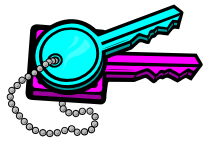
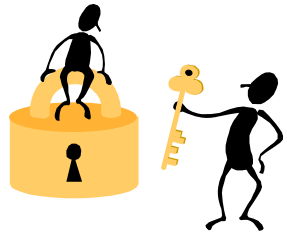
Infrastruktura javnih ključev

- Šifriranje z javnimi ključi
- Digitalno potrdilo
  - PGP
  - X-509



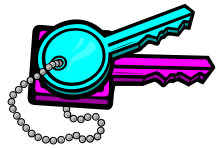


Namen digitalnega podpisa

- Digitalni podpis dodajamo nešifriranemu sporočilu in zato ne zagotavlja tajnosti komunikacije.
- Pošiljatelj z digitalnim podpisom zagotovi:
  - verodostojnost sporočila,
  - potrjuje svojo identiteto in s tem
  - sprejme tudi odgovornost za sporočilo.
- Prejemnik lahko hkrati preveri verodostojnost in avtentičnost:
  - Ali je sprejeto sporočilo res enako oddanemu sporočilu ?
  - Ali nam sporočilo res pošilja predstavljeni pošiljatelj ?
- Če prejemnik potrdi verodostojnost sporočila in avtentičnost pošiljatelja, potem tudi pošiljatelj ne more sporočila zanikati:
  - Če se prstna odtisa ujemata, potem sporočilo ni bilo spremenjeno in podpisal ga je lahko le pošiljatelj, ki ima edini pravi zasebni ključ.
- Digitalni podpis omogoča zagotavljanje verodostojnosti, avtentičnosti in neovrgljivosti sporočil.

Uporaba zasebnih in javnih ključev

- Digitalni podpis temelji na asimetričnem šifrirnem postopku, ki uporablja parov imetnikovih ključev: javni ključ + zasebni ključ

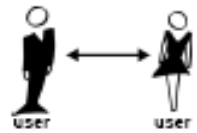


- Vsak uporabnik nosi odgovornost za uporabo in varovanje zasebnega ključa. Dostop do tajnega ključa varujemo z dolgim geslom, ki ga imenujemo fraza. Uporabnik ne sme zaupati nikomur svojega zasebnega ključa. Če to stori, potem nosi tudi vso odgovornost za zlorabe.

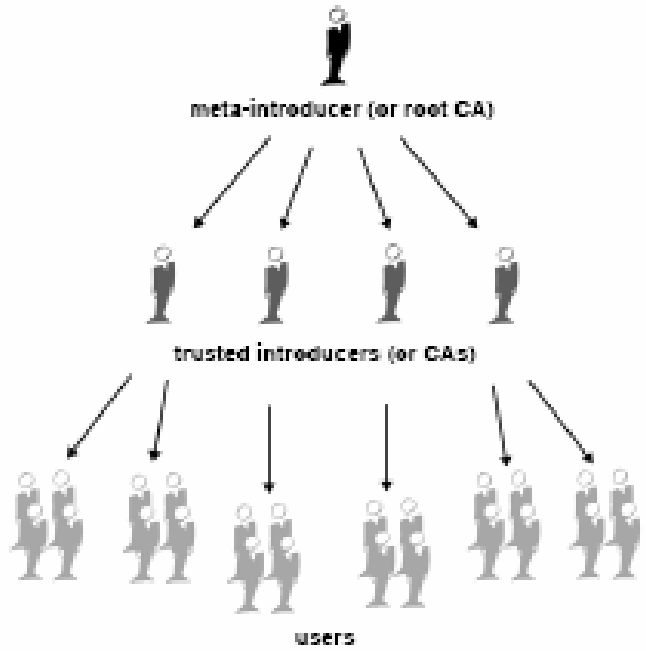
- Javni ključ mora biti vsakomur dostopen z jamstvom, da pripada navedenemu uporabniku. V nasprotnem primeru lahko pride do problemov:
  - Problem lažne identitete: napadalec podtakne lažni javni ključ in dešifrira vsa prestrežena sporočila.
  - Problem zanikanja identitete: pošiljatelj zanika lastno sporočilo.

