

Digital Security with VeriSign Certificates

Overview	
General Information	<p>VeriSign is the trusted provider of Internet infrastructure services for the networked world.</p> <p>An SSL (Secure Sockets Layer) certificate secures customers' online transactions by encrypting credit card and personal information and providing a safe route of communication for your online payments. SSL certificates are globally accepted technology that helps customers to confirm the website they are dealing with is secure.</p> <p>In Bangladesh, SSL Wireless -- a leading provider of banking based Value-Added Services (VAS) -- brings the entire line of VeriSign® Secure Sockets Layer (SSL) Certificates to the sectors requiring data communication protection and security. In expanding its banking VAS product offerings, SSL Wireless will also carry Extended Validation (EV) SSL solutions and SSL Certificates from GeoTrust and Thawte, other VeriSign brands.</p>
What are SSL and Digital Certificates?	<p>Secure Socket Layer (SSL) is a protocol developed by Netscape in 1996 which quickly became the method of choice for securing data transmissions across the Internet. SSL is an integral part of most Web browsers and Web servers and makes use of the public-and-private key encryption system developed by Rivest, Shamir, and Adleman.</p> <p>In order to make an SSL connection, the SSL protocol requires that a server should have a digital certificate installed. A digital certificate is an electronic file that uniquely identifies individuals and servers. Digital certificates serve as a kind of digital passport or credential which authenticate the server prior to the SSL session being established.</p> <p>Typically, digital certificates are signed by an independent and trusted third party to ensure their validity. The "signer" of a certificate is known as a Certification Authority (CA), such as VeriSign, thawte and GeoTrust.</p>
When should SSL be used and what can it secure?	<p>There are two main online security problems that SSL certificates help solve:</p> <ul style="list-style-type: none"> ▪ Authentication - proving a company's (or server's) identity online and in so doing create a sense of trust and confidence in using a Web site. ▪ Encryption - offering protection for the data submitted to a Web site (or between servers) so that in the event of interception, it will be unintelligible without the unique key used for decryption.

	<p>Solving these security problems allows online business to protect against the following scenarios:</p> <ul style="list-style-type: none"> ▪ Spoofing - The low cost of Web site design and ease with which existing pages can be copied makes it all too easy to create illegitimate sites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional-looking storefronts that mimic legitimate businesses. ▪ Unauthorized Disclosure - when information is transmitted "in the clear", making it possible for hackers to intercept the transmissions and obtain sensitive information from customers. ▪ Data alteration - the content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card, and social security numbers as well as currency amounts; indeed any information sent "in the clear" is all vulnerable to alteration. <p>So what are the practical applications of SSL certificates?</p> <p>Firstly, looking at categories of data, the most common deployment is for securing transmission of financial information in ecommerce. However, with incidence of identity theft on the rise, protecting the transmission of a broad range of personally-identifiable information is becoming ever more important. This category of data would include identity and social security numbers, e-mail addresses and demographic information as well as account registration and login information.</p> <p>In terms of applications and protocols, SSL Certificates can be used to secure the following:</p> <ul style="list-style-type: none"> ▪ Web Servers ▪ Mail Servers ▪ Databases ▪ FTP Sites ▪ Internet Chat ▪ NNTP
<p>What are Code Signing and Digital Certificates?</p>	<p>Code signing is the process of digitally signing executables and scripts using asymmetric encryption. A digital signature confirms that the software originated from the Publisher who signed it and that the code has not been altered or corrupted since it was signed.</p> <p>Asymmetric encryption uses a pair of complementary keys, the public key and the private key. As their names imply, one of the keys is intended to be kept by the Publisher while the other one is shared freely with the world. A Software Publisher uses the private key to encrypt a digital signature and the rest of the world can then use the corresponding public key to decrypt and analyze that signature. This signature includes a hash, which allows users of the software to verify</p>

