What is an SSL File Transfer?

http://www.jscape.com/blog/bid/82339/What-is-an-SSL-File-Transfer

Overview

SSL file transfer is a term sometimes used in referring to a secure file transfer protocol known as FTPS or FTP-SSL. FTP is a network protocol used for transferring files, while SSL is a protocol for encrypting information sent over a network. This post is meant to help users understand what FTPS is and what it is capable of doing, particularly in terms of enhancing the security of your file transfers.

The term "SSL file transfer" is also used to refer to file transfers using HTTPS, another secure network protocol. However, to keep this post concise, we'll just focus on FTPS.

SSL Certificates

At the heart of SSL (Secure Sockets Layer) file transfers are special files called SSL certificates. These files contain information that is vital to achieving security during file transfers. The two most common security functions of an SSL certificate is to help in authenticating the identity of a server and in facilitating encryption.

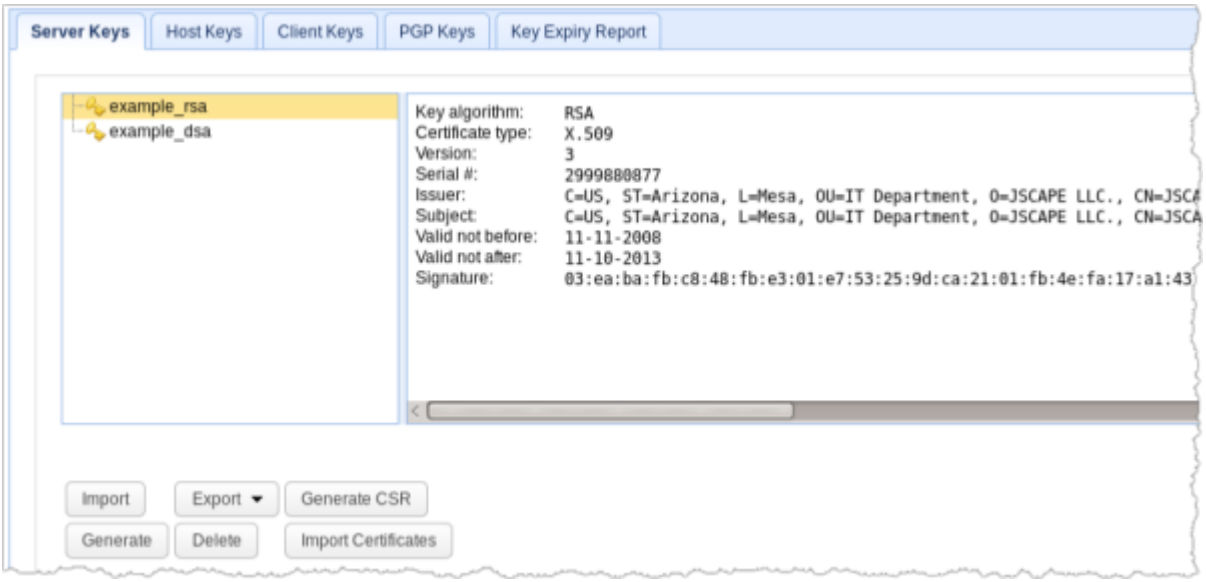
Some of the information found in an SSL certificate include:

- The dates over which the certificate could be considered valid;
- Information regarding the subject (usually the organization/company who owns the server or the server itself);
- The subject's public key (this is what is used for encryption);
- Information regarding the issuer of the certificate; and
- The digital signature of the issuer

All the information that should go into an SSL certificate is outlined by what is known as the X.509 standard.

The digital signature (which is virtually impossible to forge) is an attestation of the issuer that the public key belongs to the "subject" whose identity is being described in the certificate.

When used internally in an organization, SSL certificates are mostly self-signed. The person in charge of generating the certificates would use the company's certificate-generating program (For example, JSCAPE MFT Server's Key Manager.) to issue the certificates. The program would then automatically affix the company's signature to each generated certificate.



In the case of companies who offer file transfer services to a large number of external users, these companies normally issue what is known as a Certificate Signing Request (CSR) and submit it to a Certificate Authority or CA. The CA then puts the company under a vetting process to verify the company's true identity before issuing the requested digital certificate.

