



EV (Extended Validation) SSL Certificates

February 2009

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



EV 'Extended Validation' SSL Certificates

Management summary

Two years after the launch of EV SSL Certificates mounting evidence suggests that EV SSL certificates help turn browsers in to buyers. Quite simply, you are losing business to competitors that use EV SSL technology if you don't – and this is equally relevant to transactional sites (eCommerce & on-line banking) and interactive sites where you have to identify yourself via registration page and then log-in page (On-line portals, gaming etc).

A green EV validated address bar does many things. It shows the customer that your site is not fraudulent, that you take security seriously and are doing everything you can not to let your customers personal or financial information be stolen. By making the investment in EV SSL technology you are proactively informing the customer that they are safe and you are doing your bit to keep them that way. (Before EV SSL green bar technology- the customer had to open up your standard SSL certificate and check out the company that issued the cert to you and then check what type of SSL you were using and whether checks were carried out by the issuing company to see that you were legitimate...a long winded and complicated process and yes you just lost another customer.)

EV certificates are bold and "in your face", they are easy to use and understand & provide a statement of fact and security; and the customer doesn't have to lift a finger to get this simple but important message.

All EV SSL Certificates have to conform to the EV SSL guidelines in form and issuance, written by the CA (Certificate Authority) Browser Forum. The aim of the EV SSL Certificate was to create an 'as near perfect as possible' SSL certificate to gain confidence of users visiting web-sites, and to differentiate web-sites from those protected by previous versions of SSL Certificates. EV SSL Certificates are backwardly compatible with older browsers, but do require the latest browsers (e.g. IE7, Firefox3) to have the full functionality including the green-bar user experience. EV SSL Certificates were also introduced to ensure that all CAs issued certificates to the same technical specification, and with the same due diligence procedures followed (& documented). An annual audit is undertaken in order for all CAs to retain their EV SSL certificate accreditation.

From a technical perspective, there is very little difference between an EV and a normal SSL certificate. The main difference is in the due diligence that is done by the CA before a certificate is issued, in that additional checks are done on the organisation & the people requesting the certificate. This will prevent EV SSL certificates being issued to fraudulent organisations, or phishing web-sites. From a user experience, the main difference is the address bar turning green, and the addition of an information bar rotating between the Legal organisation behind the web-site, and the name of the CA that issued the certificate.

There are 17 organisations world-wide that are accredited to provide EV SSL Certificates, whereas there are over 100 organisations world-wide that are accredited to provide normal SSL Certificates. The number of organisations accredited to sell EV SSL Certificates is unlikely to increase, primarily to ensure that the authorised CAs can be closely monitored to ensure they keep their accreditations.

The CA/Browser Forum is a group of certification authorities, web browsers, and other industry participants (such as legal and audit practitioners) that came together to look at ways to increase the

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



reliability of SSL as a protection against phishing and other Internet attacks. All certification authorities wishing to issue EV certificates must pass a special annual audit of their capabilities to reliably operate a public key infrastructure and to enforce the EV Guidelines. QuoVadis is a member of the CA/Browser Forum and contributed to the creation of the EV Guidelines, as did Microsoft, Mozilla, Apple and the top 17 certified CAs.

For any web-sites that are transactional, or interactive (e.g. sales, registration or log-in pages), on either a public facing or B2B site, an EV SSL certificate will give your visitors added confidence that they are authenticating to the correct site, and not a phishing site. What is also important is that you encourage your web-site visitors to use a secure browser, in other words a browser that is up-to-date. What you don't want is people using older browsers that have well documented security issues resulting in the browser security being compromised.

QuoVadis have a unique pricing policy which enables the purchase of pools of certificates which can be used up over multiple years. This, in essence, means that customers can take advantage of our volume pricing discounts. Additionally, QuoVadis are the only vendor that does not charge extra for using certificates in a load-balancing environment. As a result, for organisations running web-sites over a load-balanced environment of perhaps 4 or 5 servers, QuoVadis will offer very substantial savings.