	<p>that (a) the software really did come from the publisher as claimed, and (b) the software hasn't been modified since the Publisher released it. If the decryption is successful, they've successfully verified your identity.</p> <p>A digital certificate is an electronic trusted ID card which utilizes a digital signature to bind a public key together with respective user identity for the purpose of public trust. A Certificate Authority (CA) such as VeriSign creates, manages, distributes, and revokes digital certificates.</p> <p>In the real world, customers trust software they buy in a store because they can tell who published the product and can see whether the package has been opened or not. The Internet cannot offer the same security reassurance provided by shrink-wrapped software. With a Code Signing Certificate, your code will be as safe to install as it would be if you shrink-wrapped it and sold it off a store shelf.</p>
<p>When should Code Signing be used and what can it secure?</p>	<p>A Code Signing Certificate is strongly recommended for any Software Publisher who plans to distribute code or content over the Internet or corporate extranets and wants to assure the integrity and authorship of that code. Code Signing is essential to the publisher's business for several reasons:</p> <ul style="list-style-type: none"> ▪ Builds customer confidence and trust ▪ Protects your intellectual property and business reputation ▪ Meets the requirements of platforms and network providers as well as business customers ▪ Eliminates disruptive security alerts that might turn away customers or increase support inquiries ▪ Helps increase market reach and adoption of downloadable software <p>Code Signing is advantageous in either external or internal use case as long as the code runs on the client machine.</p> <p>Code signing supports your commercial sales and external distribution efforts by reassuring would-be users and buyers with the digital equivalent of shrink-wrap. It also satisfies the requirements of platforms, business customers, and partners.</p> <p>Even if you're focused only on internal distribution of code to users within your company, code signing is still important. Potential users will already know who you are but might not be able to run your code if your IT department requires all code to be signed.</p> <p>So what are the practical applications of Code signing certificates? Many platforms and applications are supported including:</p> <ul style="list-style-type: none"> ▪ ActiveX controls

	<ul style="list-style-type: none"> ▪ Kernel-mode code for the 64-bit editions of Windows® Vista ▪ Device drivers ▪ Macros and VBA ▪ Java™ Applets ▪ MIDlet (J2ME™) ▪ Plug-ins and other executables ▪ Adobe® AIR™ applications 																		
<p>Application areas for SSL</p>	<ul style="list-style-type: none"> + Web Domains + Payment Gateways + Multiple Hosts /Sub domains + Multiple Domains + eCommerce Sites + Intranets (Private IP ranges) + Banking Applications + User/Member Login pages + Sign-up Pages + VPN + Web Access to email + SMTP/IMAP/POP + Partners remote offices + FTP Sites + Database & App servers + Email Servers 																		
<p>VeriSign fits whom?</p>	<table border="1" data-bbox="552 1115 1382 1832"> <thead> <tr> <th>Company Type</th> <th>Solution</th> </tr> </thead> <tbody> <tr> <td>Financial Institutions</td> <td>VeriSign Secure Site Pro with EV</td> </tr> <tr> <td>Retail Merchants</td> <td>VeriSign Secure Site with EV and VeriSign Secure Site Pro with EV</td> </tr> <tr> <td>Healthcare Industry</td> <td>VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV</td> </tr> <tr> <td>Application Service Providers</td> <td>VeriSign Secure Site</td> </tr> <tr> <td>E-Government</td> <td>VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV</td> </tr> <tr> <td>Domain Registrars</td> <td>VeriSign Secure Site</td> </tr> <tr> <td>Educational Institutions</td> <td>VeriSign Secure Site and VeriSign Secure Site with EV</td> </tr> <tr> <td>Hosting Providers</td> <td>VeriSign Secure Site</td> </tr> </tbody> </table>	Company Type	Solution	Financial Institutions	VeriSign Secure Site Pro with EV	Retail Merchants	VeriSign Secure Site with EV and VeriSign Secure Site Pro with EV	Healthcare Industry	VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV	Application Service Providers	VeriSign Secure Site	E-Government	VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV	Domain Registrars	VeriSign Secure Site	Educational Institutions	VeriSign Secure Site and VeriSign Secure Site with EV	Hosting Providers	VeriSign Secure Site
Company Type	Solution																		
Financial Institutions	VeriSign Secure Site Pro with EV																		
Retail Merchants	VeriSign Secure Site with EV and VeriSign Secure Site Pro with EV																		
Healthcare Industry	VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV																		
Application Service Providers	VeriSign Secure Site																		
E-Government	VeriSign Secure Site Pro and VeriSign Secure Site Pro with EV																		
Domain Registrars	VeriSign Secure Site																		
Educational Institutions	VeriSign Secure Site and VeriSign Secure Site with EV																		
Hosting Providers	VeriSign Secure Site																		
<p>Secure your web site today</p>	<p>As an eCommerce business, we understand the importance of consumer confidence on the Internet. By securing your site you increase your level of data protection, your customers' confidence and</p>																		

