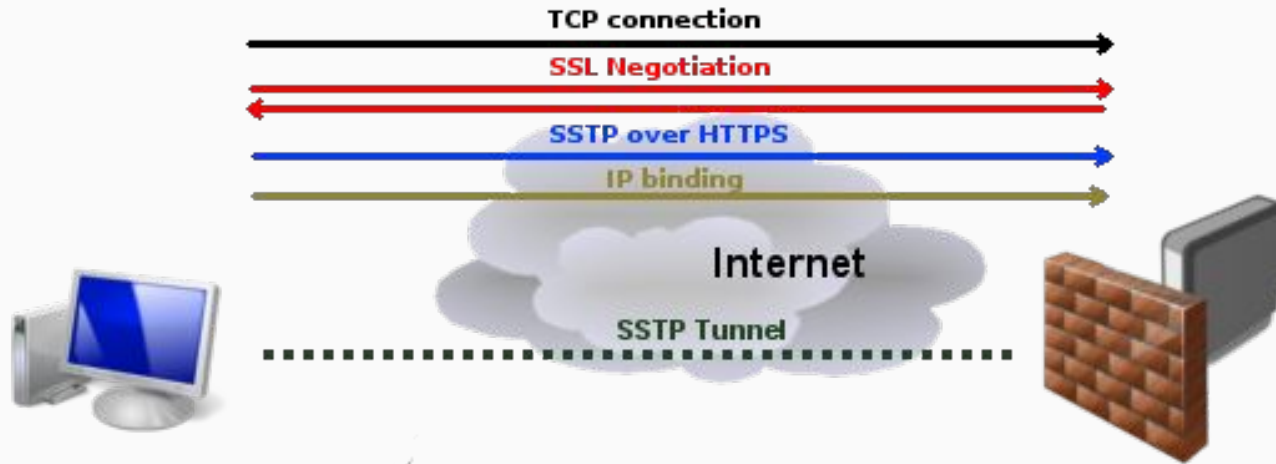


Certificados Digitales

SSL

SSTP



Un **certificado SSL** sirve para brindar seguridad al visitante de su página web, una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales. Las **siglas SSL** responden a los términos en inglés (**Secure Socket Layer**), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.

Al tener un certificado SSL confiable, nuestros datos están encriptados, en ese momento podemos asegurar que nadie puede leer su contenido. Todo esto nos lleva a entender que la tecnología que brinda un certificado SSL es la transmisión segura de información a través de internet, y así confirmar que los datos están libres de personas no deseadas.

Al tener un certificado SSL confiable, nuestros datos están encriptados, en ese momento podemos asegurar que nadie puede leer su contenido. Todo esto nos lleva a entender que la tecnología que brinda un certificado SSL es la transmisión segura de información a través de internet, y así confirmar que los datos están libres de personas no deseadas.

Tipos de Certificados

Certificados con validación de Dominio

Certificados de validación de organización

Certificados de validación extendida

Certificados autofirmados

Los servidores SSTP deben autenticarse en la fase SSL/TLS.
Los clientes SSTP pueden ser autenticados en la fase SSL/TLS pero obligatoriamente deben ser autenticados en la fase PPP.
El uso de PPP permite el soporte de métodos de autenticación común como EAP-TLS y MS-CHAP

Cómo se ve el menú de certificados en Mikrotik

New Certificate

General Key Usage Status

Key Usage:

☐ digital signature	☐ content commitment
☐ key encipherment	☐ data encipherment
☐ key agreement	☒ key cert. sign
☒ crl sign	☐ encipher only
☐ decipher only	☐ dvcs
☐ server gated crypto	☐ ocsp sign
☐ timestamp	☐ ipsec user
☐ ipsec tunnel	☐ ipsec end system
☐ email protect	☐ code sign
☐ tls client	☐ tls server

OK

Cancel

Apply

Copy

Remove

Sign

Sign via SCEP

Import

Card Reinstall

Card Verify

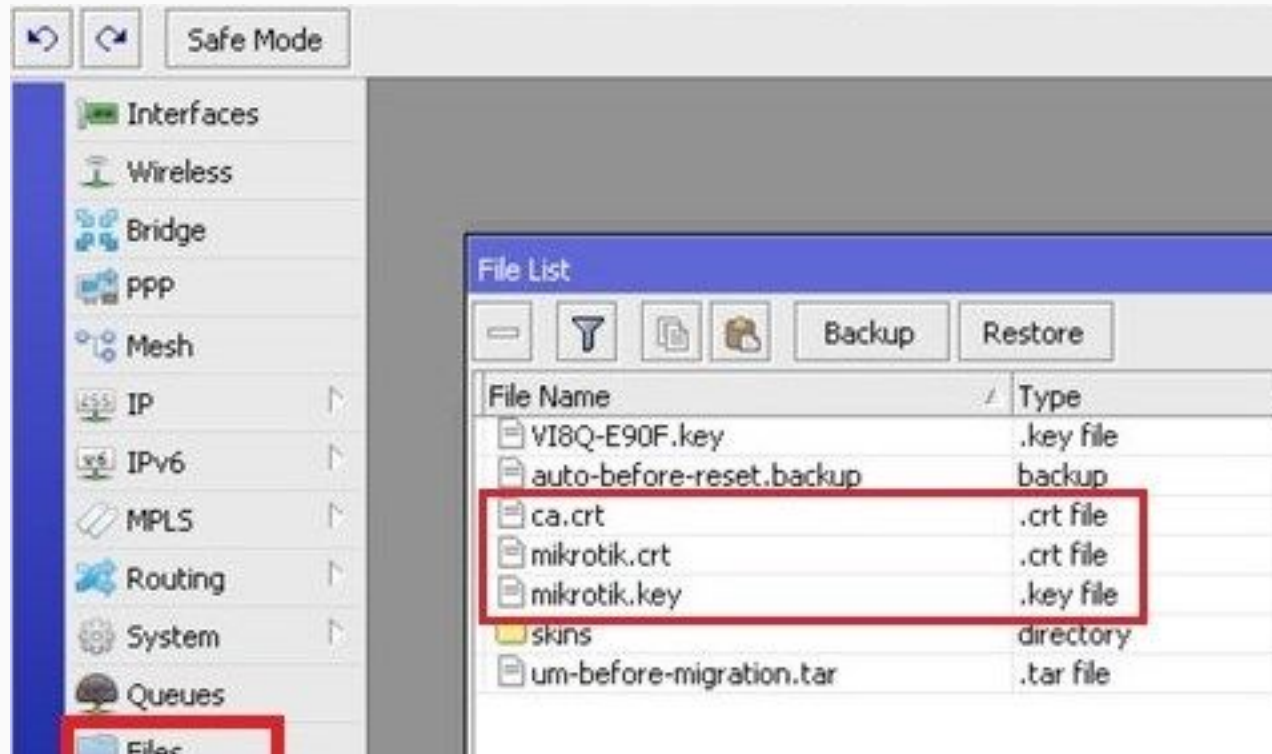
Set CA Passphrase

Export

Revoke

private key: crl expired smart card key: trusted

Dónde se guardan los certificados en Mikrotik



Telecomunicaciones de voz y Data

Stevenson Canó

