GlobalSign ExtendedSSL Certificates

Securing online data and increasing customer confidence
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>The risks of non-secured websites</td>
<td>4</td>
</tr>
<tr>
<td>What is SSL and what is the role of an SSL Certificate?</td>
<td>4</td>
</tr>
<tr>
<td>Extended Validation SSL, how it makes the difference</td>
<td>4</td>
</tr>
<tr>
<td>Visible trust and credibility</td>
<td>4</td>
</tr>
<tr>
<td>The benefits of using an EV SSL Certificate</td>
<td>5</td>
</tr>
<tr>
<td>Why choose GlobalSign’s ExtendedSSL Certificates?</td>
<td>6</td>
</tr>
<tr>
<td>Where are GlobalSign’s ExtendedSSL Certificates available?</td>
<td>6</td>
</tr>
<tr>
<td>About GlobalSign</td>
<td>7</td>
</tr>
</tbody>
</table>
INTRODUCTION

The green address bar has become one of the Internet’s most familiar features. Usage and education have helped website users grow aware that green means security.

However, recognising the green bar is different from understanding it, and it is only legitimate to ask ourselves: what is the technology behind the green bar and what makes it so valuable?

As organisations increasingly rely on websites for providing information to the public, as well as for generating retail sales and other online services, digital security is of the utmost importance. Extended Validation (EV) SSL Certificates are responsible for the green bar. They provide credibility to a website, reassuring a visitor that the site is legitimate and owned by the organisation so claimed, and ensures a secure connection for any data submitted through the browser.

In 2011, the Online Trust Alliance research showed an increase of 7.1% in Extended Validation SSL Certificates usage amongst retail and banking sites since 2010, with 45% of websites now secured across the sector. Over 35,000 certificates were issued overall, reflecting a significant 68% growth rate on the previous year, as more organisations realised the need to use EV SSL as standard on their public facing web pages.

This White Paper will highlight the benefits, both technical and commercial, of using GlobalSign’s ExtendedSSL Certificate. It will explain how EV SSL differentiates from other types of Certificates and why it is organisations’ best ally in their hunt for website conversions.
The risks of non-secured websites

Every hour, billions of transactions take place online by individuals unaware of the risk they could be taking. It is commonly believed that hackers target only large organisations and financial institutions, underestimating the severity of today’s online security issues. However, phishing, the virtual equivalent of impersonation, is one of the most common methods of fraud on the Internet. Usernames, passwords, contact and bank details, any private or sensitive information is constantly at risk of being stolen and used maliciously. This can result in a “phisher” creating a fake website in the name of a well-known organisation tricking unaware visitors into entering further personal details.

What is SSL and what is the role of an SSL Certificate?

The Secure Sockets Layer (SSL) along with Transport Layer Security (TLS) is the most widely used security protocol today. It provides a secure channel between two machines operating over the Internet or an internal network. We typically see SSL in use when a web browser needs to securely connect to a web server over the inherently insecure Internet.

An SSL Certificate is required in order to be able to use the SSL protocol. An SSL Certificate is a small data file that digitally binds a cryptographic key to an organisation’s corporate details. Once a certificate is installed it is possible to connect to a website using a HTTPS connection, as this tells the server to establish a secure connection with the browser. When the secure connection is established all Web traffic between the server and browser is encrypted and secure.

The number of active SSL Certificates is growing at a global rate of 25% year on year, but less than 2% of all websites worldwide currently utilise SSL, when arguably a lot more should be using the security protocol.

Extended Validation SSL, how it makes the difference

When a website is secured with an SSL Certificate, any data transmitted between the browser and the server is encoded in a way that makes it unreadable to anyone except the intended recipient. This is commonly referred to as encryption.

Online security does not only constitute data protection, but also ensures that the recipient of the data is genuine and the intended recipient - this is where Extended Validation SSL comes in.

An Extended Validation SSL Certificate offers more than just encryption, as it also enables the organisation behind the website to present its own validated identity and hence authenticate itself to website visitors.

The EV SSL Certificate provides the highest level of identity assurance and works as a guarantee that the organisation behind the website, as well as the trusted third party validating the identity, completed a thorough identity verification process. The issuance process of EV SSL Certificates is strictly defined within the EV guidelines (a set of vetting principles and policies approved by the CA/Browser forum) and GlobalSign, as the issuing Certification Authority, must be WebTrust accredited to complete the validation steps. This verification process requires the applicant organisation to prove exclusive rights to use a domain, confirm its legal, operational and physical existence, and finally prove the entity has authorised the issuance of the Certificate.

Certification Authorities must also maintain the validity status of each EV SSL Certificate. This verification is completed via the OCSP (Online Certificate Status Protocol). Every time the end user visits a website secured with a GlobalSign ExtendedSSL Certificate, the browser automatically checks GlobalSign’s revocation status service and is immediately informed if the certificate has been revoked and is no longer valid.

The extensive validation process (coupled with the certificate status verification) is where the true value of Extended Validation SSL Certificates resides.

Visible trust and credibility

The stringent vetting processes would mean very little unless it can easily translate into visible trust indicators easily understood by end users. EV SSL activates:

- The Green Address Bar, “https” and the standard padlock: they visually guarantee that the website is being secured with the highest level of security, the Extended Validation SSL Certificate, and they confirm that all data will be encrypted and sent to a genuine verified organisation, and that it cannot be intercepted by an external online fraudster.
The name of the organisation that owns the website and the name of the Certification Authority that issued the certificate: both names alternate in the address bar as a constant reminder that the site owner has been verified by an accredited Certification Authority.

