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

Public Key Infraestructure (PKI)

Infraestructura que permite enlazar entidades/personas con sus claves públicas

- Web of Trust: PKI sin autoridad central, cualquiera puede certificar
- Certificados: PKI con autoridad central, solo los CA (Autoridad de Certificación) pueden certificar

Autoridad de Certificación

- Una entidad (AC) certifica que el usuario/entidad (su clave pública) es quien dice ser (Depende de la confianza en la AC que lo certifica)
- Almacena las claves públicas por nosotros

Certificados digitales

- La AC emite un certificado digital
- En el certificado digital el CA firma mediante su clave privada la clave pública de un usuario/entidad

Agencia de Registro

- Independiente de AC
- Comprobar la identidad del usuario/entidad antes de emitir el certificado
- Agencias tributarias, seguridad social, zuzenean, …

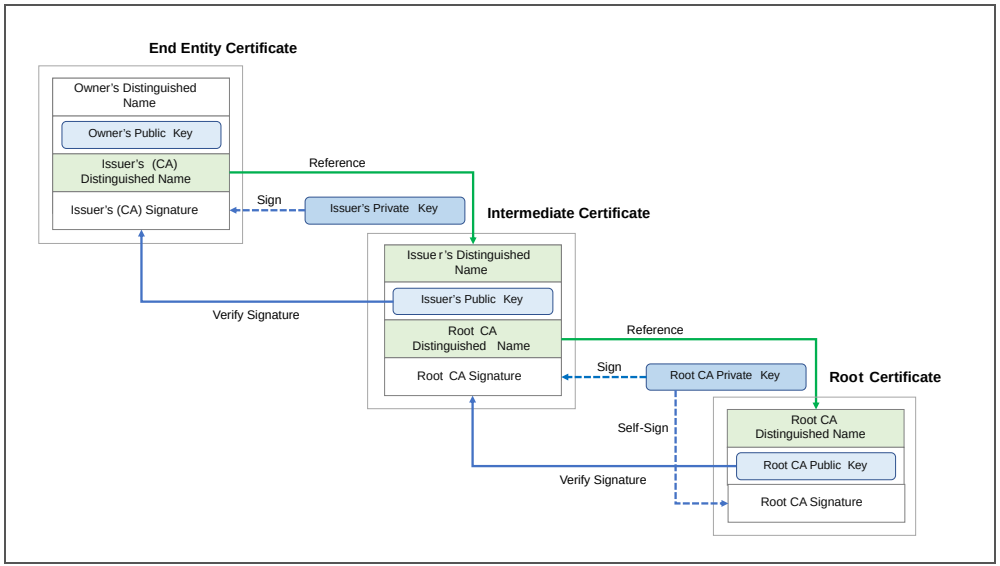
Certificados digitales: X.509

- Estándar X.509 de International Telecommunication Union (ITU)
- Contiene una identidad (Persona, entidad, ...) y una clave pública
- Firmado por un CA - el poseedor de la clave pública puede:
  - Firmar con su clave privada (Esa firma se puede comprobar con la clave publica firmada por el AC, y que por tanto es de confianza)
  - Establecer comunicaciones seguras (SSL, ...)
- El CA debe mantener una base de datos de nombres distinguidos (ND) y de CAs subordinadas

Certificados digitales: X.509

- Cadena de confianza (Certification path validation algorithm)
- Certificate Revocation List (CRL)

Cadena de confianza



https://upload.wikimedia.org/wikipedia/commons/0/02/Chain_Of_Trust.svg

Certificate Revocation List (CRL)

Una lista pública de certificados revocados, mantenida por el AC

Revocar: AC declara que ese certificado no es confiable

Certificate Revocation List (CRL)

Definido en RFC 5280

Posibles razones para revocación: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn, aACompromise

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 CRLs: CRLs en desuso
- Ventaja: su actualización constante
- Desventaja: necesidad de conexión para la comprobación

