Unidad 0 – Precurso

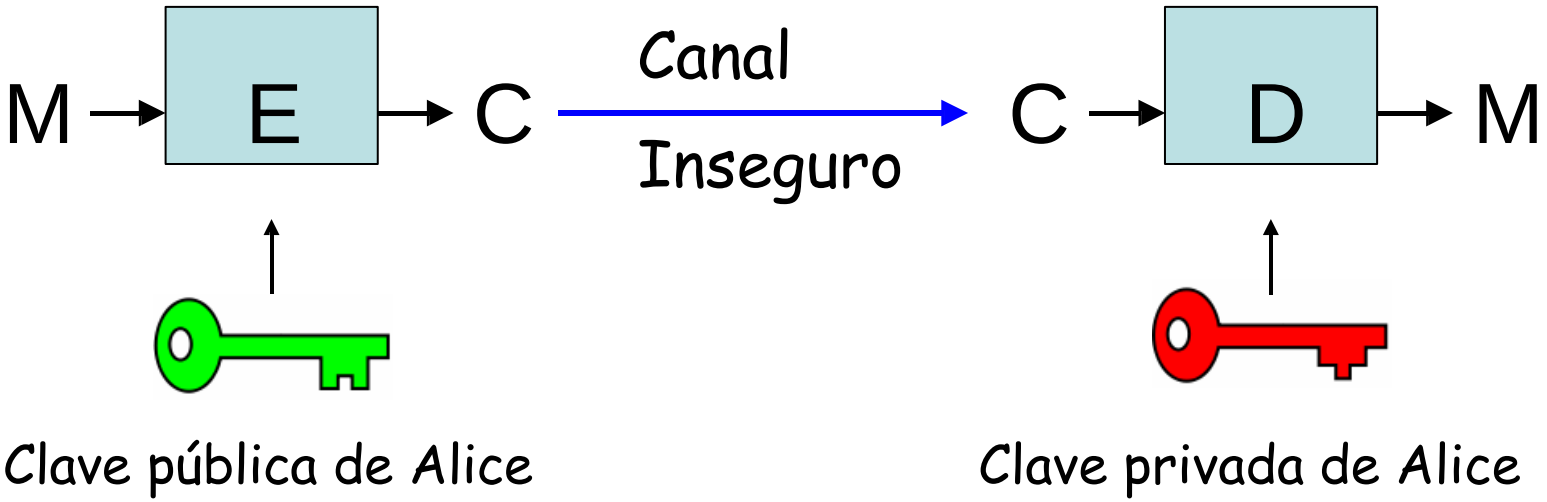
Módulo 4
Fundamentos de Criptografía
PKI

