customers

COMODO
Creating Trust Online®

Q: Why do my customers need an EV SSL certificate on their site?

A: The Internet has successfully created many new global business opportunities for enterprises conducting online commerce. However, that growth has also attracted fraudsters and cyber criminals. Today's fastest growing threat is Phishing. This is where a fraudulent website impersonating a legitimate business attempts to woo unsuspecting visitors into divulging personal information. The increasing awareness to this problem has presented an opportunity to e-commerce providers to capitalize on consumer fears by displaying trust indicators. Just like the real world, people need to be confident before they proceed down an unknown path.

Over the past 10 years, consumer magazines, industry bodies and SSL security providers have educated the market on the basics of online security. The majority of consumers now expect security to be integrated into any online service they use. As a result, they expect any details they provide via the Internet to remain confidential and integral. For many customers, the only time they will ever consider buying products or services online is when they are satisfied their details are secure. Using an SSL Certificate to secure your online business indicates to your customers you take their security seriously.

They will visibly see that their transactions are secure, confidential and integral and it gives them the confidence that you have removed the risk associated with trading over the Internet. Using a High Assurance certificate will also assure them that the website really is who it claims to be, now verifiable directly.

Q: What do these changes means to my customers' business?

A: Soon browser providers will allow consumers to distinguish between a High Assurance SSL certificate where the business identity was verified versus Low Assurance, domain only verified SSL certificates. Simply, once consumers can tell the difference between the "good, trusted" SSL Certificate from the "bad, untrusted" Certificates, consumers will show preference for sites that can be more trusted. Now one click from a customer will automatically reveal Certificate details and whether the business' identity has been validated or not.

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. So submit your contact information and we can make you an upgrade offer for $299.

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 SSLcertificates can start helping you make more money when they do become available early next year.

Q: How is a consumer expected to distinguish between these sites?

A: The presence of a verifiable Extended Validation 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.

Microsoft IE 7.0 address bar for a site with an EV SSL
(showing the identity of the site from the SSL certificate)

*phishing filter needs to be turned on

Mozilla Firefox 3.0 address bar for a site with an EV SSL
(showing the identity of the site from the SSL certificate)

Opera 9.5 address bar for a site with an EV SSL
(showing the identity of the site from the SSL certificate)

Q: What browser versions are compatible with EV SSL?

A: EVSSLcertificates are compatible with all major browsers including IE 7.0, Firefox 3.0 and Opera 9.5.

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

A: SSLcertificates 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.

Q: What browser versions are compatible with EV SSL?

A: EV SSL certificates are compatible with all major browsers including IE 7.0, Firefox 3.0 and Opera 9.5.

About Comodo

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internetconnected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and Email Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure email and fax services.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies asvital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

To learn more and purchase
EV Multi-Domain SSL certificates, please visit **www.comodo.com/evmdc**

Comodo Group Inc.

525 Washington Blvd.,
Jersey City, NJ 07310
United States

Tel : +1.888.266.6361
Tel : +1.703.581.6361
Email : sales@comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester
M5 3EQ,
United Kingdom

www.comodo.com