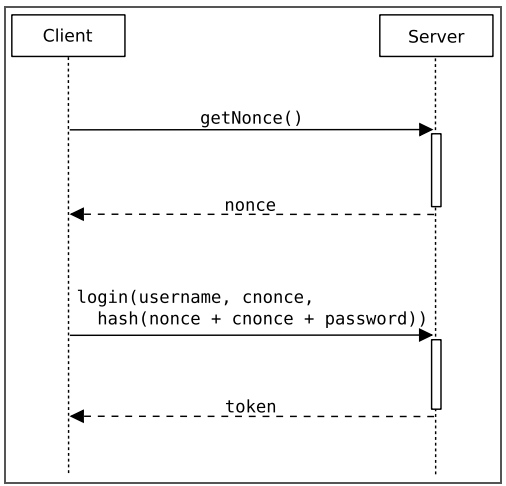
OCSP (Online Certificate Status Protocol)

- 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

OCSP: Replay attack

- El atacante retiene un certificado válido hasta después de su revocación, y entonces lo envia al cliente
- Solución: uso de **nonce**

OCSP: uso de nonce



https://commons.wikimedia.org/wiki/File:Nonce-cnonce-uml.svg

Estructura de un certificado

Certificate

- Version Number
- Serial Number
- Signature Algorithm ID
- Issuer Name
- Validity period
- Subject name

Estructura de un certificado

```
Subject Public Key Info
    Public Key Algorithm
    Subject Public Key
...
Certificate Signature Algorithm
Certificate Signature
```

Estructura de un certificado

Distinguished Name

- C: country
- SP: state or province
- Locality: L
- Organization: O
- Organizational Unit: OU
- Common Name: CN

Estructura de un certificado

IZENPE

Descarga de certificados izenpe

Política de certificación: certification practice statement

Estructura de un certificado

Izenpe.com

Identity: Izenpe.com
Verified by: Izenpe.com
Expires: 13/12/37

✓ Details

Subject Name

C (Country):	ES
O (Organization):	IZENPE S.A.
CN (Common Name):	Izenpe.com

Issuer Name

C (Country):	ES
O (Organization):	IZENPE S.A.
CN (Common Name):	Izenpe.com

Issued Certificate

Version:	3
Serial Number:	00 B0 B7 5A 16 48 5F BF E1 CB F5 8B D7 19 E6 7D
Not Valid Before:	2007-12-13
Not Valid After:	2037-12-13

Certificate Fingerprints

SHA1:	2F 78 3D 25 52 18 A7 4A 65 39 71 B5 2C A2 9C 45 15 6F E9 19
MD5:	A6 B0 CD 85 80 DA 5C 50 34 A3 39 90 2F 55 67 73

Public Key Info

Key Algorithm:	RSA
Key Parameters:	05 00
Key Size:	4096
Key SHA1 Fingerprint:	C4 52 72 20 A9 5B C0 6E 9D 4B F2 0B 21 12 3C EB 3A 0B 6B 6F
Public Key:	30 82 02 0A 02 82 02 01 00 C9 D3 7A CA 0F 1E AC A7 86 E8 16 65 6A B1 C2 1B 45 32 71 95 D9 FE 10 5B CC 99 15 DA 81 A2 87 F4 7B 6E 26 77 89 58 AD D6 EB 0C B2 41 7A 73 6E 6D DB 7A 78 41 E9 08 88 12 7E 87 2E C3 EC 3B 34 C5 95 41 69 7E 75 C2 3C 20 C5 61 BA 51 47 A0 20 90 93 A1 90 4B F3 4E 7C 85 45 54 9A D1 05 87 22 BC AD 1B A3 FE 26 B5 15 F3 A7 FC 84 19 E9 EC A1 88 B4 44 69 84 83 F3 89 D1 74 06 A9 CC 0B D6 C2 CB A9 6F 44 E5 1B 41 CF E1 86 A7 CA D0 6A 9F BC 4C 8D 06 33 5A A2 85 E5 90 35 A0 62 5C 16 4E F0 E3 A2 ED 7B 70 D7 02 D6 ED 87 18 28 2C 04 24 4C 77 E4 48 8A 1A C6 3B 9A D4 0F CA FA 75 D2 01 40 5A 8D 79 BF AE 05 46 E5 F1 A8 16 EC 47 A4 17 02 03 01 00 01

