Concepts

Encryption for Entire Net-Work provides support for the Secure Sockets Layer (SSL) to manage the security of message transmissions. This support is provided for Entire Net-Work on mainframe and open operating systems.

On mainframe systems, only z/OS and z/VSE support is provided at this time. On open systems, SSL Toolkit support is provided only in 32-bit Windows environments. Mainframe support is provided in a new SSL line driver distributed with Encryption for Entire Net-Work. Open systems support is provided through Software AG's implementation of OpenSSL.

Secure Sockets Layer (SSL) is a standard protocol used to manage the security of message transmissions in an open communications network, such as the Internet. Two types of security are provided:

- Authentication
- Encryption

SSL uses TCP/IP for its physical communications. In addition, SSL uses public and private key encryption for both authentication and data encryption keys. These keys are obtained from a certificate authority, as described elsewhere in this guide.

- Authentication
- Encryption and Decryption
- Certificate Authorities

Authentication

Using *digital signatures*, the partners in a conversation (the client and server) can be authenticated.

A digital signature is a digital code that can be attached to an electronically-transmitted message that uniquely identifies the sender. The purpose of a digital signature is to authenticate the identity of the individual sending the message using a private key to sign the message and a public key to verify the signed message. These keys are obtained from a certificate authority of some kind, as described in *Certificate Authorities*.

Encryption and Decryption

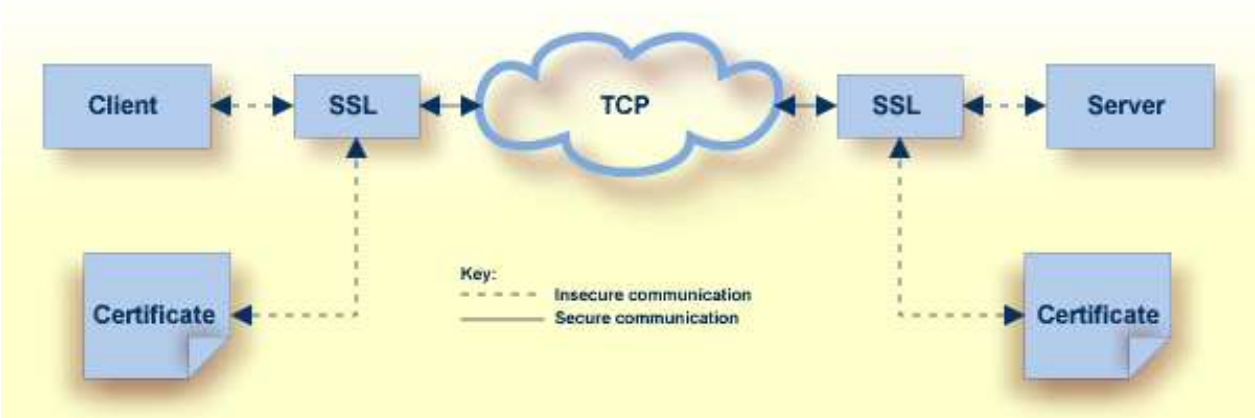
Using data *encryption* and *decryption*, messages are secured as they pass through the network.

Encryption is the conversion of data into ciphertext, which cannot be easily understood without access to the encryption or decryption key. Decryption is the process of converting encrypted data back into its original form, so it can be understood. To decrypt the contents of an encrypted message, a decryption key is required. Encryption keys are generated automatically after the successful handshake between the client and server. The handshake between the client and server is handled through the use of private and public keys, which are obtained from a certificate authority of some kind, as described in *Certificate Authorities*.

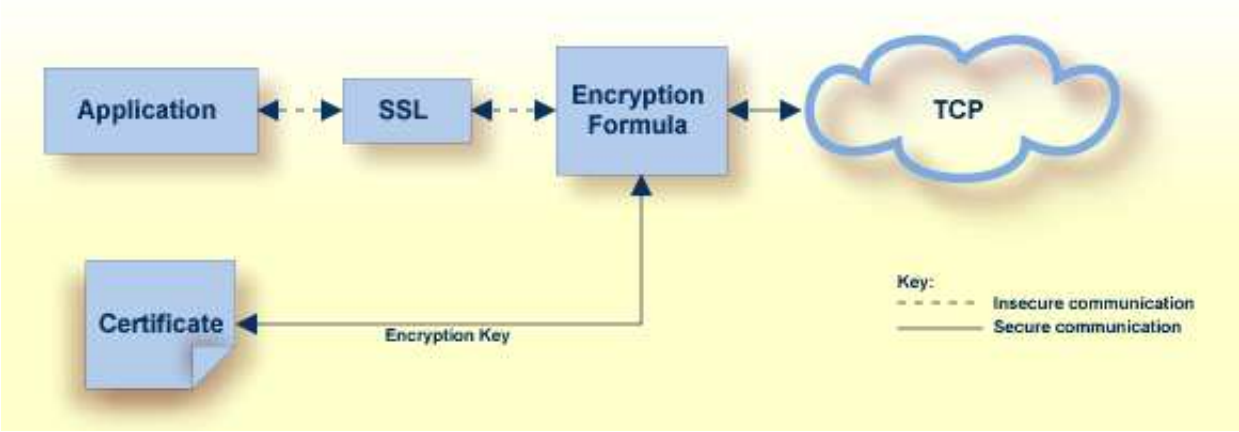
Certificate Authorities

A *certificate authority* issues and manages *certificates* for message encryption. It also verifies (authenticates) the information provided by the requestor of a digital certificate. If verification is successful, the certificate authority can then issue a certificate.

The following diagram depicts how certificates are used during authentication.



The following diagram depicts how certificates are used during data encryption.



Various organizations, such as VeriSign, act as external certificate authorities for other companies and supply certificates for authentication and encryption as requested by their clients. For Entire Net-Work, you can use an external certificate authority to provide your certificates or, *for testing only*, you can use the open source SSL Toolkit (provided with Encryption for Entire Net-Work) to become your own certificate authority.

For more information about the open source SSL Toolkit, read *Using the SSL Toolkit*.