

Criptografía

Profesor: Melvin Fernández Ch.

Video 12



fidÉlitas
Virtual

Funciones de Hash y protocolos de seguridad



Módulo: 4



Certificado Digital

- Documento electrónico que usa la firma digital de una tercera parte de confianza para vincular una clave pública con una identidad.
- Se confía en una clave porque se sabe de dónde procede:
 - Los certificados se verifican siguiendo la cadena de firmas hacia atrás, hasta que se encuentra un certificado raíz de confianza (directa).
 - Usada en PKI X.509.
 - Usada para verificar que una clave pública pertenece a un individuo, organización o servicio.

Certificado Digital

- Proporciona el servicio de no repudio.

Certificado Digital

- Cada certificado incluye un periodo de validez:
 - Se emite un nuevo certificado justo antes de que expire el antiguo.
- Puede ser necesario revocar un certificado antes de que expire debido a las siguientes razones:
 - Se cree que la clave privada ha sido comprometida.
 - El usuario ya no está certificado por esta CA.
 - El nombre de sujeto ha cambiado, el certificado ha sido sustituido, o el certificado no se emitió de conformidad con las políticas de la CA.
 - Se cree que el certificado de la CA ha sido comprometido.

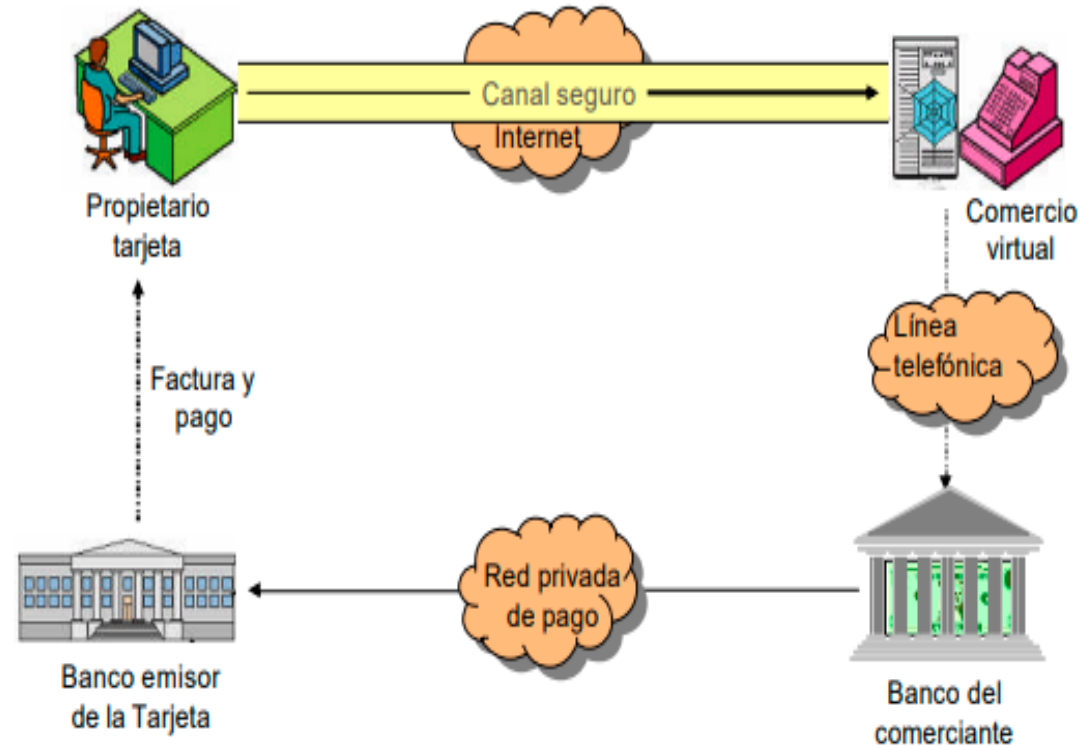
Creación y verificación de certificados



(Ribera, 2022)

Protocolo SSL

- El protocolo SSL fue desarrollado por Netscape con el fin de asegurar las transacciones en línea.
- Permite al usuario sin un certificado enviar eficientemente los datos de la tarjeta de crédito.

