NSI Registry
Copyright © 1999 Network Solutions, Inc. All rights reserved.
Network Solutions, Inc.
505 Huntmar Park Dr.
Herndon, VA 20170
USA
+1 703 742 0400

mailto:info@NSIRegistry.net

Enabling SSL

Introduction

This document provides a high-level introduction to Secure Socket Layer (SSL) and cryptographic techniques that are used by SSL to provide secure communication over the Internet. It also describes the steps required to SSL-enable a client who needs to connect to an SSL server.

SSL

SSL is a defacto industry standard Internet protocol for secure communications. It is a connection-based protocol that offers encryption, authentication, and message integrity. SSL resides between TCP/IP and upper-layer applications, requiring no changes to the application layer.

http://www.rsa.com/ssl/qa/index.html

Public Key Cryptography

In this scheme, every user has a public key that is given out freely and a private key that the user holds secretly. To send a private message to someone else, the user encrypts it with the recipient’s public key. The recipient then decrypts it with their private key.

http://www.rsa.com/rsalabs/faq/html/2-1-1.html

Secret Key Cryptography

This scheme uses the same key for encryption and decryption. To decrypt a message, the recipient must know the key used to encrypt the message. Secret key algorithms in general are faster than public key algorithms.

http://www.rsa.com/rsalabs/faq/html/2-1-2.html

Certificate

A certificate is a digital document attesting to the binding of a public key to an individual or other entity. It allows verification of the claim that a specific public key does in fact belong to a specific individual. Certificates help prevent someone from using a phony key to impersonate someone else.

http://www.rsa.com/rsalabs/faq/html/4-1-3-10.html

Digital Signature

A signature provides two security services: authentication and integrity. A signature gives the user assurance that a message has not been tampered with and that it originated from a certain person. Signatures do not provide confidentiality.

http://www.rsa.com/rsalabs/faq/html/2-2-2.html

MAC

A Message Authentication Code (MAC) is basically a keyed message digest. Like a message digest, a MAC takes an arbitrary amount of input data and creates a short digest value. Unlike a message digest, a MAC uses a key to create the digest value. This makes it useful for protecting the integrity of data that is sent over an unsecured network.

http://www.rsa.com/rsalabs/faq/html/2-1-7.html

Writing an SSL Client

The following steps are necessary in writing an SSL client.

1. Choose/Select/Buy an SSL Library. Review the user guide.
2. Specify the client certificate.
3. Specify the cipher suites that the user intends to use for SSL handshake. Order the elements in order of preference, from best to worst.
4. Initiate the SSL connection.
5. Perform the SSL handshake.
6. Request a server certificate.
7. Verify the server certificate.
8. Implement the application logic.

The Registry SSL Server

The following list details the Registry SSL server as it is and what changes can be expected in the near future.

1. The Registry SSL server currently has an RSA certificate and only supports clients who have obtained an RSA certificate from Thawte (www.thawte.com) or Verisign (www.verisign.com).
2. Currently, the Registry SSL server has the following cipher suites enabled:

   SSL_RSA_EXPORT_WITH_RC4_40_MD5

SSL_RSA_WITH_RC4_128_MD5

SSL_RSA_WITH_RC4_128_SHA

SSL_RSA_EXPORT_WITH_DES_40_CBC_SHA

SSL_RSA_WITH_DES_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

SSL_DHE_DSS_WITH_DES_CBC_SHA

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

SSL_DHE_RSA_WITH_DES_CBC_SHA

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

3. It is important for the SSL client to choose at least one cipher suite that is supported by the SSL server; otherwise, the SSL handshake will fail.

4. It is important that the SSL client uses a secure RSA certificate issued by Thawte or Verisign.