Certificados

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Certificados

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Certificados digitales

- Un certificado digital consiste en que una entidad “de confianza” firme mediante su clave privada, la clave pública de un usuario
- Sirve para certificar que el usuario es quien dice ser
- Depende de la confianza en la entidad que lo certifica

Certificados digitales

- Siguen el estándar X.509
- Validez != Confianza
  - Validez: cumple los requisitos de una firma (caducidad, etc.)
  - Confianza: nos podemos fiar de esa firma
- Una firma puede ser válida, pero no de confianza
- Una firma de confianza que no sea válida no tiene sentido

Certificados digitales

Una autoridad de certificación (AC) certifica la validez de una firma

- Prestadores de Servicios de Certificación (PSC): Ley de Firma Electrónica (Ley 59/2003, LFE), Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007, LAESCP)
- Los PSCs deben proporcionar un método de consulta de la vigencia de sus certificados: Sólo las Administraciones Públicas tienen la obligación de que sea gratuito

Certificados digitales

Jerarquía de certificación (RFC 1422)

Internet Policy Registration Authority (IPRA) >> Policy Certification Authorities (PCA) >> Certification Authorities (CA): Verisign, Thawte, GeoTrust, RapidSSL, DigiCertSSL

Un AC debe

- Mantener una base de datos de nombres distinguidos (ND) y de ACs subordinadas
- Permitir la revocación de certificados:
  - Clave privada del usuario comprometida
  - AC ha emitido un certificado a quien no debía
  - El usuario cambia de AC
  - Violación de la seguridad de la AC
- CRL, Certification Revocation List: ejemplo GeoTrust

Un AC debe

- El protocolo OCSP (Online Certificate Status Protocol RFC 2560) permite validar el estado de un certificado digital de manera online
- Es más eficiente que la verificación mediante Listas de Revocación de Certificados (CRL)
- Ventaja: su actualización constante
- Desventaja: necesidad de conexión para la comprobación

Certificados digitales

Cada AC que proporciona el servicio, mantiene un servidor OCSP

Este servicio responde a las aplicaciones cliente que remitan una petición estandarizada y sepan interpretar la respuesta

Certificados digitales

Tipos de certificados de clave pública:

- Certificado de autoridad
- Certificado de servidor
- Certificado personal
- Certificado de productor de software

Certificados digitales

Componentes de un certificado:

- Versión
- Número de serie
- Identificador del algoritmo de firmado
- Nombre del emisor
- Periodo de validez
- Nombre del sujeto

Certificados digitales

Con un certificado digital conseguimos:

- Confidencialidad al poder encriptar la información
- Integridad al poder realizar hash de la información y poder firmarla
- Autenticidad al venir firmada la información
- No repudio al firmar la información