Certificate Authorities are independent, trusted bodies whose digital signature on a certificate is meant to assure end users that the bearer of the certificate is really who he claims to be.

How authentication is done in SSL File Transfers

When a user attempts to connect to your managed file transfer server via FTPS, the server will send the user an SSL certificate. The user (or the user's file transfer client) should then review the contents of that certificate to verify whether the server he is about to establish a connection with is in fact the server he wants to connect to.

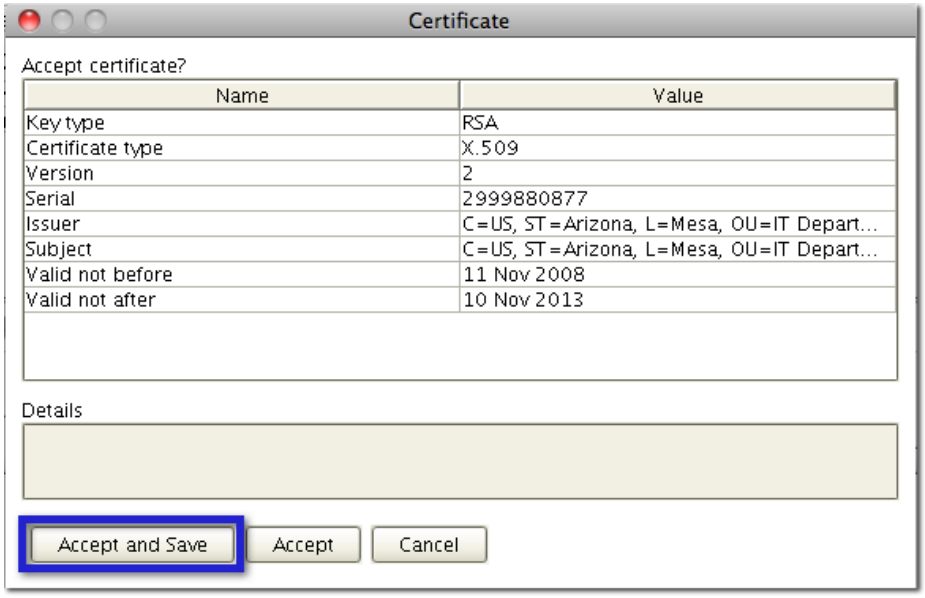
You see, it is possible for an attacker to go between a user and your managed file transfer server and then pretend to be your server. If that attacker succeeds in impersonating your server, the user can be duped into sending vital information to him instead. SSL certificates can prevent that from happening.

When a user does not recognize the SSL certificate coming from a server, that user can opt to cancel the connection. This would prevent any confidential information from falling into the wrong hands.

But how can you be sure a certificate itself is legit? Can't an attacker simply issue a fake certificate and use that to trick your users?

If your file transfer client is designed to identify certificates signed by CAs, it would prompt the user the moment it receives a certificate that hasn't been signed by one. If a CA's signature is found, the session will be allowed to proceed. The client (AnyClient is used in figure below) would also prompt the user if it receives a self-signed certificate. In this case, the user may contact the server admin to verify the certificate.

Prompting is mostly only done at the start of the first session. After verifying the certificate, the user can opt to save the certificate details into the client to avoid getting prompted again in future sessions.



How SSL certificates facilitate encryption

As mentioned earlier, one of the items in an SSL certificate is the server's public key. This public key has a corresponding private key, which is stored on the server. This pair of keys is responsible for encrypting the session key, which in turn is responsible for encrypting data exchanged over the FTPS connection.

Because encryption renders information unreadable, any attacker who manages to get hold of data during transmission would not be able to read, tamper with, or make unauthorized alterations to the contents. Therefore, even if files have to go through highly insecure networks like the Internet, their contents can be kept safe when sent through an SSL file transfer.

Summary

SSL file transfers or FTPS is one of the protocols supported by JSCAPE MFT Server. This article introduced the reader to essential features of FTPS such as SSL certificates, authentication, and encryption.