THE BRIDGE DIGITAL TALENT ACCELERATOR

Cifrado de clave pública

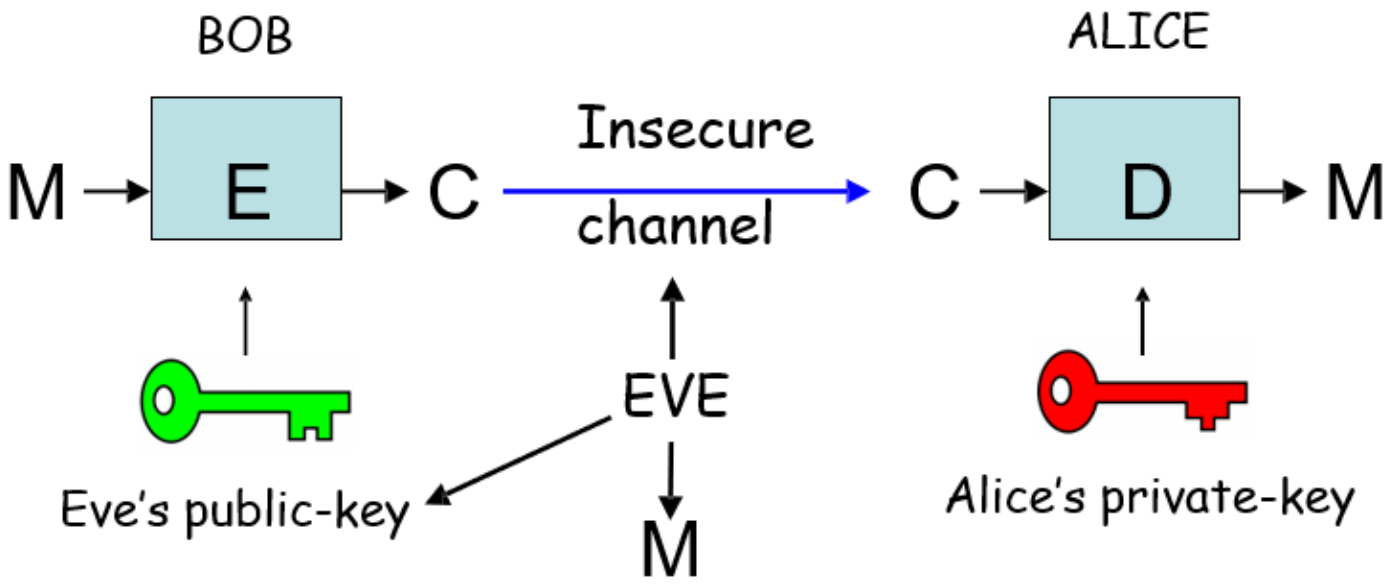
BOB

ALICE



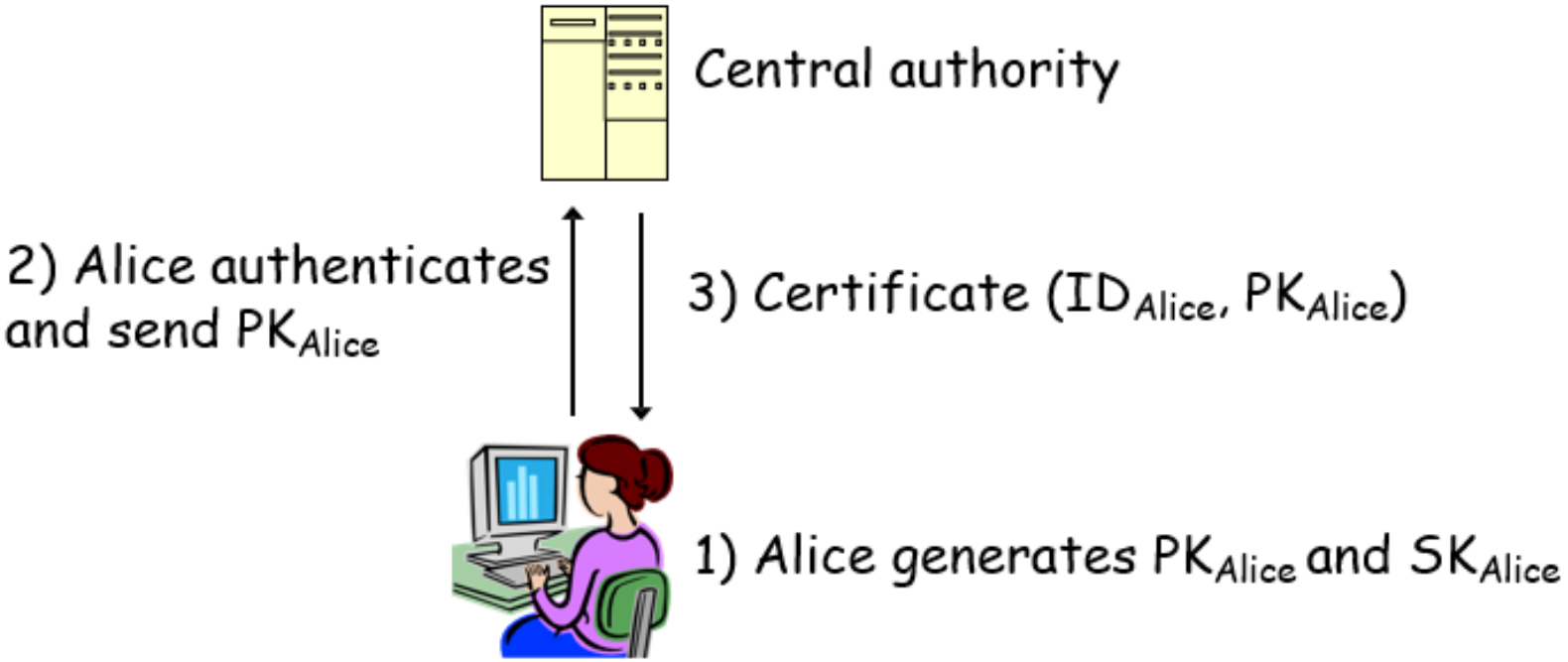
Autenticación

- Las claves públicas deben ser autenticadas
  - Bob necesita estar seguro de que la clave pública pertenece a Alice.
  - De lo contrario, puede ocurrir un ataque de suplantación de identidad.



Infraestructura de Clave Pública

- Una autoridad central vincula las claves públicas a las identidades.
- La clave pública se almacena en un certificado.



Certificado de clave pública

- Certificado:
  - La firma de la autoridad certificadora une una clave pública con una identidad.
  - Bob puede estar seguro de que la clave pública pertenece a Alice al verificar la firma usando la clave pública de la CA (Central Authority).
  - Todos los participantes confían en la CA.

Entidad certificadora

- La CA se encarga de crear certificados con la clave publica que atestiguan que la clave privada que esta en el certificado se corresponde con la identidad del certificado:
  - La CA debe verificar la identidad del usuario antes de emitir el certificado.
  - Si la clave privada de la CA se ve comprometida, se pierde la seguridad.
- Mayores proveedores de certificados:
  - Verisign, Geotrust, Global Trusted Sign (GTS)

