Sinadura

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Sinadura

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

https://github.com/mikel-egana-aranguren/EHU-ISSKS-31

Sinadura digitala

Mirenek Ikerreri mezua bidaltzen dio, gako publikoko sistema erabiliz

Edonork ezin du irakurri Mirenen Ikerrentzako mezua, baina edozeinek bidali ahal du

Nola daki Ikerrek Mirenek bidali diola edo inork ez duela mezua aldatu?

Soluzioa: Mirenek mezua sinatzen du

Sinadura digitala

Erabiltzaile zilegiak soilik sinatu ahal du bere dokumentua

Ezin du inork sinadura faltsutu

Edozeinek balioztatu ahal du sinadura digitala

Sinadura digitala

Ezin da sinadura bat berrerabili

Ezin da sinadura bat aldatu

Ezin da dokumentu bat sinatu izana ukatu

Ezin da dokumentu bat aldatu sinatu ostean

Kautotzea, **Osotasuna** eta **Zapuztezintasuna**

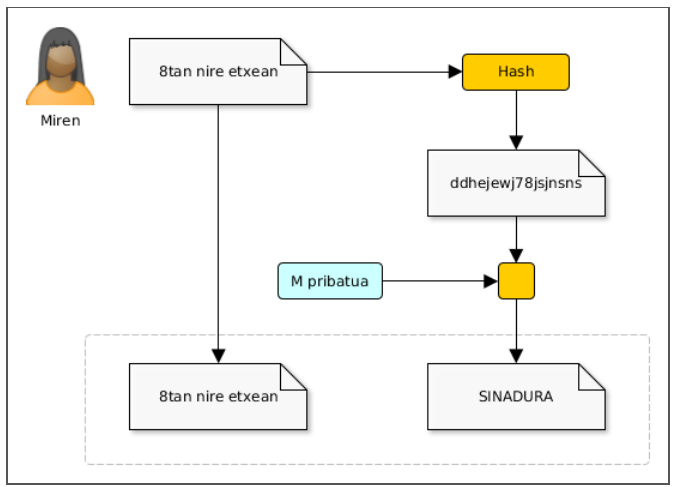
Sinadura digitala

Mirenek mezuaren laburpen kriptografikoa lortzen du: RC = hash (m)

Mirenek bere klabearekin zifratzen du laburpen kriptografikoa: Sinadura = e (RC, M_{pri})

Mirenek bere mezua (Zifratua edo zifratu gabe) eta bere sinadura bidaltzen ditu

Sinadura digitala



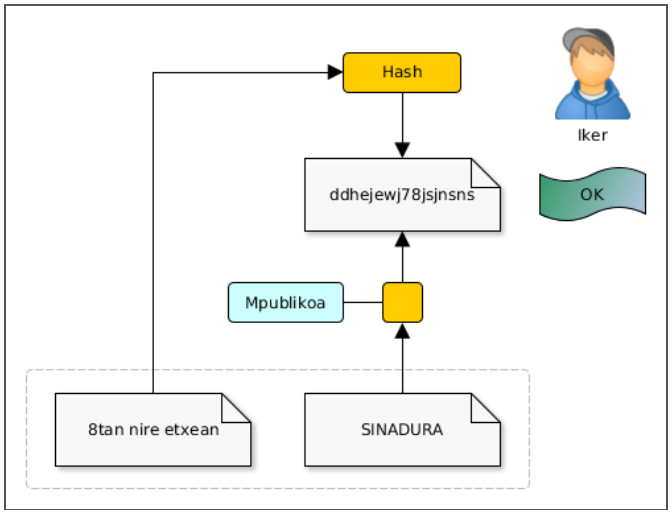
Sinadura digitala

Ikerrek sinadura deszifratzen du Mirenen gako publikoa erabiliz: RC = (Sinadura, M_{pu})

Ikerrek mezuaren laburpen kriptografikoa lortzen du: RC’ = hash (m)

Ikerrek RC’ eta RC alderatzen ditu ezer aldatu ez dela baieztatzeko

Sinadura digitala



Sinadura digitala

Sinatzeaz gain, Mirenek mezua zifratzen badu, Ikerrek bakarrik irakurriko du:

