VeriSign®
The Value of Trust℠

Guide to Securing Your E-Government Web Site

CONTENTS

Introduction

Protecting the confidentiality and integrity of sensitive information electronically transmitted whether to and from the federal government, or between government agencies, is a crucial step to complying with new federal security and privacy regulations. The E-Government Act of 2002[1] mandates that agencies use technology to its fullest to provide citizen-centered services and information over the Internet. President George W. Bush presented five goals for this government-wide reform: strategic management of human capital, budget and performance integration, competitive sourcing, expanded use of the internet and computer resources to provide government services electronically, and improved financial management. The president said, "Effective implementation of E-Government is important in making Government more responsive and cost-effective."[2]

Ensuring Compliance With the E-Government Act

A key provision of the E-Government Act for this paper is Section 208, which "is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." Title III, Sec. 301 acknowledges the "highly networked nature" of the federal computing environment and directs agencies to "provide for development and maintenance of minimum controls required to protect Federal information and information systems." The Act also acknowledges "commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures…."[3]

As part of compliance, your agency must secure information exchange between Web servers and clients, server-to-server, and among other networking devices such as server load balancers or SSL accelerators. For a complete solution, cross-network security must protect servers facing both the Internet and private intranets.

Secure Sockets Layer (SSL) is the World Standard for Web security

SSL[4] technology is used to protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL protects against site spoofing, data interception and tampering. Support for SSL is built into all major operating systems, Web applications and server hardware. By leveraging the powerful encryption through SSL Certificates on E-Government site servers with the confidence instilled by VeriSign's authentication procedures, your agency can immediately demonstrate compliance efforts and protect sensitive data transmitted between your servers and other agencies, constituents, employees and e-government partners.

VeriSign Solutions for Stronger Security and Compliance

VeriSign Secure Site Services offer your agency the power to secure E-Government sites for safe information transfer, even for financial transactions. With VeriSign, citizens and other agencies' users of your E-Government sites will get the trustworthy Web experience they demand. Securing your web sites with VeriSign also enables compliance with security provisions of the E-Government Act. Information for obtaining a free trial of a VeriSign SSL certificate is available at the end of this guide..

[1] *Public Law 107-347, at www.whitehouse.gov/omb/egov/pres_state2.htm.*

[2] *Presidential Memorandum, July 10, 2002 (www.whitehouse.gov/news/releases/2002/07/print/20020710-6.html).*

[3] *E-Government Act of 2002, Title III, Sec. 3541: 2, 4, 5.*

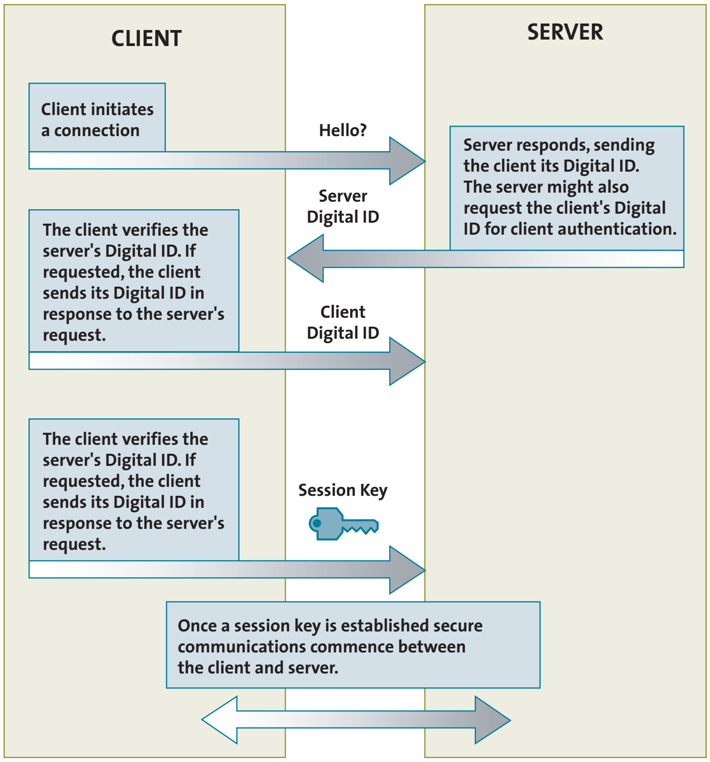
[4] *The Internet Engineering Task Force has renamed SSL to Transport Layer Security (TLS), and is working on wider adoption of the TLS protocol. SSL, however, remains the popular nomenclature.*

Encryption Technology and SSL Certificates

Encryption, the process of transforming information to make it unintelligible to all but the intended recipient, forms the basis of data integrity and privacy necessary for e-commerce. Citizens and other government agencies will submit sensitive information and transactions to your E-Government site via the Web only when they are confident that their sensitive information is secure. The solution for agencies that are serious about E-Government is to implement a trust infrastructure based on encryption technology.