What are EV SSL certificates?

Extended Validation or EV SSL certificates are a new generation of digital certificates.

SSL (Secured Sockets Layer) certificates are a core security reassurance tool to create trust and confidence online. However, as low assurance (domain validated) SSL certificates have been introduced to the market, it became clear that a new approach was needed to protect legitimate businesses from the erosion of that all important trust and confidence in customers caused by low assurance (domain validated) certificates.

Because there is no difference from the user experience of a low and a high assurance certificate the low-assurance certificates are often misunderstood by web-site visitors. If fraudulent/criminal people can purchase low-assurance certificates, how can the visitor be sure that they are actually at the site of a reputable organisation – and equally, how can they really know if there is a legal entity behind the web-site in question? And who that legal entity is? There are many fraudulent phishing sites that have domain validated certificates attributed to them – and although this does provide an encrypted session, it still enables web-site visitors to have their identity and/or money stolen through visiting & authenticating with fraudulent sites.

That is why browser providers such as Microsoft and Mozilla and certification authorities including QuoVadis have worked together throughout the last few years to create a new level of trust online through new browser based identity indicators. This group of organisations are known formally as the Certificate Authority Browser Forum or CA /Browser Forum.

Windows Internet Explorer 7 and the latest versions of the three other most popular browsers (Firefox, Safari and Opera) provide 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 location of the company that controls the site. If there are any problems with that certificate, or it is reported as a fraudulent site, then the address bar will be red. In time, ultimately, all previous

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



versions of SSL certificates are likely to give errors, but the timescale when this will happen is yet unknown.

EV 'Extended Validation' SSL certificates are designed essentially to increase trust and confidence in website visitors and encourage transactions and transmission of information through the welcoming and informative 'green' URL address bar. It is also designed to protect legitimate organisations who want to differentiate themselves from both competition and illegitimate organisations by showing that they are who they say they are, they have been tried and tested and care about their brand image and the protection of their customer information. They have been proactive in demonstrating a level of Corporate Social Responsibility by sourcing their secure certificates through one of the 17 members of the CA/Browser Forum who have had to go through rigorous tests and accreditations themselves in order to become accredited to supply EV SSL certificates.

Why did EV SSL certificates become available?

Many people identify SSL with encryption protection, but encryption is only part of what SSL certificates were intended to do. SSL certificates are also intended to validate a website's identity to site visitors. When a visitor opens a web page secured with SSL, the browser interface displays an identifier signifying that an SSL secured session has been initiated to encrypt all data transmitted through the web page and that the site's identity has been verified. The SSL session identifier in the browser window is traditionally a small padlock icon (either in the address bar or at the bottom of the browser) and an "s" added to the http in the address.

Traditional SSL is still quite adequate in some instances but there are chinks in its armour. Weak identity vetting and the obscurity of the browser interface for the end user undermine the effectiveness of some SSL certificates. Additionally it is impossible to tell the level of authentication that has been carried out with standard SSL certificates.

Identity validation for traditional SSL certificates lacks standardised procedures. Even today, the process used for identity reassurance is strong for some certificates and weak for others. This results in the availability of both high authentication certificates and low authentication certificates (Organisation Validated Vs Domain Validated). Online criminals have figured out that they can work the system to obtain low authentication certificate SSL certificates (Domain Validated) for their fraudulent site(s) to help them appear more legitimate.

The lock icon most closely associated with secure SSL web transactions is not prominently featured in a web browser (if it appears at all – websites designed using "frames" do not display the lock icon). The "s" added to the http: is easily overlooked and the SSL certificate data is buried within an obscure browser menu. Plus, regardless of whether a certificate has been vetted with high (organisation) authentication or low (domain) authentication procedures, the same user interface conventions are displayed – leading some end users to assume that one SSL certificate is as secure as any other SSL certificate. This is definitely not the case.

The confusion created by low authentication (Domain Validated) combined with a low-impact and undifferentiated user interface makes it too easy for malicious web schemes to be perpetrated. A new solution was needed...