Konfidentzialtasuna, **Osotasuna**, **Kautotzea**, **Zapuztezintasuna**

Hurrengoak erabiltzea dauka:

- Kriptografia asimetrikoa
- Kriptografia hibridoa

Sinadura digitala

Kriptografia asimetrikoa. Ikerreri bidali:

- Mezu zifratuaren kriptograma (M_{pri} eta I_{pu}-rekin zifratua)
- Bere sinadura digitala (Laburpen kriptografikoa, M_{pri}-rekin zifratua)

Sinadura digitala

Kriptografia hibridoa. Ikerreri bidali:

- Saio gakoarekin zifratutako mezuaren kriptograma
- Saio gako zifratuaren kriptograma, I_{pu}-rekin zifratua
- Bere Sinadura digitala (Laburpen kriptografikoa, M_{pri}-rekin zifratua)

Sinaduren konfidantza

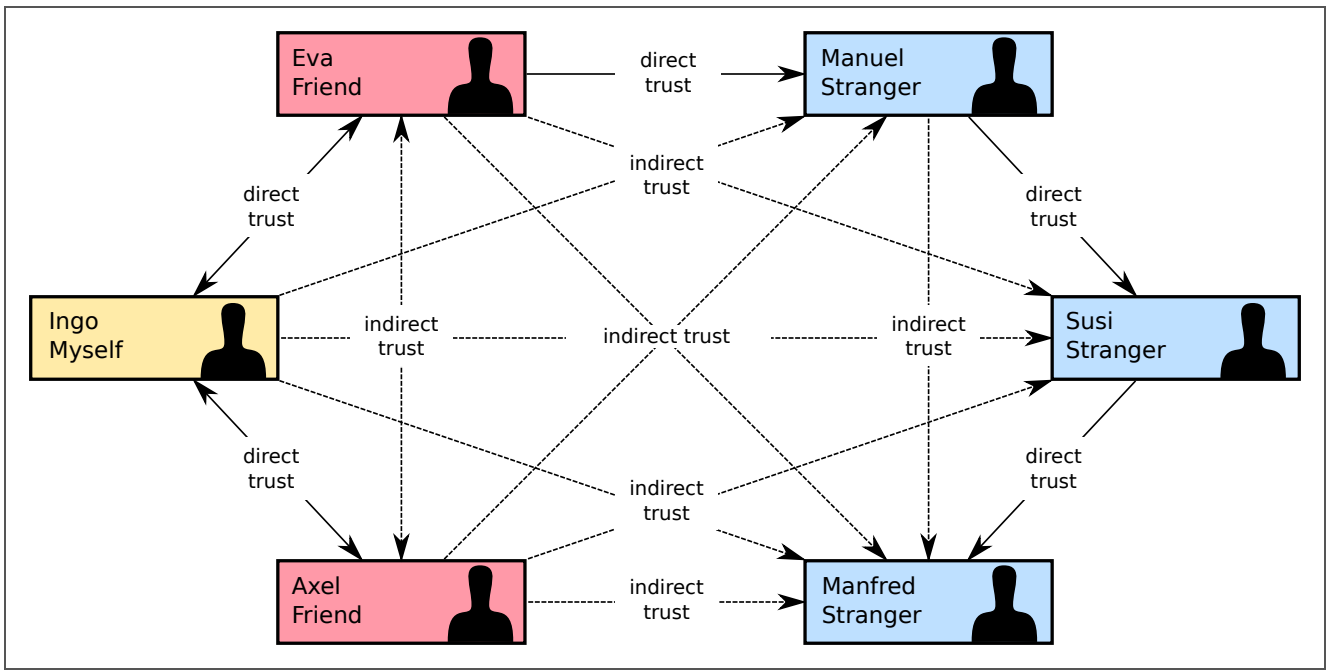
Sinadura digitalak erabilita ere:

- 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 (Web of trust)

- 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

Web of trust



https://commons.wikimedia.org/wiki/File:Web_of_Trust-en.svg

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