

Varne komunikacije

Digitalni podpis in digitalno potrdilo:

- Elektronski prstni odtis dokumenta



- Digitalni podpis



- Upravljanje s ključi



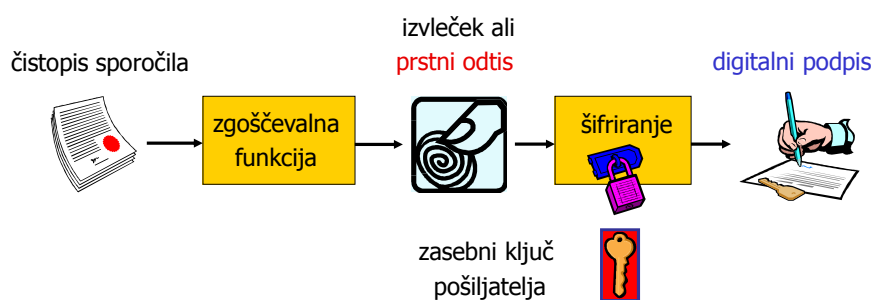
- Digitalno potrdilo



1

Digitalni podpis

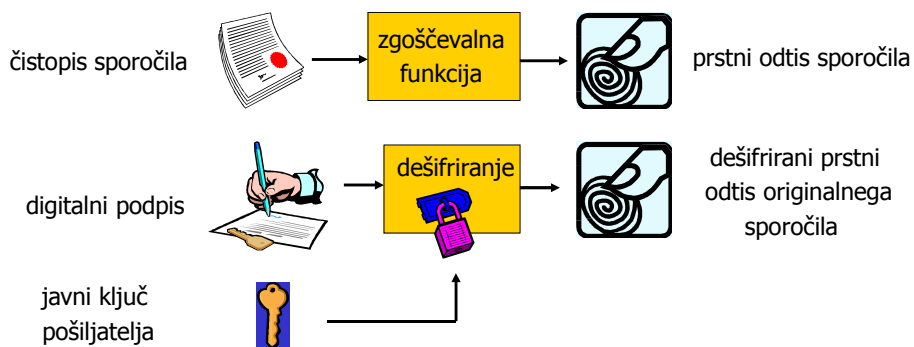
- Digitalni podpis je s tajnim ključem šifrirani **prstni odtis** sporočila:



- Zgoščevalna funkcija je enosmerna funkcija in vsaka sprememba čistopisa spremeni tudi prstni odtis sporočila.
- Napadalec bi lahko spremenil sporočilo in dodal nov prstni odtis !
- Pošiljatelj zaščiti prstni odtis s šifriranjem!

2

Preverjanje digitalnega podpisa



- Prejemnik preveri ujemanje prstnih odtisov in če sta enaka
 - je **sporočilo verodostojno**,
 - potrjena je **identiteta pošiljatelja** in
 - **pošiljatelj ne more zanikati** sporočila.

3

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.

4

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.

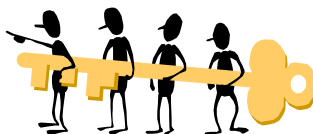


- **Javni ključ** mora biti vsakomur dostopen z jamstvom, da pripada navedenemu uporabniku. V nasprotnem primeru lahko pride do problemov:
 - Problem lažne identitete: napadalec podtakne lažni javni ključ in dešifrira vsa prestežena sporočila.
 - Problem zanikanja identitete: pošiljatelj zanika lastno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

5

Upravljanje s ključi

- Javni ključ mora nositi garancijo, da res pripada navedenemu uporabniku. **Overjanje javnih ključev** 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.



6

Digitalno potrdilo

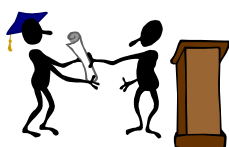
- Digitalno potrdilo (digital certificate) je overjena kopija javnega ključa.
- Digitalno potrdilo vsebuje:
 - kopijo javnega ključa
 - identifikacijske podatke imetnika
 - digitalni podpis [Urada za overjanje \(CA\)](#)
 - datum začetka veljavnosti potrdila
 - datum poteka veljavnosti potrdila
 - serijsko številko
 - ...
- Veljavnost digitalnega potrdila je odvisna od zaupanja uporabnikov v [CA](#).
- Neznani CA ne smemo zaupati !!



7

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 ..



8