Representatives from over 25 organisations including CAs and browser manufacturers joined forces to create the Certificate Authority (CA)/Browser Forum and along with a number of WebTrust

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



auditors they created the new EV SSL standard. To achieve their ambitious goals almost every aspect of the web's trust structure was adapted to support the new standard.

Validity is central to EV SSL – validity of a website's identity, validity of the issuing CA, validity of the SSL certificate and finally clear identification of that validity to the end user. These validity elements result in stricter website identity vetting standards, real-time certificate revocation checking, stricter, WebTrust audit authorisation for CAs and a high visibility browser interface for the end user.

At the end of 2006, the new Extended Validation (EV) SSL certificate standard made its debut. The CA/Browser Forum published the first version of its identity verification process guidelines and the first CAs completed the new WebTrust audits thereafter. In early 2007, Microsoft enabled the new browser user interface and revocation checking features in IE7. Mozilla (Firefox), Opera and Apple (Safari) followed suit with their new browsers in 2008.

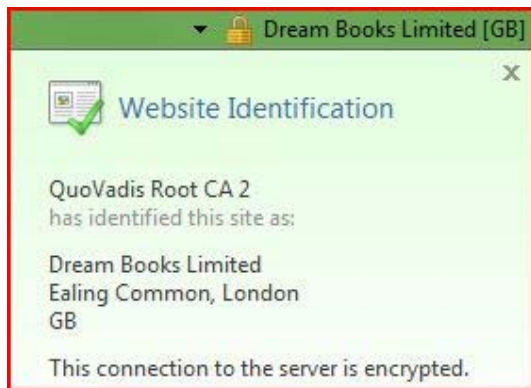
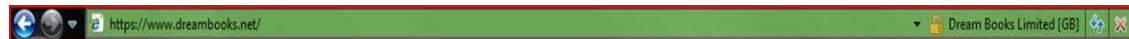
EV SSL provides the highest level of identity assurance available today from an SSL certificate. A website secured with an EV SSL certificate will instil extra confidence in consumers and help increase the percentage of completed transactions experienced by that website.

How do different browsers handle EV SSL certificates?

A familiar theme pervades all of the EV "ready" browsers and that is of the "green bar". However, each browser handles the EV certificate in its own unique way. Therefore, highlighted below is a graphic example of each of these and an indication of the percentage of users who use each browser.

MICROSOFT INTERNET EXPLORER 7

46.77% market share (source: Net Applications - Dec 08)



MOZILLA FIREFOX 3.x

17.18% market share (source: Net Applications - Dec 08)

