Chapter 28

TRUSTING SSL CAS IN SERVERS AND BROWSERS

INTRODUCTION

The practical means of implementing PKI and digital signatures are via Web server certificates that enable authentication and SSL encryption. SSL certificates form the basis of an Internet trust infrastructure by allowing websites to offer safe, secure information exchange to their customers. SSL server certificates satisfy the need for confidentiality, integrity, authentication and nonrepudiation [1].

SSL DEFINED

Secure Sockets Layer (SSL), originally developed by Netscape Communications, is an information technology for securely transmitting information over the Internet. The SSL protocol has become the universal standard on the Web for authenticating websites to Web browser users and for encrypting communications between browser users and Web servers [1].

Server certificates are available from Certificate Authorities (CAs) such as trustworthy, independent third parties that issue certificates to individuals, enterprises and websites. CAs use thorough verification methods to ensure that certificate users are who they claim to be before issuing them. CA's own self-signed SSL digital certificates are built into all major browsers and Web servers, including Netscape Communicator and Microsoft Internet Explorer, so that simply installing a digital certificate on a Web server enables SSL capabilities when communicating with Web browsers. SSL server certificates fulfil two necessary functions to establish e-commerce trust: SSL server authentication and SSL encryption [1].

SSL Server Authentication

Server certificates allow users to confirm a Web server's identity. Web browsers automatically check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) included in the list of trusted CAs built into browser software. SSL server authentication is vital for secure e-commerce transactions in which users, for example, are sending credit card numbers over the Web and first want to verify the receiving server's identity [1].

SSL Encryption

SSL server certificates establish a secure channel that enables all information sent between a user's Web browser and a Web server to be encrypted by the sending software and decrypted by the receiving software, thus protecting private information from interception over the Internet. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering: that is, for automatically determining whether the data has been altered in transit. This means that users can confidently send private data, such as credit card numbers, to a website, trusting that SSL keeps it private and confidential [1].

HOW SSL SERVER CERTIFICATES WORK

SSL Certificates take advantage of SSL to work seamlessly between websites and visitors' Web browsers. The SSL protocol uses a combination of asymmetric public key encryption and faster symmetric encryption [1].

The process begins by establishing an SSL "handshake" – allowing the server to authenticate itself to the browser user and then permitting the server and browser to cooperate in the creation of the symmetric keys used for encryption, decryption and tamper detection. The following steps show the process flow:

1. A customer contacts a site and accesses a secured URL: a page secured by a SSL Certificate (indicated by a URL that begins with "https:" instead of just "http:" or by a message from the browser). This might typically be an online order form collecting private information from the customer, such as address, phone number and credit card number or other payment information.
2. The customer's browser automatically sends the server the browser's SSL version number, cipher settings, randomly generated data and other information the server needs to communicate with the client using SSL.
3. The server responds, automatically sending the customer's browser the site's digital certificate, along with the server's SSL version number, cipher settings etc.
4. The customer's browser examines the information contained in the server's certificate and verifies that:
   a. The server certificate is valid and has a valid date
   b. The CA that issued the server been signed by a trusted CA whose certificate is built into the browser