An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communications. SSL Certificates serve as a kind of digital passport or credential. Typically, the "signer" of a certificate is a "Certificate Authority" (CA), such as VeriSign.

The diagram below illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of SSL Certificates occur within seconds, and require no action by the consumer.



Client initiates a connection

Server responds, sending the client its Digital ID. The server might also request the client's Digital ID for client authentication.

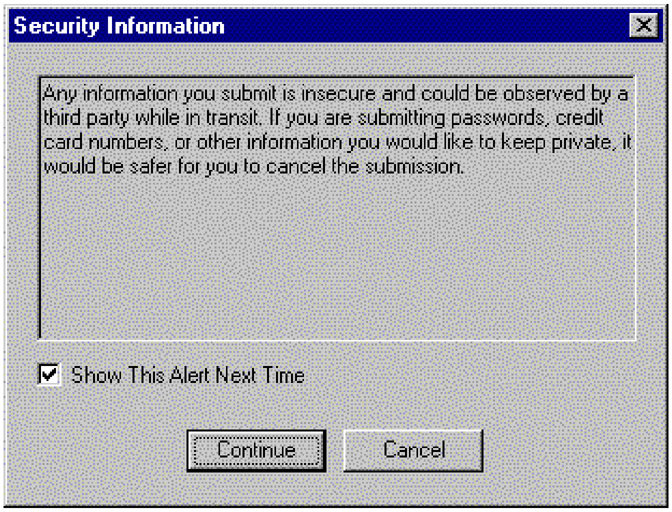
The client verifies the server's Digital ID. If requested, the client sends its Digital ID in response to the server's request.

The client verifies the server's Digital ID. If requested, the client sends its Digital ID in response to the server's request.

Once a session key is established secure communications commence between the client and server.

Making E-Government Easy

Installing VeriSign SSL Certificates makes E-Government transactions with your agency safer for citizens and other agencies – and easier to submit sensitive information over the Internet. Browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured site (a site without an SSL Certificate), the browsers will by default show a warning, which can lead users to question the trustworthiness of an E-Government site.



Any information you submit is insecure and could be observed by a third party while in transit. If you are submitting passwords, credit card numbers, or other information you would like to keep private, it would be safer for you to cancel the submission.

☑ Show This Alert Next Time

VeriSign Is the Commercial Standard for SSL Security

VeriSign is the world's leading Certificate Authority having issued more than 400,000 SSL certificates. Web users are used to seeing commercial e-commerce sites display the VeriSign Secure Site Seal – prominently displayed to assure online users that their Web business is legitimate and authentic, and that all financial transactions with that site are secured by SSL encryption.

Authenticate Your E-Government Site to Ensure Trust

Encryption alone is not enough to ensure a secure Web site and to build trust between your agency and your E-Government site users. It is imperative that your agency's identity be verified to improve Web visitors' trust in you and your Web site. VeriSign assures trust by coupling rigorous business authentica-tion practices with state-of-the-art encryption technology in its SSL certificate solutions. VeriSign will only issue an SSL certificate to your online business after it has performed the following authentication procedures:

- Verifying your agency's identity and confirming it is a legal entity
- Confirming that your agency has the right to use the domain name included in the certificate
- Verifying that the individual who requested the SSL certificate on behalf of the agency was authorized to do so

VeriSign's rigorous authentication practices set the industry standard. VeriSign documents its carefully crafted and time-proven practices and procedures in a Certificate Practices Statement. And VeriSign annually undergoes an extensive SAS 70 Type II audit by KPMG. (The Statement of Auditing Standard 70, SAS 70, was established by the American Institute of Certified Public Accountants to certify trusted practices.)

VeriSign's established authentication and verification procedures can help your agency comply with security provisions of the E-Government Act, inspire trust and confidence in citizens and other agencies by verifying its identity, and reduce the risk of fraud. Procedures used by VeriSign are the result of years of operating trusted infrastructure for the Internet and authenticating more than half a million commercial businesses.

VeriSign Solutions

VeriSign 40-bit SSL Encryption

The SSL Certificate included with your Secure Site service enables visitors to verify your agency's E-Government site's authenticity and to communicate with it securely via state-of-the-art SSL encryption, which protects confidential information from interception and hacking.

40-bit SSL (Secure Server) IDs, included with Secure Site service, are ideal for security-sensitive intranets, extranets, and Web sites. They enable 40-bit SSL when communicating with export-version Netscape and Microsoft Internet Explorer browsers (used by most people in the U.S. and worldwide), and 128-bit SSL encryption when communicating with domestic-version Microsoft and Netscape browsers. You must use one SSL Certificate per domain name per server. 40-bit SSL (Secure Server) IDs run on virtually all server software platforms.

