Certificado Digital

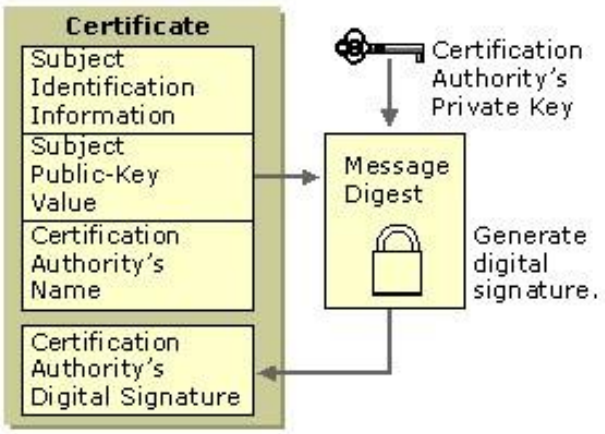
Los certificados digitales son credenciales electrónicas usadas para certificar las identidades online de personas, entidades o redes mediante el uso de una infraestructura de clave pública (**PKI**). Los certificados digitales son emitidos por CAs, que tienen que verificar la identidad del solicitante de un certificado antes de su expedición. Son principalmente utilizados para la securización de las comunicaciones digitales vía el protocolo **TLS** (Transport Layer Security), como por ejemplo, en las comunicaciones web (**HTTPS**) o las comunicaciones por email (**SMTP, IMAP, POP3**).

Los certificados digitales garantizan:

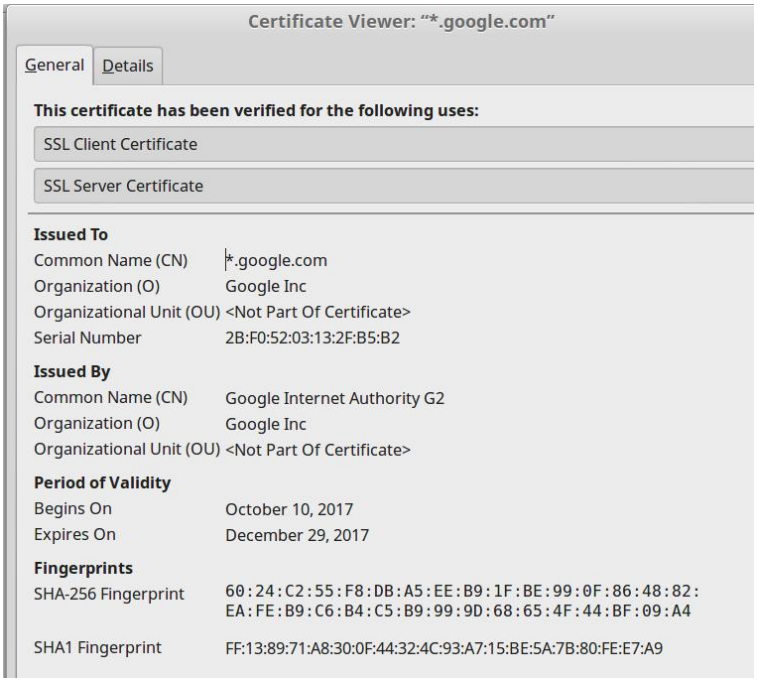
- Identificación / Autentificación
- Confidencialidad
- Integridad
- No Repudio
- Control de acceso

Los certificados digitales contienen información que identifica al propietario del certificado, y la clave pública del propietario. Además se incluye la información de la CA que ha emitido el certificado, así como una firma digital de la CA. Esto es debido a que el contenido de los certificado digitales están organizados según la especificación X.509 version 3, que es la recomendada por la International Telecommunications Union (ITU) desde 1988.

En la siguiente figura se muestra como una CA emite un certificado.

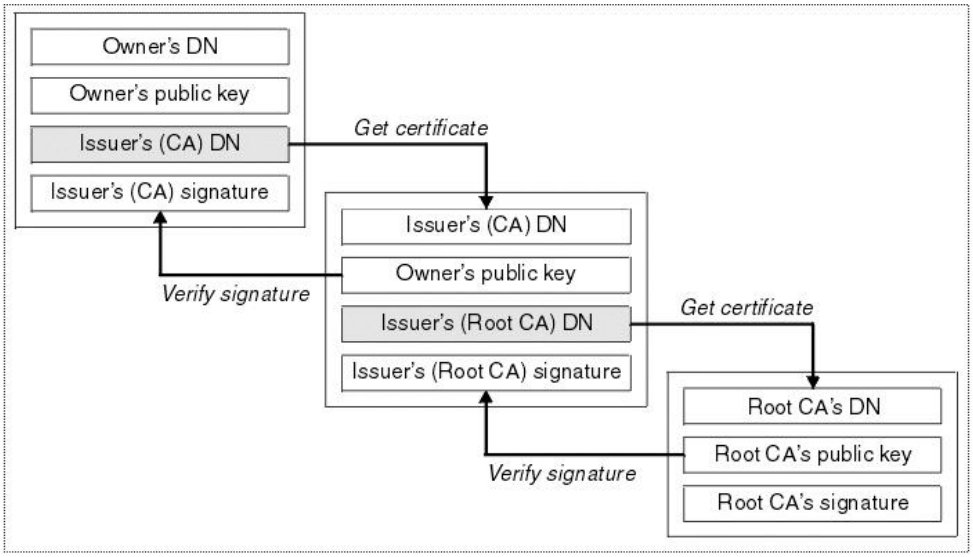


A continuación, se puede ver un ejemplo de certificado emitido a la entidad de google.com.



*** <u>Cadena de certificación</u>**

Un certificado está asociado con una cadena de certificados llamada cadena de confianza, dependiendo de la estructura jerarquica de la CA. Que se puede observar en la siguiente figura.



Durante la validación del certificado, se necesita validar la firma buscando la clave pública de la siguiente CA. El proceso continúa hasta llegar al certificado raíz, ya que las CA raíz están auto-firmadas y son confiadas por las aplicaciones, como navegadores.