ŠOLSKI CENTER KRANJ
ZA POKLICE PRIHODNOSTI

DIGITALNI PODPISI IN DIGITALNI CERTIFIKATI

Seminarska naloga pri računalništvu

Kranj, september 2014

POVZETEK

Digitalno potrdilo predstavlja enolično povezavo med imetnikom potrdila in javnim ključem, vsebuje vse osnovne podatke o imetniku in javnem ključu. Če ne gre za zaprt sistem uporabnikov, so digitalna potrdila javno objavljena, kar omogoča ugotovitev ter preverjanje identitete podpisnika na osnovi njegovega javnega ključa. Osnovna fukncija digitalnega podpisa je v dokazovanju identitete podpisnika elektronskega dokumenta in zagotavljanju celovitosti podatkov oziroma zaščite pred spreminjanjem vsebine e-dokumentov. Temeljijo na asimetrični kriptografiji, zato par ključev – zasebnega za podpisovanje in javnega za preverjanje veljavnosti podpisov. Digitalno podpisovanje je pravzaprav izdelava prstnega odtisa podatkov, ki je vedno unikaten – vsakemu dokumentu pripada samo en prstni odtis. Ko se dokument digitalno podpiše, se vhodni podatki pretvorijo z hash (zgoščevalno) funkcijo, katere rezultat je prstni odtis dokumenta. Ko le tega enkripiramo z zasebnim ključem, dobimo digitalni podpis dokumenta.

KLJUČNE BESEDE

- digitalni podpisi,
- digitalna potrdila,
- javni ključ,
- zasebni ključ,
- kriptografija.

Slika 1: podpisovanje

ABSTRACT

A digital certificate represents a unique link between the holder of the certificate and public key, it contains all the basic information about the holder and the public key. If it is not a closed system, the digital certificates are publicly available, which allows finding and verifying the identity of the signer based on his public key. Basic function of the digital signature in proving the identity of the signer of an electronic document and ensuring data integrity and protection against changing the content of the e-documents. Based on asymmetric cryptography, we need the key pair - private for the signature and the public to check the validity of signatures. Digital signature is actually like fingerprint data, which is always unique - each document belongs to only one fingerprint. When a document is digitally signed by the input data is converted to hash function, the result of which is the fingerprint of the document. When only this is encripted with a private key, we obtain a digital signature of the document.

KEYWORDS

- digital signature,
- digital certificate,
- public key,
- private key,
- cryptography.

KAZALO

1.DIGITALNI PODPIS

1.1.UVOD

Digitalni podpis redstavlja sodobno alternativo klasičnemu podpisu in zagotavlja identiteto, integriteto sporočila, kar pomeni da niti dela podatkov ni mogoče spremeniti oz. popraviti brez vednosti lastnika podpisa. Je niz šifriranih znakov, dodan ali logično povezan z drugimi podatki, ki omogoča preverjanje istovetnosti podatkov in podpisnika. Pravno gledano ima digitalni podpis enako težo kot lastnoročni podpis.

Slika 2: naprava za elektronsko podpisovanje

Izpolnjevati mora naslednje zahteve:

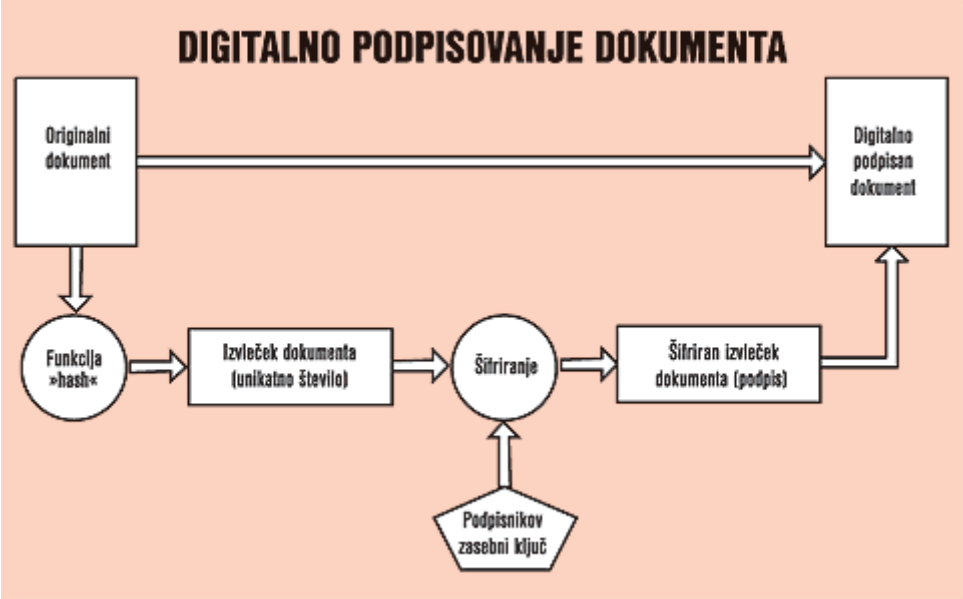
- da je povezan izključno s podpisnikom,
- iz njega ni mogoče zanesljivo ugotoviti podpisnika,
- ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom,
- povezan je s podatki, na katere se nanaša, tako da je opazna vsaka sprememba teh podatkov ali povezave z njimi

Običajno se uporabljajo za distribucijo programske opreme, finančne transakcije, in v primerih, ko so potrebni za odkrivanje ponarejanja ali nedovoljenih posegov.

1.2.KAKO DELUJE

Elektronski podpis, ki temelji na asimetrični (javni) kriptografiji je praktično edina tehnična rešitev, ki jo lahko danes uporabimo za varne elektronske podpise. Elektronski podpis zagotavlja pristnost podatkov in jih varuje pred spremembami s kriptografskimi metodami. (Kriptografija je matematična veda, ki se ukvarja z zakrivanjem podatkov s pomočjo matematičnih operacij).

Naprimer: ko se podpišemo z m, podpisnik vstavi $\sigma \equiv m^d \pmod N$, prejemnik pa preveri da drži: $\sigma^e \equiv m \pmod N$. Ta osnovna operacija pa ni najbolj varna, zato jo kodiramo z hash (zgoščevalno) funkcijo - to je algoritem, ki dobi kot vhod poljubno dolgo sporočilo, kot izhod pa vrne fiksno dolgo binarno vrednost (hash value). Uporabljamo jo za preoblikovanje poljubno dolgih vhodnih sporočil v izhodne vrednosti dolžine 128 bitov. Pomembnost te funkcije je, da je nepovratna ali enosmerna, to pomeni, da je nemogoče najti vhodno sporočilo, če poznamo izhodno vrednost. Prav tako je nemogoče najti dve vhodni sporočili, ki bi ob izhodu tvorili enaka rezultata. Najpogostejši algoritmi so MD4 (zgodnješa fukncija MD5), MD5 (Message-Digest algorithm 5) je znan kot pogosto uporabljana kodirna funkcija s 128-bitnim izhodom, ki se pogosto uporablja za preverjanje datotek., SHA-1, itd.



Slika 3: prikaz digitalnega podpisovanja dokumenta

1.3.TIPI KLJUČEV

Javna kriptografija uporablja naslednje ključe:

- **zasebni (tajni) ključ** je skrivni podatek, ki ga poseduje samo njegov imetnik. Je majhen košček kode, ki je združen z javnim ključem do ujemanja algoritmov za šifriranje besedila in dekripcijo. Prejemnik uporablja svoj zasebni ključ za dešifriranje sporočil.

- **javni ključ** je dostopen vsem, potrebno ga je povezati z njegovim imetnikom in ga javno objaviti. Javna kriptografija v ta namen uporablja infrastrukturo javnih ključev (PKI), ki s pomočjo digitalnih potrdil, ki jih izdajajo pooblaščene agencije poskrbi za razpečavo javnih ključev in vzpostavitev zaupanja v njih ter povezavo javnih ključev z ljudmi, strežniki, informacijskimi sistemi itd.

2.DIGITALNO POTRDILO

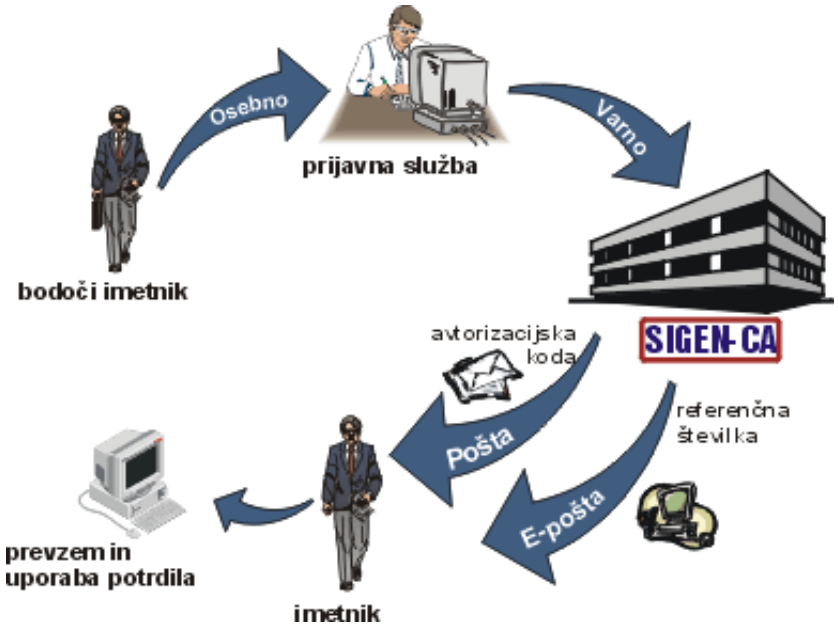
2.1.UVOD

Je elektronski "potni list", ki omogoča osebi, računalniku ali organizaciji izmenjavo informacij na varnen način prek interneta z uporabo infrastrukture javnih ključev. Digitalno potrdilo je sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica, ...), s specifičnim namenom - zagotavljanju varnega in legitimnega e-poslovanja.

Je računalniški zapis, ki vsebuje podatke o imetniku (ime, e-naslov, enolična številka,...) in njegov javni ključ, poleg tega pa še podatke o overitelju oz. izdajatelju digitalnega potrdila ter obdobje veljavnosti digitalnega potrdila. Zapis je digitalno podpisan z zasebnim ključem izdajatelja potrdila, da se ga ne da ponarediti.

V Sloveniji deluje več izdajateljev digitalnih potrdil (CA):

- http://www.sigen-ca.si/
- http://postarca.posta.si/
- http://www.halcom-ca.si/index.php?section=1
- http://www.nlb.si/cgi-bin/nlbweb.exe?doc=5458



Slika 4: shema pridobitve potrdila

2.2.KAKO DELUJE

Tako kot potni list, digitalni certifikat zagotavlja identifikacijo, in je mogoče preveriti, kje je bil izdan, kar prepreči ponaredke. Vsebuje ime imetnika potrdila, serijsko številko, rok veljavnosti, kopijo javnega ključa imetnika certifikata (ki se uporablja za šifriranje sporočil in digitalnih podpisov) in digitalni podpis overitelja, ki izdaja, tako da prejemnik lahko preveri, da je certifikat pravi. Za dokaz, da je potrdilo resnično, je digitalno podpisano s strani organa. OSin brskalniki držijo liste pooblaščenih agencij za izdajanje digitalnih potrdil, tako da jih je mogoče zlahka preveriti.