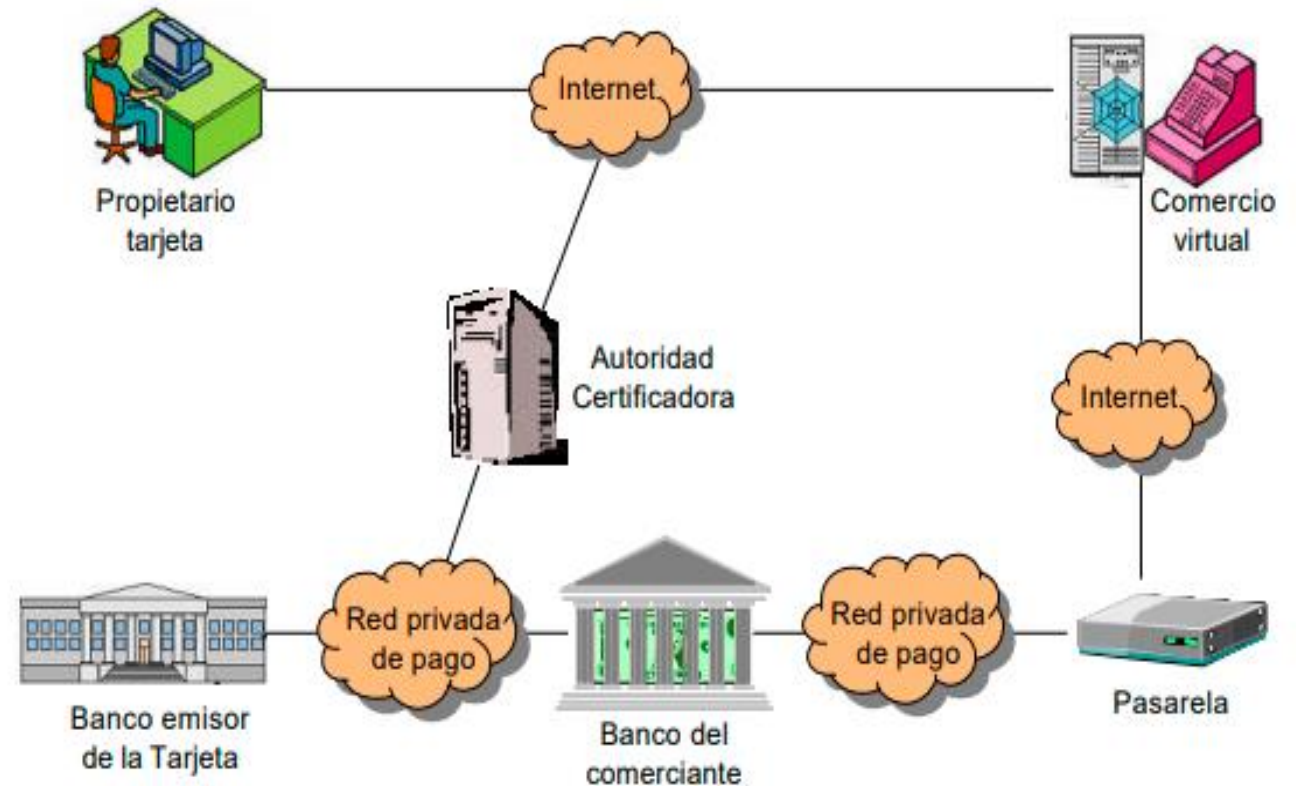


Características de SSL


- El protocolo SSL asegura la transmisión de datos con una combinación de cifrado de clave pública y la clave simétrica.
- SSL comienza siempre con un apretón de manos que permite al servidor que se autentifique al cliente. Si el servidor no puede ser autenticado, la conexión no puede ser establecida.

Protocolo SET

- El protocolo SET fue desarrollado conjuntamente por MasterCard y Visa con el objetivo de asegurar los navegadores web para transacciones de tarjetas bancarias.
- Actualmente es uno de los modos más seguros de realizar transacciones con tarjetas de crédito a través de internet.



Características de SET

- SET utiliza dos firmas para asegurar una transacción.
 - SET requiere la compra de software a utilizar para un sitio de comercio electrónico. El diseño del protocolo SET requiere la instalación de un monedero electrónico en el cliente.
- 
- A decorative graphic consisting of several parallel blue diagonal lines is located in the bottom left corner of the slide.

Gracias