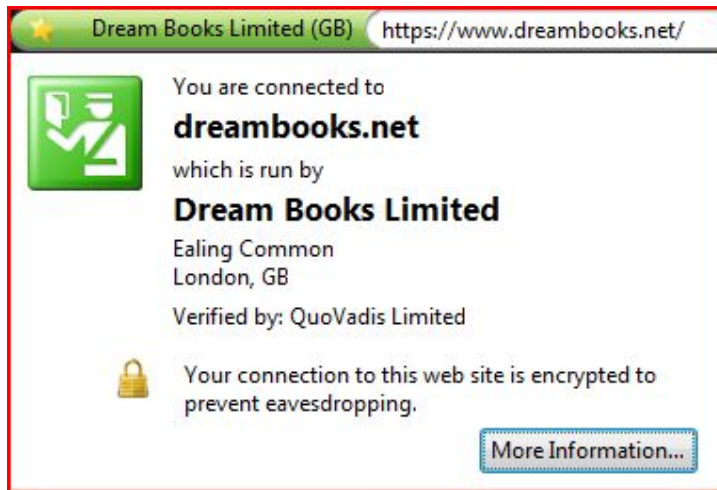


QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

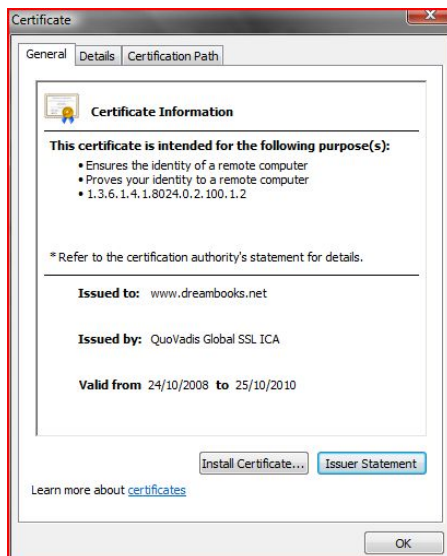
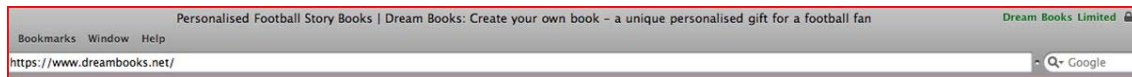
Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



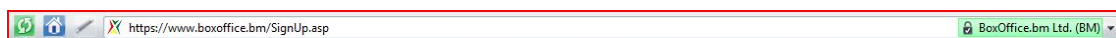
APPLE SAFARI 3.2

3.39% market share (source: Net Applications - Dec 08)



OPERA 9.x

0.68% market share (source: Net Applications - Dec 08)

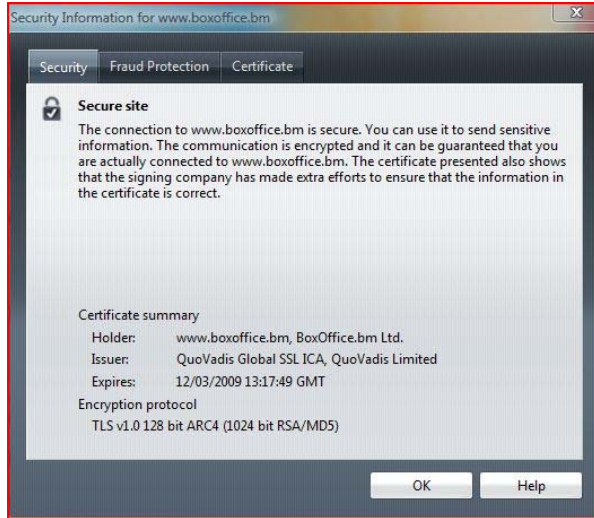


QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

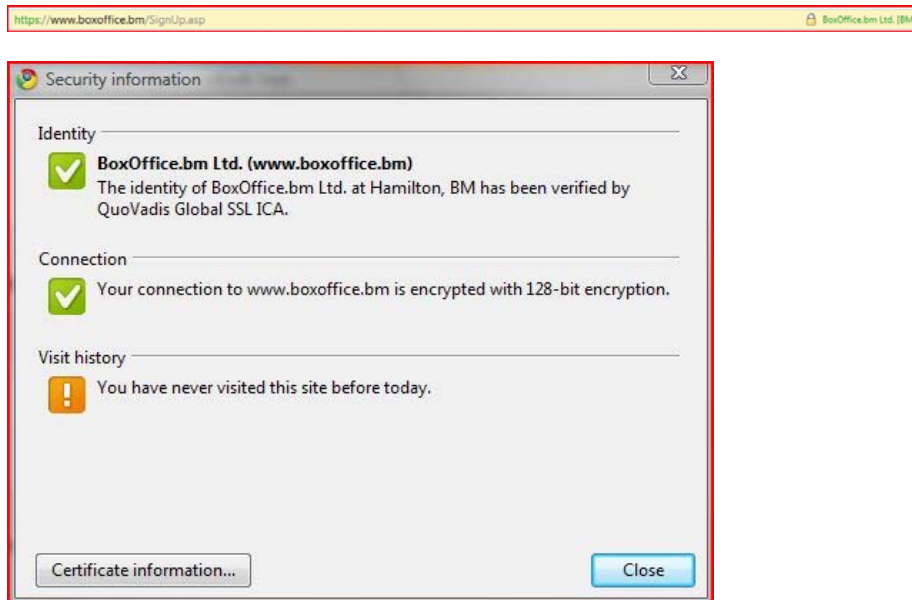
Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



GOOGLE CHROME 1.0

0.52% market share (source: Net Applications - Dec 08)



Why have EV SSL certificates?