Website without EV SSL Certificate

Website with EV SSL Certificate

More details about the certificate are displayed when clicking on the certificate itself. The visitor can see information about the issuer and the certificate validity.

Website Identification

Certificate details

All major browsers include an enhanced user interface display for web security – triggered positively by the presence of a valid EV SSL Certificate or negatively by known association with malware or a revoked or misconfigured SSL Certificate.

GlobalSign’s ExtendedSSL Certificates are compatible with all browsers and mobile devices, and offer “fallback” standard SSL support for devices yet to implement the enhanced display of EV SSL. If a certificate has expired or has been revoked the green bar will no longer show in the browser, risking the visitor’s sense of trust in the website. If they decide to visit the website anyway, the address bar will become red as a visible reminder that they are visiting a site secured with an invalid Certificate.

The benefits of using an EV SSL Certificate

Extended Validation SSL Certificates should be used when identity assurance, visible trust and a guaranteed level of encryption are required. High profile websites often targeted for phishing attacks, such as major brands, banks or financial institutions, should use EV SSL for all public facing websites, but any website collecting data, processing logins or online payments also need the increased trust provided by EV SSL. EV SSL also allows less well known brands to use a standardised level of trust to compete against the more familiar brands already established on the Internet.

EV SSL provides high levels of encryption for any data transmitted online. Therefore, as part of an overall security policy, EV SSL can also help companies achieve compliance with regulatory standards surrounding the security of personal information.

But the primary benefit of EV SSL is to render trust and security in a simple, visible way for end users to see and understand - helping companies establish online trust and increase their perceived credibility. This directly translates into increased conversions and customer loyalty.

When visitors experience worry-free browsing and know that any data exchange with the website is secure, it makes them feel confident about coming back. Website visitors will feel safer when buying on a website that has been verified and secured, and as such EV SSL provides the virtual equivalent of a safe, known location of a retail shop. Good service is a start, but a secure service is a goal, as safety leads directly to higher conversions, and higher conversions to higher revenue.
Why choose GlobalSign’s ExtendedSSL Certificate?

GlobalSign’s SSL Certificates are trusted by all known devices and include many advanced features, some of which competing SSL Providers offer as paid-for premium options. These features include:

- 2048 bit future proof root CA
- Universal Compatibility with all browsers, mobile phones and devices
- SGC Security for minimum 128 bit minimum to 256 bit SSL encryption levels
- Unlimited Server Licensing - a single SSL Certificate for all servers
- Secures both www.domain.com and domain.com
- Secure Site Seal – includes all verified information of the website owner
- Unlimited reissues/ replacements for lifetime of the Certificate
- Installation Healthcheck
- Warranty – underwritten Liability Program

As Europe’s first Certification Authority and one of the first worldwide, GlobalSign has been issuing more than 15 million trusted digital certificates around the world since 1996.

By choosing GlobalSign’s SSL Certificates, customers benefit from:

- A simple but sophisticated product range
- An easy ordering system and customer account accessible 24/7
- Localised language support and superior customer service levels
- A well-established brand universally recognised and trusted

Where are GlobalSign ExtendedSSL Certificates available?

GlobalSign certificates are available directly from any GlobalSign website in numerous languages and currencies. See the contact section below for more information about the languages available or visit www.globalsign.com/ev/ to start your purchase.

Enterprise Solutions

When an organisation requires multiple certificates, GlobalSign’s Managed SSL is the perfect solution. Managed SSL allows enterprises of all sizes to conveniently and quickly purchase SSL Certificates, including EV SSL Certificates, through a web based management interface or web service API. Once the organisation has been pre-vetted, certificates can be applied for and issued. Managed SSL offers volume discounts and directly results in a significant reduction in costs and time associated with SSL management.

For more information about GlobalSign’s SSL Managed service you can read the White Paper or visit the website www.globalsign.com/managed-ssl/.

Partner Solutions

The Partner Programme allows organisations, such as hosting companies, domain registrars, web designers, integrators and VARs to add ExtendedSSL Certificates to existing product portfolios as a standalone product or as a bundled value add. Features of the Partner Programme include discounted pricing and high margin potential, sales and technical training, a free Certificate for the Partner’s site and an official Partner site seal. For more information about the Partner Programme and reselling GlobalSign SSL Certificates visit: www.globalsign.com/partners/.

If you would prefer to discuss your individual requirements with one of our SSL specialists, please refer to the contact details below to find the appropriate contact information.
ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices and Applications and include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. It's trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

<table>
<thead>
<tr>
<th>GlobalSign US &amp; Canada</th>
<th>GlobalSign EU</th>
<th>GlobalSign UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: 1-877-775-4562</td>
<td>Tel: +32 16 891900</td>
<td>Tel: +44 1622 766766</td>
</tr>
<tr>
<td><a href="http://www.globalsign.com">www.globalsign.com</a></td>
<td><a href="http://www.globalsign.eu">www.globalsign.eu</a></td>
<td><a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a></td>
</tr>
<tr>
<td><a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GlobalSign FR</th>
<th>GlobalSign DE</th>
<th>GlobalSign NL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: +33 1 82 88 01 24</td>
<td>Tel: +49 30 8878 9310</td>
<td>Tel: +31 20 8908021</td>
</tr>
<tr>
<td><a href="http://www.globalsign.fr">www.globalsign.fr</a></td>
<td><a href="http://www.globalsign.de">www.globalsign.de</a></td>
<td><a href="http://www.globalsign.nl">www.globalsign.nl</a></td>
</tr>
<tr>
<td><a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a></td>
<td><a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a></td>
<td><a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a></td>
</tr>
</tbody>
</table>