Subject Alternative Names

Email:	info@izenpe.com
Directory Name:	O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8, STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
Critical:	No

Basic Constraints

Certificate Authority:	Yes
Max Path Length:	Unlimited
Critical:	Yes

Key Usage

Usages:	Certificate signature ↵ Revocation list signature
Critical:	Yes

Subject Key Identifier

Key Identifier:	1D 1C 65 0E A8 F2 25 7B B4 91 CF E4 B1 B1 E6 BD 55 74 6C 05
Critical:	No

Signature

Signature Algorithm:	1.2.840.113549.1.1.11
Signature Parameters:	05 00
Signature:	78 A6 0C 16 4A 9F 4C 88 3A C0 CB 0E A5 16 7D 9F B9 48 5F 18 8F 0D 62 36 F6 CD 19 6B AC AB D5 F6 91 7D 92 E1 60 6D AE 7A 6B 09 AA C6 29 EE 68 49 67 30 80 24 7A 31 16 39 5B 7E F1 1C 2E DD 6C 09 AD F2 31 C1 81 EC BE 6D 26 E6 1C E4 42 20 9E 47 B0 AC 83 59 70 2C 35 D6 AF 36 34 B4 CD 3B F8 32 A8 EF E3 78 89 FB A7 85 E1 B9 7B 3C DE BE 1E 79 84 CE 9F 70 0E 59 C2 35 2E 90 2A 31 D9 E4 45 7A 41 A4 2E 13 9B 34 0E 66 23 A7 1F 48 DD 35 46 98 B2 10 68 E4 A5 31 C2 0A 58 2E 19 81 10 C9 50 75 FC EA 5A 16 CE 11 D7 EE EF 50 80 3E 9D A3 3C 4C 72 C2 57 C4 A0 D4 CC 38 27 CE D5 06 9E A2 48 D9 E9 9F CE 82 70 36 93 9A 3B DF 96 21 88 C7

Certificado raíz

Subject Name == Issuer Name

Esta firmado por sí mismo: es el origen de la confianza (Nos fiamos de la entidad directamente, no hay una clave privada externa que firme su clave pública)

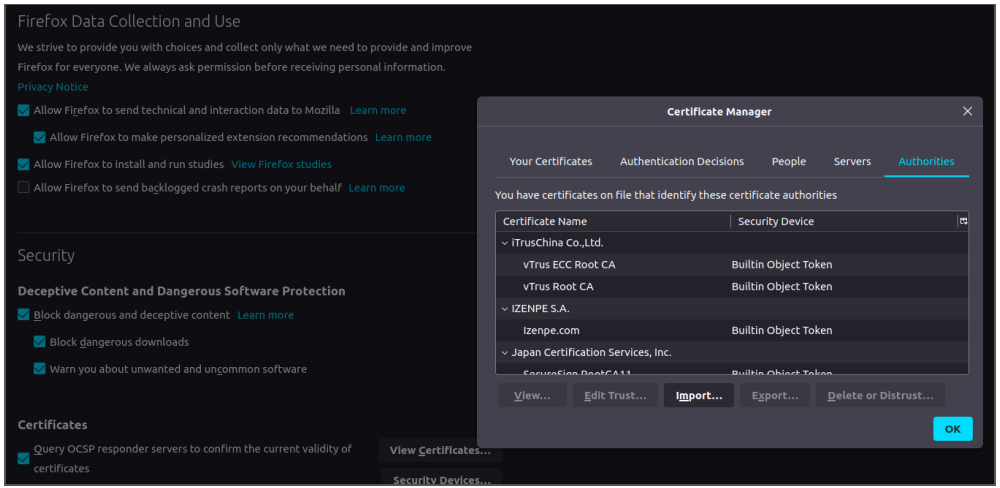
Tipos de certificados

- Certificado de usuario final (persona jurídica)
- Certificado de firma de software
- Certificado de servidor SSL

Implementación

- Los sistemas operativos y navegadores incluyen certificados raíz, asumiendo confianza de facto
- Firefox OCSP query responder, Izenpe

Implementación



Let's encrypt

AC que emite certificados de forma gratuita para que todas las conexiones HTTP sean cifradas

https://letsencrypt.org/