Model zaupanja

- Neposredno zaupanje:
  - uporabniki si paroma izmenjajo certifikate

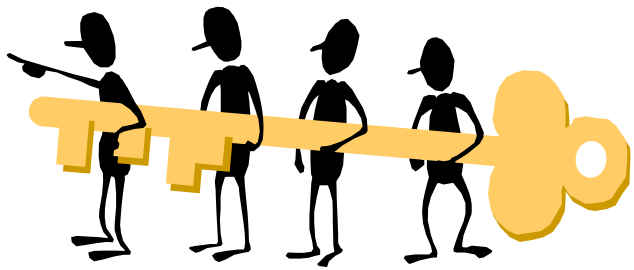


- Hierarhični model ima obrnjeno drevesno strukturo:
  - vrhovni overitelj - root CA upravlja digitalna potrdila overiteljev, ki ležijo en nivo nižje v strukturi
  - najnižji CA upravljajo s potrdili uporabnikov



Upravljanje s ključi

- Javni ključ mora nositi garancijo, da res pripada navedenemu uporabniku. Overjanje javnih ključov opravlja posebna služba (podobno notarju), ki skrbi tudi za upravljanje s ključi.
- Urad za overjanje (**CA**=Certification Authority) potrjuje verodostojnost javnih ključev z digitalnim podpisom odgovorne osebe. Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba (RA=Registration Authority).
- Na zahteve imetnikov opravlja CA tudi razveljavitve javnih ključev. Potreba po preklicu javnega ključa nastopi v primeru izgube tajnosti zasebnega ključa.

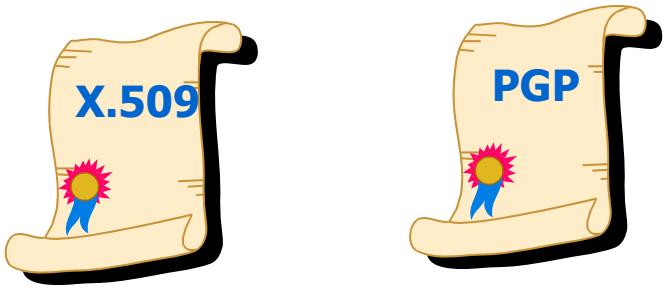


Digitalno potrdilo

- Digitalno potrdilo (digital certificate) je kopija javnega ključa, ki je overjena od tretje osebe ali institucije.
- Imetnik javnega ključa se mora ob registraciji identificirati in s tem prevzema tudi odgovornost za uporabo zasebnega ključa. Identifikacijo izvrši uradna oseba RA (Registration Authority).
- Urad za overjanje potrdil CA (Certification Authority) je nevtralna organizacija, ki ji uporabniki zaupajo.
- Upravljanje z javnimi ključi ne zajema samo shranjevanje digitalnih potrdil na strežniku, pač pa celoten postopek posrednih overjanj izdajateljev potrdil, razveljavitve javnih ključev itn.
- Infrastruktura javnih ključev PKI (Public Key Infrastructure) določa protokole in storitve pri upravljanju z javnimi ključi.

Format digitalnega potrdila

- Digitalno potrdilo vsebuje poleg javnega ključa tudi množico identifikacijskih podatkov uporabnika in izdajatelja potrdila.
- Najbolj znana formata sta X-509 in PGP:
  - ITU-T mednarodni standard predpisuje X-509 format digitalnih potrdil. V opisu je določeno katere informacije so vsebovane v poljih potrdila in kakšen je njihov format zapisa.
    - X-509 v1 1988, osem polj
    - X-509 v2 1993, + dodani dve identifikacijski polji = 10 polj
    - X-509 v3 1996, + dodano polje za razširitve
  - PGP format digitalnega potrdila se uporablja v programskem paketu za varno izmenjavo podatkov PGP (Pretty Good Privacy). PGP je v začetku devetdesetih let ustvaril Phil Zimmerman.



X.509 - demo

- Version: 3 (0x2)
- Serial Number: 0 (0x0)
- Signature Algorithm: sha1WithRSAEncryption
- Issuer: OU=Demo SI-CA, O=SETCCE, C=SI
- Validity
  - Not Before: Dec 20 11:49:01 2004 GMT
  - Not After : Dec 18 11:49:01 2014 GMT
- Subject: OU=Demo SI-CA, O=SETCCE, C=SI
- Subject Public Key Info:
  - Public Key Algorithm: rsaEncryption
  - RSA Public Key: (4096 bit)
    - **modulus (4096 bit): JAVNI KLJUČ**
  - X509v3 extensions:
    - X509v3 Basic Constraints: critical
    - CA:TRUE
    - X509v3 Subject Key Identifier: B6:16:5E:27:5B:B2:2E:E4:CF:3A:83:71:7C:AF:4E:B8:EB:F6:22:3E X509v3
    - Key Usage: critical Certificate Sign, CRL Sign
- Signature Algorithm: sha1WithRSAEncryption

Pridobitev digitalnega potrdila

- Glavni overitelj digitalnih potrdil za pravne in fizične osebe je SIGEN-CA (Slovenian General Certification Authority)
- Spletno kvalificirano digitalno potrdilo pridobimo nekaj dni po oddaji izpolnjenega formularja na Upravni enoti ob identifikaciji z osebnim dokumentom.
- Digitalno potrdilo lahko med drugim uporabimo tudi za različne storitve na portalu e-uprava
  - oddaja vlog za upravne storitve,
  - oddaja obrazcev za dohodnine,
  - vpogled v osebne podatke centralnega registra prebivalstva ..