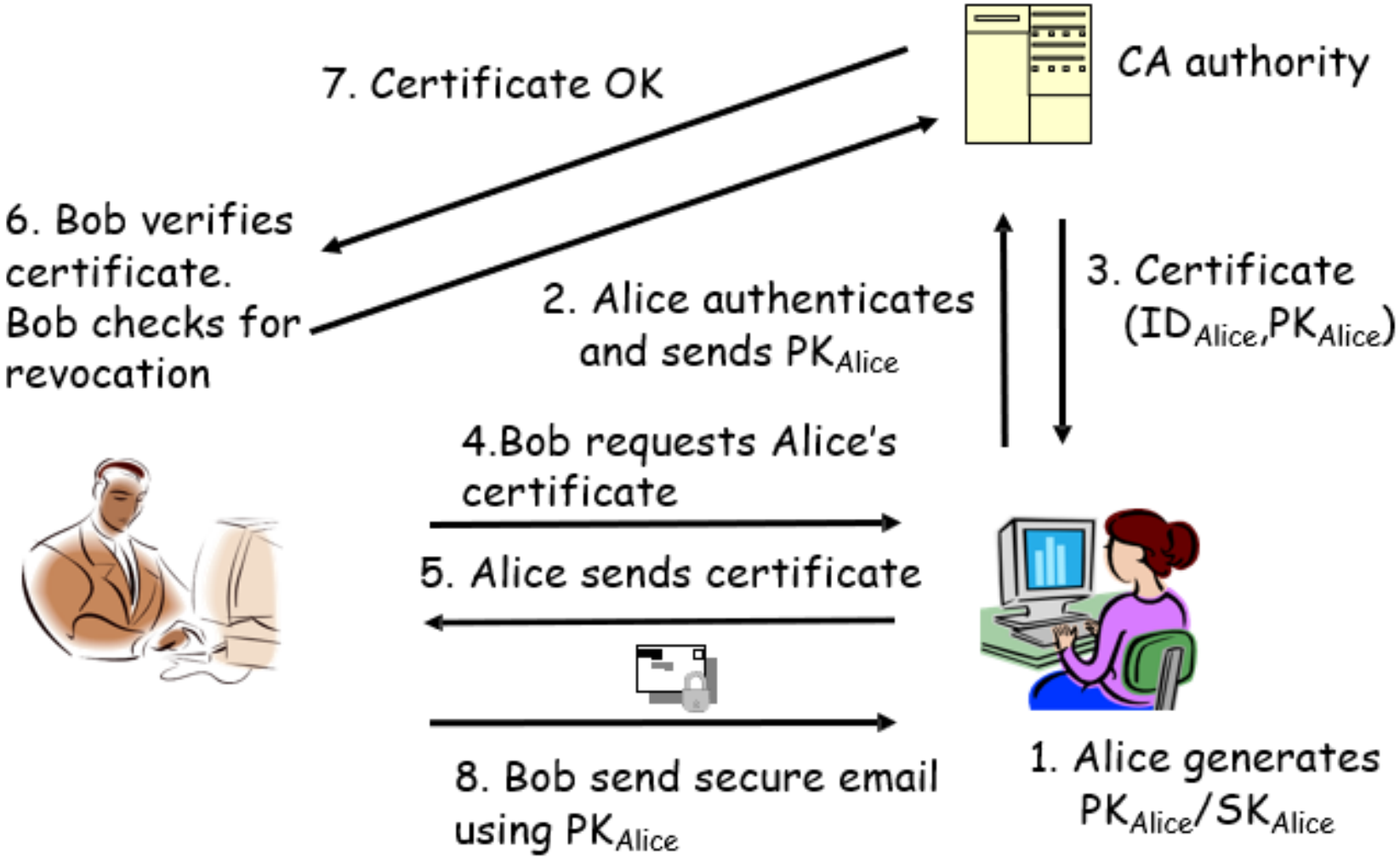
Certificado de Clave Pública

- Un certificado de clave pública puede incluir:
  - Clave pública del usuario.
  - Nombre (persona, equipo o empresa).
  - Período de validez.
  - Ubicación (URL) de un centro de revocación.
  - Firma digital del certificado, producida por la clave privada de la CA.

Revocación de certificado

- Revocación del certificado cuando:
  - La clave privada está comprometida.
  - La identidad y la PK (clave publica) no se corresponden.
- Un usuario siempre debe comprobar la validez de un certificado
  - La CA puede mantener una lista de revocación de certificados (CRL)
  - Debe estar actualizada y fácilmente disponible.

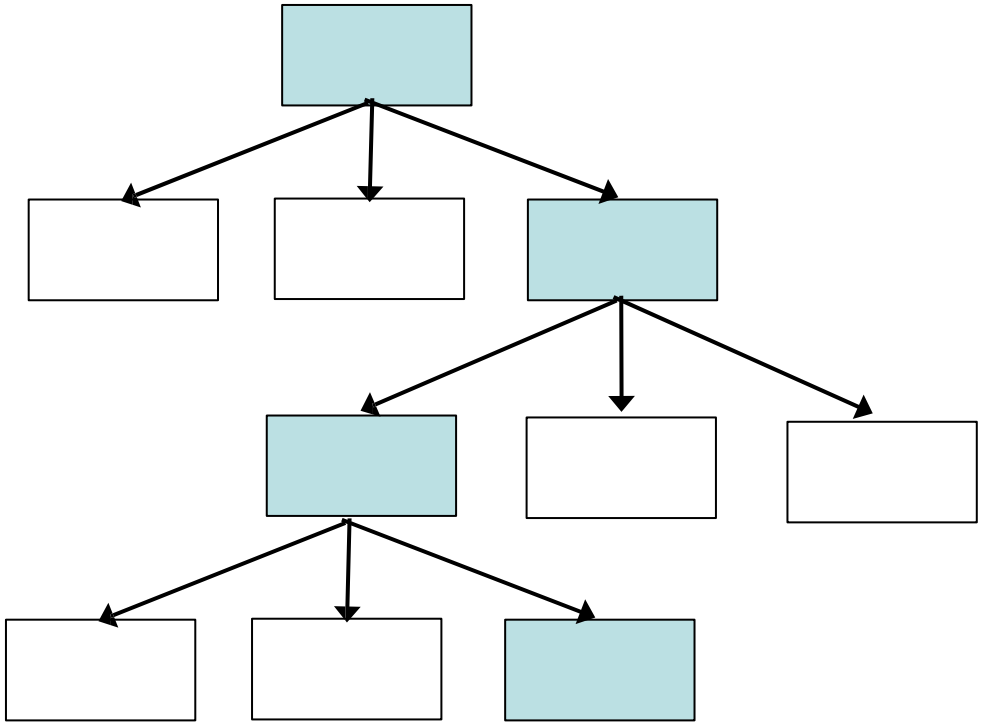
PKI o Cifrado en la Infraestructura de Clave Pública



Jerarquía de los certificados

- Es posible que Bob no conozca la CA de Alice.
- La CA puede ser la empresa de Alice y Bob puede trabajar para una empresa diferente.
- El certificado de Alice puede incluir la clave pública de su CA firmada por una CA2 de nivel superior.
- Esta CA2 puede ser reconocida por Bob.
- Finalmente, esto conduce a una jerarquía de certificados.

Jerarquía de los certificados



Ejemplo:

CA País (root certificate)

CA Comunidad Autónoma

CA Provincia

CA Municipio…

Estándar de certificado

- X509
  - Estándar de certificado más común.
  - Especifica el formato del certificado y la ruta de validación del certificado.
  - Asume que hay una CA superior que valida.
  - El certificado raíz es de confianza implícita.
  - Tiene una lista de revocación implementada (CRL).

Certificado Root

- Es el que está en lo más alto de la cadena, lo más alto de la jerarquía.
- Típicamente en el estándar X509.
- Confianza implícita.
- Incluido en los navegadores web.
- Utilizado para conexiones SSL/TLS.
- En la práctica, la jerarquía es plana.

PGP(Pretty Good Privacy)

- Software que proporciona cifrado y firma de correo electrónico.
- Primera versión de P. Zimmermann en 1991.
- Utiliza el cifrado PK para cifrar una clave compartida, que se utiliza para cifrar el mensaje.
- Por comentar cómo funciona PGP… Usa la clave pública para cifrar un mensaje de correo y con la privada lo descifras, es el funcionamiento habitual del cifrado asimétrico que venimos viendo.
- Ahora el reemplazo es GPG (GNU Privacy Guard), para cifrar nuestro correo, que lo que hace es metafóricamente ponerle un "sobre" a nuestra carta para que sólo el destinatario la pueda abrir… GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios.

PGP(Pretty Good Privacy)

- En cuanto a la firma digital:
  - Al enviar un mensaje m, Bob puede firmar m con su clave privada.
  - Alice verifica la firma con el PK de Bob, de modo que Alice está convencida de que Bob envió la m y la recibió sin cambios.
  - Firma RSA o firma DSA.
  - Se usa de forma predeterminada con el cifrado, pero también se puede usar para texto plano o sin cifrar.

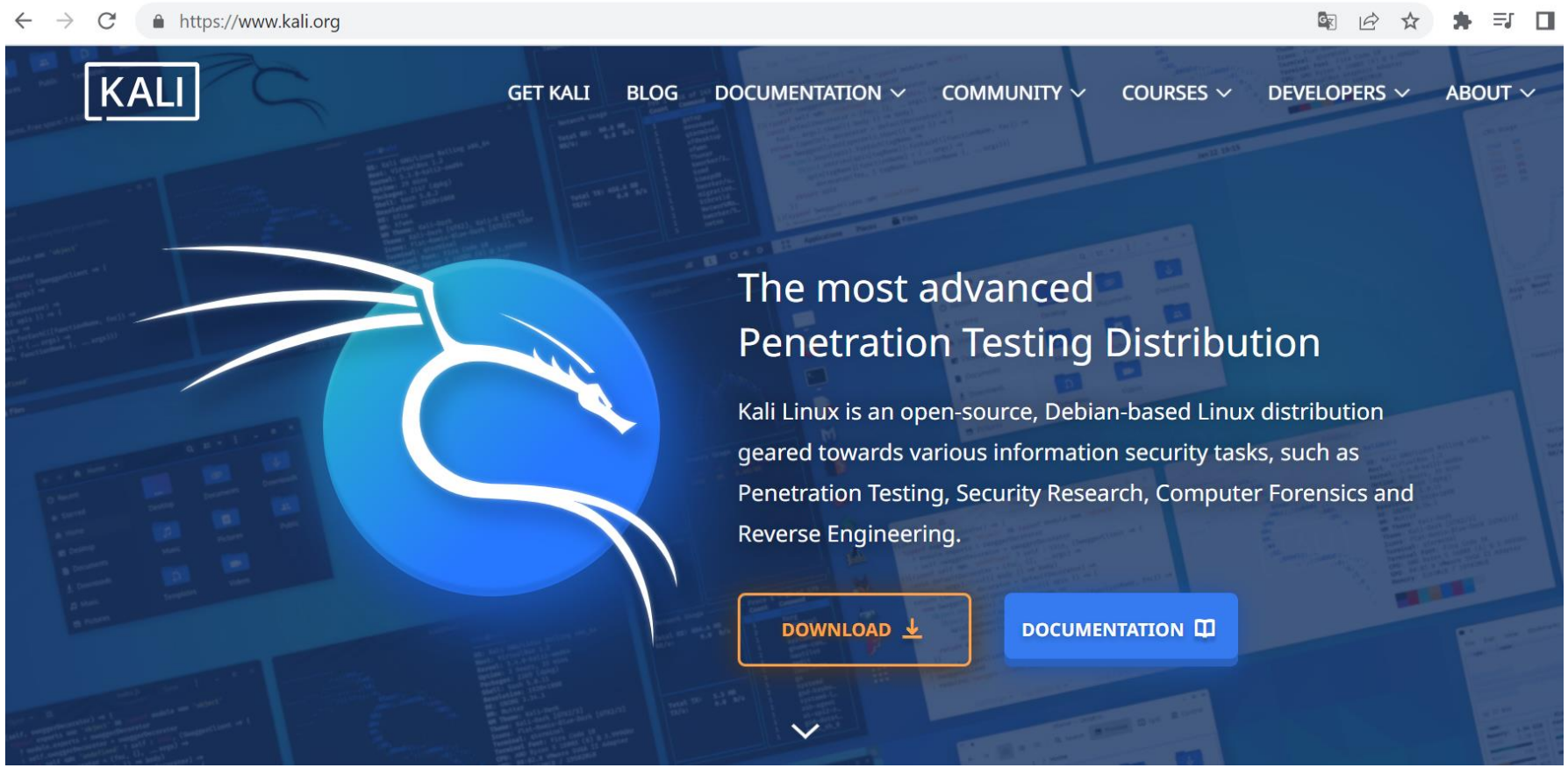
SSL (Secure Sockets Layer) y TLS (Transport Layer Security)

- **Secure Sockets Layer** (capa de sockets seguros), es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los atacantes lean y modifiquen cualquier dato que se transfiera.
- SSL 3.0 es similar a TLS 1.0
  - Garantiza la confidencialidad, integridad y autenticidad a través de Internet (triada CIA).

- **Transport Layer Security** (seguridad de la capa de transporte) es una versión actualizada y más segura de SSL.
- Hay que confiar en el navegador que instalamos.

Aplicaciones de SSL

- Utilizada principalmente para asegurar HTTP => HTTPS



Las tarjetas de crédito a través de https

- https solo protege el número de tarjeta de crédito durante el tránsito entre la computadora del usuario y el servidor.
  - No protege contra un ataque al servidor.
- El ataque al servidor suele ser más fácil que la intercepción en tránsito.
  - Número de tarjeta de crédito a menudo guardado en una base de datos en el sitio del comerciante.
  - Los ataques generalmente se concentran en el servidor y la base de datos.