Zifraketa

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Zifraketa

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

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

Sinaduren konfidantza

Sinadura digitalak erabilita ere:

- Nola dakigu sinadura bat esaten duenarena dela?
- Nola bermatzen du Zertifikazio Autoritate batek hori horrela dela?
- Ezin gara fidatu Zertifikazio Autoritate batek bermatu duen sinadura batetaz?

Sinaduren konfidantza

- PGP, GnuPG eta horrelakoak erabiltzen dira
- Erabiltzaile batek bermatzen du, bere gako pribatuarekin sinatuz, beste erabiltzaile baten gako publikoa fidagarria dela
- Konfidantza hedatzen doa, gakoak sinatzen dituzten erabiltzaileei ematen diegun konfidantzaren arabera

Konfidantza mailak

- Ezezaguna: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (ezezaguna delako)
- Eza: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (Badakigulako txarto egiten duela)
- Marginala: konfidantza marginala duten bi erabiltzailek sinatutako klabeengan konfidantza dugu
- Osoa: Erabiltzaile horrek sinatzen duen guztiaz fidatzen gara

Ziurtagiri digitalak

- Ziurtagiri digitala: konfidantzazko erakunde batek erabiltzaile baten gako publikoa sinatzea, bere gako pribatuarekin
- Erabiltzailea berak esaten duena dela bermatzeko balio du
- Bermea ematen duen erakundearenganako konfidantzaren arabera

Ziurtagiri digitalak

- X.509 estandarra
- Baliozkotasuna != konfidantza
  - Baliozkotasuna: sinadura baten eskakizunak betetzen ditu (iraungipena, etab.)
  - Konfidantza: sinadura horretaz fida gaitezke
- Sinadura batek baliozkotasuna eduki dezake, baina ez konfidantza
- Konfidantza duen baliogabeko sinadura batek ez dauka zentzurik

Ziurtagiri digitalak

Zertifikazio Autoritate batek sinadura baten baliozkotasuna bermatzen du

- Ziurtapen-zerbitzuen emaileak (PSC): Ley de Firma Electrónica (Ley 59/2003, LFE), Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007, LAESCP)
- PSC-ak beraien ziurtagirien indarraldia kontsultatzeko metodo bat eman behar dute: erakunde publikoen kasuan musutruk izan behar du

Ziurtagiri digitalak

Zertifikazio Hierarkia (RFC 1422)

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

CA (Zertifikazio Autoritate) batek

- Distinguised Name eta CA subordinatuak gordetzen dituen DB-a
- Ziurtagirien baliogabetzea:
  - Erabiltzailearen klabe pribatua konprometitua
  - CA ziurtagiri bat okerreko norbaiteri eman dio
  - Erabiltzaileak CA-z aldatzen du
  - CA-aren segurtasuna apurtua
- CRL, Certification Revocation List: adibidez GeoTrust

CA (Zertifikazio Autoritate) batek

- OCSP (Online Certificate Status Protocol RFC 2560) protokoloak ziurtagiri baten egoera online balioztatzea bermatzen du
- CRL-ak baino eraginkorragoa da
- Abantaila: beti eguneratua
- Desabantaila: konprobatzeko konektatu behar

Ziurtagiri digitalak

Zerbitzua ematen duen CA bakoitzak OCSP zerbitzari bat mantentzen du

Eskakizun egokia egiten duten bezeroei erantzuten die

Ziurtagiri digitalak

Gako publikoko ziurtagiri motak:

- Autoritate ziurtagiriak
- Zerbitzari ziurtagiriak
- Ziurtagiri pertsonalak
- Software ziurtagiriak

Ziurtagiri digitalak

Ziurtagiri baten osagarriak:

- Bertsioa
- Serie zenbakia
- Sinadura algoritmoaren identifikatzailea
- Iraungipena
- ...

Ziurtagiri digitalak

- Konfidentzialtasuna informazioa enkriptatuz
- Informazioaren osotasuna hash eta sinadura bidez
- Kautotzea informazioa sinatua datorrelako
- Zapuztezintasuna informazioa sinatzean