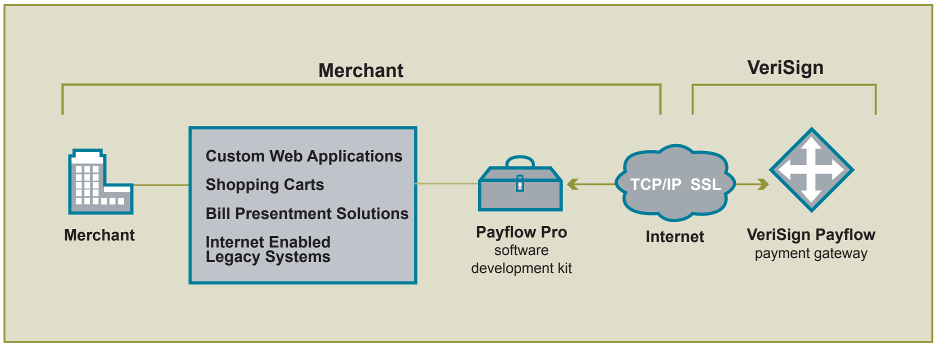
VeriSign 128-bit SSL Encryption

The SSL Certificate included with your Site Trust service enables visitors to verify your site's authenticity and to communicate with it securely via state-of-the-art SSL encryption, which protects confidential information from interception and hacking.

128-bit SSL (Global Server) IDs, included with Secure Site Pro, enable the world's strongest SSL encryption with both domestic and export versions of Microsoft® and Netscape® browsers. 128-bit SSL is the standard for large-scale online merchants, banks, brokerages, health care organizations, and insurance companies worldwide.

You must use one SSL Certificate per domain name per server. 128-bit (Global Server) IDs can run on server software from any non-U.S. software vendor, or software from a U.S. software vendor properly classified by the U.S. Department of Commerce.

VeriSign Solutions Grow with Your E-Government Business



Simplify management of multiple SSL Certificates

Is your site hosted on 10 or more servers? With one simple purchase, VeriSign's Managed PKI for SSL service lets you issue all the SSL Certificates you need—either standard or true 128-bit SSL certificates—in bundles of 10, 25, 50, 100, or more. A convenient one-step purchasing process lets you take advantage of a single purchase order, and volume discounts make Managed PKI for SSL the most cost-effective way to secure Web sites with large numbers of Web servers or other trust devices.

Managed PKI for SSL is simple to set up and configure: start issuing server certificates quickly via our intuitive Web-based process. Renewing IDs or buying additional IDs is just as easy. To find out more about Managed PKI for SSL, go to http://www.verisign.com/products/onsite/ssl/index.html

Accept Online Payments with VeriSign Payment Services

VeriSign Payment Services provide the ideal payment transaction platform for E-Government sites providing financial transactions on the Internet. Regardless of your agency site's size or demands, VeriSign delivers the right solution: a fast, scalable, and reliable Internet payment platform that enables you to authorize, process, and manage multiple payment types. VeriSign Payment Services bring affordability, flexibility, and convenience to Internet payment processing by combining a flat-fee monthly pricing model with a growing menu of services and solutions for merchants, financial institutions, resellers and developers.

VeriSign's Commerce Site and Commerce Site Pro Services combine SSL Certificates with the VeriSign Payflow Pro service to form a complete, integrated solution that's ideal for E-Government sites and online stores.

- Commerce Site includes a 40-bit SSL Certificate and PayFlow Pro, plus other value added services.
- Commerce Site Pro includes a 128-bit SSL Global Server ID and Playflow Pro, plus value added services.

VeriSign's Payflow Pro is designed especially to help your agency's E-Govermnent Web sites to securely accept and process credit card, debit card, purchase card, and electronic check payments. Payflow Pro is the most robust, versatile solution for online payment processing—ideal for large-scale e-commerce requiring peak performance and complete customizability.

Conclusion

By setting up an online presence for E-Government, your agency can reach the millions of citizens and other government agencies who already use the Internet for transactions. By ensuring the security of these sites, your agency can engender trust and make it easier to transact business with the Federal Government.

A VeriSign SSL Certificate also enables your agency to immediately comply with security provisions of the E-Government Act of 2002, begin conducting online business securely, with authentication, message privacy, and message integrity. As a result, your agency can minimize risk, win user confidence and streamline government business processes.

To speak with a VeriSign security expert about your agency's Web site security needs, please call toll free 866-893-6565 or call 650-426-5112. We can also be reached via email at: internetsales@verisign.com

Try a VeriSign SSL Certificate for free

You can secure your Web site for a free two-week trial. To apply for your free trial 40-bit SSL Certificate, please visit http://www.verisign.com/products/srv/trial/intro.html now. You can complete the entire enrollment process online in about 15 minutes and immediately begin using your trial SSL Certificate.

Learn more about VeriSign Payment Services at:
http://www.verisign.com/products/payment.html

ABOUT VERISIGN

VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence.