TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2-UNIDAD 2

TIC

Universidad Tecnológica de Pereira

faceIT

Certificados digitales

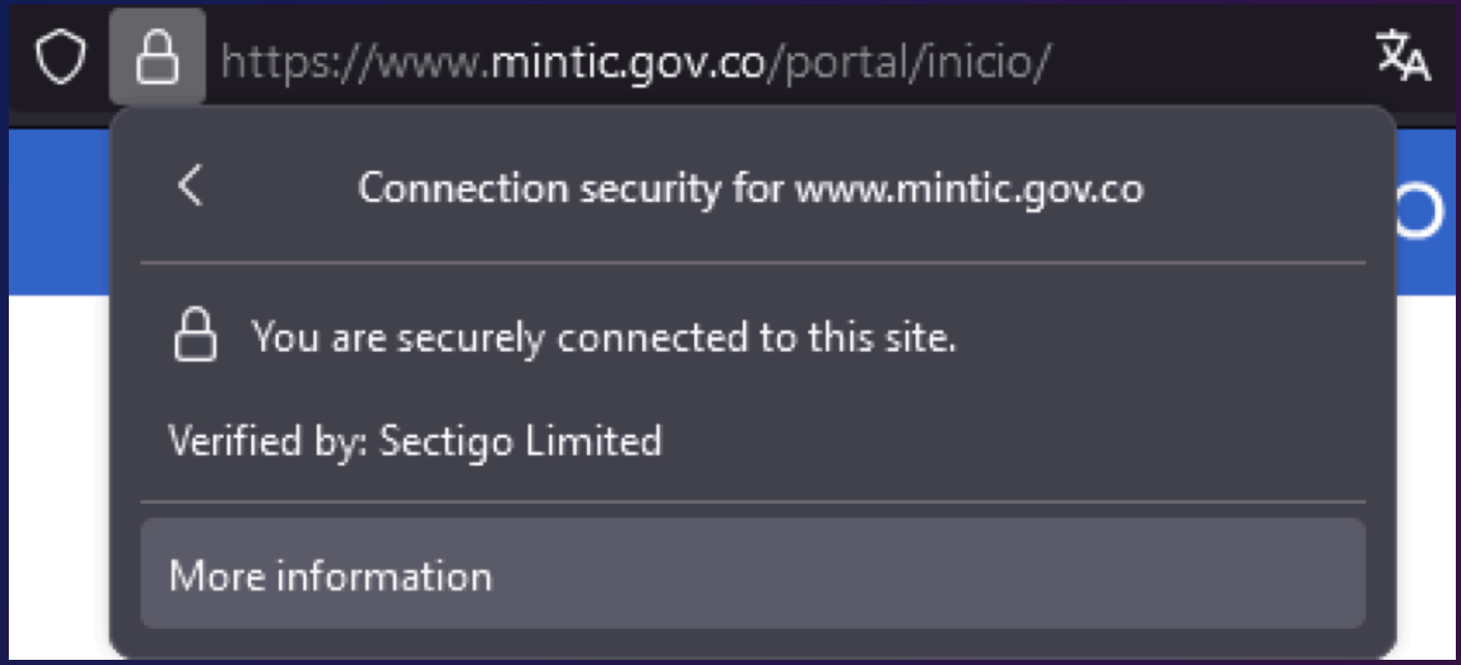
En las comunicaciones digitales existe la posibilidad de que un atacante intercepte un mensaje, lo altere y envíe la copia alterada como si fuese legítima. Para evitar que los mensajes alterados sean tenidos en cuenta se emplean certificados digitales.
Un certificado digital es una credencial emitida por una entidad de certificación (CA o certification authorithy) que se usa para comprobar la identidad de la persona o entidad a la que se emite el certificado. Esta entidad se conoce como el firmante.

Para generar un certificado, la autoridad requiere que el firmante envíe su información junto con una clave pública (generada a partir de un par clave pública y privada). La autoridad valida los datos y emite un certificado, que tendrá asociada la información del firmante junto con la clave pública. El firmante deberá conservar la clave privada y guardarla de forma segura.

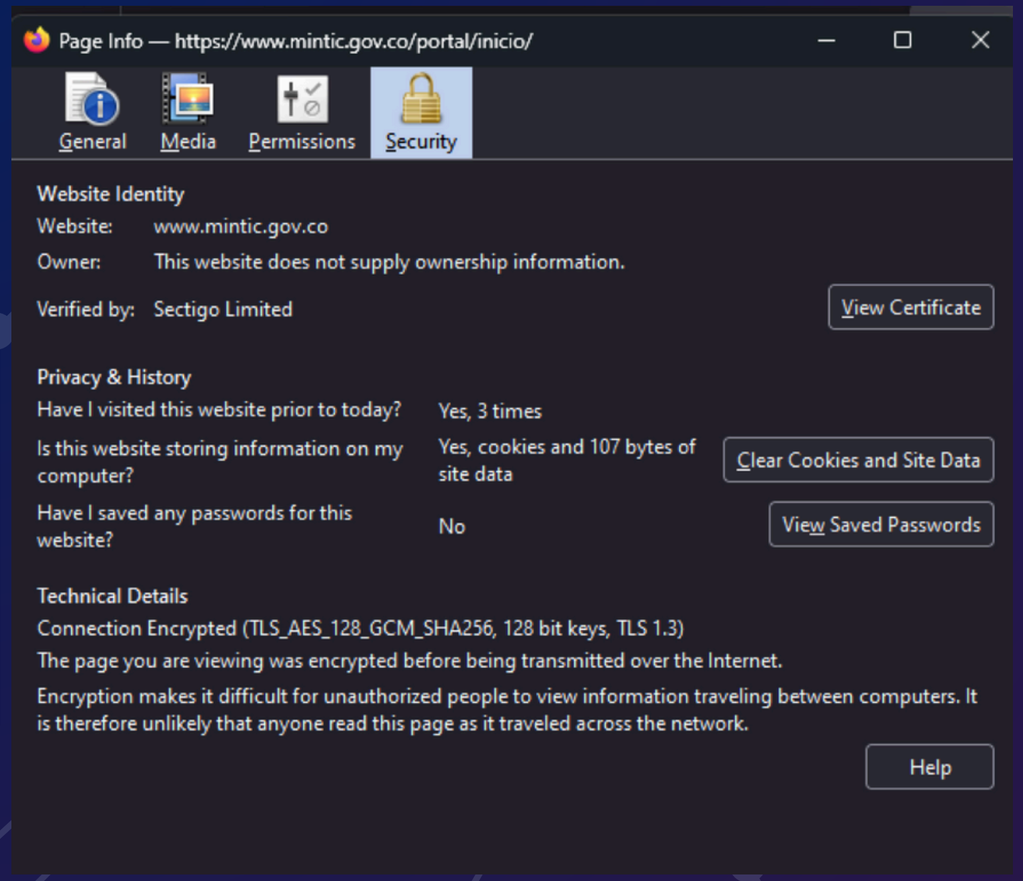
Los certificados tienden a tener una fecha de expiración (usualmente un año). Cuando un certificado digital expira, los navegadores y los programas suelen mostrar una advertencia que indica que no es posible confirmar la identidad del firmante.

Generalmente, los certificados digitales se emplean en comunicaciones web. Los certificados son cargados a los servidores, quienes cifran y envían la información

con la clave pública, permitiendo a los navegadores validar la identidad del firmante.



En la imagen se aprecia cómo un navegador muestra la información de un sitio web con un certificado vigente (sitio del ministerio de las tics) También se puede ver la información detallada de la autoridad que emite el certificado.



Usualmente el navegador almacena las cabeceras HTTPs de la comunicación, en donde se tiene los detalles del dueño del sitio web, el nombre, la autoridad y los algoritmos criptográficos empleados para el cifrado de los datos.

Cuando la información viene firmada con un certificado, es posible validar que los paquetes no han sido alterados y que su origen es legítimo. Esto reduce los ataques orientados en el navegador. Un atacante no podría generar mensajes cifrados válidos ya que no posee la clave privada. Un lector puede validar la identidad de la comunicación mediante el certificado y la clave pública emitida junto con los datos.