As already mentioned within various parts of this paper there are a whole host of reasons for purchasing the EV SSL certificate. It has benefits to both the organisation behind the website and the website visitors. The new generation of SSL certificate is designed to combat on-line threats to both businesses and consumers.

In today's modern world more and more individuals from all market segments and demographic backgrounds are using the Internet for work, leisure and other purposes. This makes the on-line market place a much more competitive environment than it has ever been before. Individuals are

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



also becoming more educated about on-line threats and therefore beginning to lose both confidence and trust in whom they provide details to. Whether its names, address's, usernames/passwords or credit/debit card details or any other personal data, people are wishing to reduce the level of data they communicate as well as being reassured that the data which they do communicate is secure.

Most organisations are fighting to build their on-line business and encourage website visitors to engage in data transactions to reap the benefits of this medium, and prevent loss of business to other organisations who better adopt this technology. EV SSL certificates show that a business has been vetted by an organisation (certificate authority) that has been accredited to issue the new generation of certificates. The EV certificate is designed to act as a welcome factor, comparable to a shop window on the high street.

EV SSL certificates can be the deciding differentiating factor for if/where to purchase goods from for a website visitor. For instance if two on-line retailers with visually attractive sites have an identical product for sale at the same price - one with a standard SSL certificate and the other with the new generation EV SSL certificate, is it not obvious which retailer is going to appeal to the website visitor more? The bright attractive, welcoming EV SSL certificate will deliver more customers who are reassured that 'green' is good, 'green' is safe and 'green' shows a responsible organisation that is keen to protect its customers and its brand image, displaying a certificate which openly outlines details on the organisation such as the legal name of the organisation and the location.

Once the customer realises that the organisation has a green URL address bar displaying an Extended Validation certificate they will feel more confident in trusting such a site and therefore become more inclined and willing to submit data again. Therefore an EV SSL certificate helps build trust and ultimately builds brand loyalty.

The process of issuing EV SSL certificates not only helps to avoid certificates being purchased by deceptive/fraudulent sites, but provides consistency, helping businesses protect their 'brand' and users from being scammed with an added level of online differentiation.

What does not having EV SSL certificates mean to my business?

As far back as 2007 a report issued by Tec-Ed Research, a computer usability think tank showed that the EV SSL certificates would actually increase consumer confidence in making a transaction online.

After interviewing 384 online shoppers on usage and attitudes toward e-commerce and EV SSL, the results were quite astounding.

Tec-Ed measured the online shoppers' responses to websites with and without green URL address bars and they found that:

- 100 percent of the participants noticed when a website did or did not have a green URL address bar.
- 93 percent of participants prefer to shop at sites that have the green EV address bar.
- 97 percent of participants would share their credit card information with sites that display the green EV address bar.
- 67 percent said they would share credit card information with or without an EV SSL certificate.
- 77 percent said that they would think twice about shopping at a website that had lost its EV SSL certification.

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>



With EV SSL certification, both the online merchant and the end-user, who will be logged in to the merchant's website, are secure in knowing that both sides have the highest level of identity and fraud protection from an SSL Certificate.

EV SSL is the best way to ensure that phishers/fraudsters don't wreck your online business reputation, and that an end user/consumer doesn't get their sensitive data stolen from them either.

Having EV SSL certificates means a win-win situation for both online businesses and end-users. Not having EV SSL certificates in today's economic environment could have a significant, negative impact on your business.

QuoVadis Online Security Ltd

8 Hayters Court, Grigg Lane, Brockenhurst, Hampshire, SO42 7PG

Tel +44 (0) 1590 624 400

<http://www.quovadisglobal.co.uk>