DIGITALNI PODPIS – uporaba v upravnih sistemih

mag. Iztok Sirnik

IZRAZOSLOVJE

- Kriptiranje,
- šifriranje,
- kodiranje.

Elektronsko poslovanje – 1/2

- E-business,
- elektronsko poslovanje organizacij,
- podatkovna infrastruktura,
- komunikacije,
- omrežja,
- podatkovna skladišča.

Elektronsko poslovanje – 2/2

- Skladišča znanja,
- programska podpora,
- spletna podpora,
- domače strani,
- skupinsko delo,
- prenova procesov.

Elektronsko trgovanje – 1/2

- E-commerce,
- povezovanje pravnih subjektov,
- pravna razmerja,
- ponudbe,
- prodaja, pogodbeni odnosi,
- elektronsko podpisovanje.

Elektronsko trgovanje – 2/2

- Špedicija in druge storitve,
- transportni dokumenti,
- elektronsko plačevanje, elektronski denar,
- varnostni ukrepi,
- marketing,
- promocija.

PODPIS - elektronski

Oznake, narejene z elektronskimi mediji,

z namenom

označiti dokument ali datoteko.

PODPIS - digitalni

Je elektronski podpis,
realiziran na osnovi
šifriranja (kriptiranja).

ELEKTRONSKI PODPIS – pravna veljavnost

- ZEPEP

  varen elektronski podpis, ki je overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki

  enakovreden

  lastnoročnemu podpisu.

  zato

  ima enako veljavnost in dokazno vrednost.

VAREN ELEKTRONSKI PODPIS

- Povezan izključno s podpisnikom,
- zanesljiva identifikacija podpisnika,
- ustvarjen s sredstvi za varno elektronsko,
- podpisovanje,
- izključen nadzor podpisnika,
- ugotavlja kasnejšo spremembo podatkov.

DIGITALNI PODPIS - namen

- Avtentičnost podpisnika,
- podpisa se ne da ponarediti ,
- podpisa se ne da kopirati,
- podpisanega dokumenta se ne da spremeniti,
- podpisa se ne da zanikati.

DIGITALNI PODPIS - realizacija

- Simetrično šifriranje,
- asimetrično šifriranje,
- zgostitev besedila.

ZGOSTITVENI ALGORITMI – definicija povzetka

- Je enolična predstavitev datoteke (prstni odtis),
- preslika poljubno dolg niz znakov v blok konstantne dolžine.

ZGOSTITVENI ALGORITMI - lastnosti

- Nemogoče je najti dve različni sporočili, ki bi ju preslikal v isti povzetek,
- isto sporočilo se vedno preslika v enak povzetek,
- iz povzetka ni mogoče restavrirati sporočila,
- vsaka sprememba v sporočilu povzroči nov povzetek.

DIGITALNI PODPIS - pošiljatelj

- Zgosti dokument,
- šifrira dokument in povzetek,
- podpiše dokument,
- pošlje.

DIGITALNI PODPIS - prejemnik

- Preveri avtentičnost prejetega dokumenta,
- dešifrira dokument in povzetek,
- naredi svoj povzetek (zgosti dokument),
- primerja povzetke.

OVEROVITELJ JAVNIH KLJUČEV – opredelitev

- Certification Authority - neodvisna in zaupanja vredna organizacija,
- Javni ključ, zasebni ključ,
- način delovanja
- nivoji zaupanja,
- enolična identifikacija uporabnika,
- digitalna potrdila,
- javni dostop do CA potrdil.

OVEROVITELJ JAVNIH KLJUČEV - značilnosti

- Generiranje in hranjenje ključev,
- overjanje lastnikov ključev,
- izdajanje digitalnih potrdil za javne ključe,
- objavljanje digitalnih potrdil (imeniki),
- upravljanje z digitalnimi potrdili,
- časovna označitev postopkov (time stamp).

DIGITALNO POTRDILO JAVNIH KLJUČEV

Je digitalni dokument,

ki potrjuje

povezavo med

javnim ključem in

osebo / institucijo / strežnikom

DIGITALNO POTRDILO - vsebina

- Serijska številka,
- algoritmi in parametri,
- izdajatelj,
- datum veljavnosti,
- identifikacija uporabnika,
- e-naslov uporabnika,
- javni ključ uporabnika,
- digitalni podpis za zgornje podatke.

DIGITALNO POTRDILO V JAVNI UPRAVI

- Upravljanje s podatki javne uprave,
- dostop in izmenjava podatkov,
- varno elektronsko komuniciranje,
- uporaba storitev.

PRAVNE IN FIZIČNE OSEBE - SIGEN – CA

- osebna digitalna potrdila
- spletna digitalna potrdila

SLUŽBENA POTRDILA - SIGOV – CA

- Zaposleni v javni upravi,
- druge osebe,

- službena osebna digitalna potrdila,
- službena spletna digitalna potrdila.

OSEBNA DIGITALNA POTRDILA - namen

- Šifriranje in dešifriranje e-podatkov,
- digitalno podpisovanje e-podatkov,
- overjanje identitete podpisnika,
- varno brisanje e-podatkov,
- opravljanje storitev.

SPLETNA DIGITALNA POTRDILA - namen

- Varno spletno komuniciranje,
- šifrirano pošiljanje e-pošte,
- opravljanje spletnih storitev.

UPORABNIKI

- Zaposleni,
- strežniki,
- pravne in fizične osebe.