	<p>therefore your online sales.</p> <p>VeriSign is the trusted provider of Internet infrastructure services for the networked world. The ability to know and trust the parties with which you do business and communicate has become critical in the networked world.</p>
<p>VeriSign Technical Review</p>	<ul style="list-style-type: none"> ▪ VeriSign facilitates as many as 50 billion authoritative Domain Name System (DNS) queries a day, and has been providing this service since 1998 with 100% availability. ▪ VeriSign plans to increase capacity of the .com and .net DNS by 10 times by 2010 to provide the security and stability required for global Internet-based transactions. ▪ VeriSign is the SSL Certificate provider of choice for over 95% of the Fortune 500 and 96 of the world's 100 largest banks. ▪ The VeriSign Secured® Seal, the most recognized symbol of trust on the Internet (Synovate/GMI Research, September 2008), is served over 150 million times a day. ▪ VeriSign has issued over 2 million VeriSign® Identity Protection (VIP) credentials to consumers for strong authentication on a network of leading Web sites.
<p>Benefits of Posting the VeriSign Secured Seal</p>	<ul style="list-style-type: none"> ▪ More recognized than any other trust mark, 91% of U.S. online shoppers are familiar with the VeriSign Secured Seal (Synovate/GMI 2008, VeriSign Secured Seal Research Review.) ▪ Show visitors that the site is secured using industry leading SSL technology. ▪ Lower shopping cart and other transaction abandonment. ▪ Associate your brand with the trusted VeriSign brand. ▪ Increase visitor-to-sales conversions.
<p>Other information for VeriSign</p>	<ul style="list-style-type: none"> ▪ The design of the VeriSign Secured Seal is recognized as an international sign of trust on the Internet. Over 90,000 domains in 145 countries display the VeriSign Secured Seal. ▪ The VeriSign Secured Seal is available in 13 different languages and viewed an average of 150 million times each day. ▪ A pop-up window displays full business authentication information when clicked by a visitor. ▪ EV Upgrader™, built into the VeriSign Secured Seal, enables all Internet Explorer 7 on Windows XP operating systems to see the visual cues associated with an Extended Validation SSL Certificate.

VeriSign Certificates:



Become a **GeoTrust** partner and offer your customers brand-name SSL Certificates and identity verification products at competitive prices.

Manage all your GeoTrust SSL Certificates from a single portal or become your own Certificate Authority with a GeoTrust root certificate.

For more information visit:
<http://www.geotrust.com/>



VeriSign® Extended Validation (EV) SSL Certificates

show that your Web site can be trusted. EV triggers new browsers like IE 7 to turn the address bar green when visitors view your site.

For more information visit:
<http://www.verisign.com/>



online security trusted by millions around the world

Get started with SSL
Discover what SSL is and why you need it.

Inspire Trust Online
Show Users the Thawte Secured Seal and Green Bar.

Beyond E-Commerce
Secure Web-based data and services with SSL.

For more information visit:
<http://www.thawte.com/>