2.3.VRSTE POTRDIL

Kvalificirana digitalna potrdila (namenjena so posameznikom, pravnim osebam in fizičnim osebam, registriranim za opravljanje dejavnosti:

- **Standardno kvalificirana** potrdila (potrdila, ki vsebujejo en par RSA[1] ključev, ki se uporabljajo za podpisovanje, de(šifriranje) podatkov, vzpostavljanje varnih omrežnih povezav in prijavo v spletne aplikacije ali informacijske sisteme. Ta potrdila s pripadajočim zasebnim ključem je shranjeno na disku v osebnem računalniku imetnika ali na kakem drugem mediju).
- **Napredno kvalificirana** potrdila (potrdila, ki vsebujejo dva para RSA[2] ključev, en par se uporablja za šifriranje in dešifriranje podatkov, vzpostavljanje varnih omrežnih povezav ter za prijavo v spletne aplikacije in informacijske sisteme, drugi par pa je zaradi varnosti namenjen izključno podpisovanju elektronskih dokumentov, s čimer se poskrbi za »nezatajljivost« digitalnega podpisa. Ta potrdila so skupaj z obema paroma RSA ključev shranjena na pametni kartici, ki je trenutno najvarnejša tehnologija zaradi mikroprocesorja na kartici, ki samodejno zaklene kartico v primeru, ko je večkrat vpisano napačno geslo (PIN kode) in zaradi generiranja tajnih ključev in podpisovanja, kar se vrši v mikroprocesorju na samem čipu pametne kartice, zato tajni ključ ni nikoli in nikjer dostopen izven čipa.

In **normalizirana** digitalna potrdila, ki so namenjena ostalim uporabnikom.

3.PODROBNO

3.1.KRIPTOGRAFIJA

Kriptografija je znanstvena veda o tajnem, nerazumljivem pisanju sporočil in njihovemu prebiranju s pomočjo dekodiranja (s katerim pridemo od nerazumljivih znakom do rešitve, ki jo razumemo). V svetu tehnologije se uporablja tudi plačevanje z digitalnim denarjem in na številnih drugih področjih interneta.

- SIMETRIČNA (sprva se je uporabljala samo ta. Pri njej uporabljamo isti ključ za šifriranje in dešifriranje, pri tem pa nastane težava upravljanja s ključi in

---

[1] *vsebuje dva ključa: javnega in zasebnega (ključ je konstantno število, ki ga kasneje uporabljamo v formuli za šifriranje). Javni ključ poznajo vsi in se uporablja za šifriranje sporočil. Sporočila lahko dešifriramo samo z zasebnim ključem. Z drugimi besedami: vsi lahko sporočilo zašifrirajo, prebere pa ga lahko samo lastnik zasebnega ključa. Praktičen primer: oseba A pošlje osebi B škatlo z odprto ključavnico, za katero ima ključ samo oseba A. Oseba B prejme škatlo in vanjo položi sporočilo, napisano v preprostem jeziku. Škatlo zaklene s ključavnico osebe A in ji jo pošlje. Oseba B pošlje škatlo osebi A, kjer jo ta odpre s svojim ključem. V tem primeru je škatla s ključavnico javni ključ osebe A in ključ za to ključavnico je njen zasebni ključ.*

[2] *(glej [1])*

sicer, kako vsakemu uporabniku, ki hoče prebrati naše sporočilo, ta ključ varno dostaviti. Zaradi tega se je razvila asimetrična, ki rešuje to težavo.

- ASIMETRIČNA (temelji na uporabi dveh ključev (javnega in zasebnega), ki ju imenujemo par asimetričnih ključev, saj sta komplementarna. Slabost te kriptografije je, da je počasnejša od simetrične, zato se v praksi uporablja hibridni pristop. Pri elektronski pošti je celotno sporočilo zašifrirano s pomočjo naključnega simetričnega ključa, ki je nato sam zašifriran z javnim ključem prejemnika. Ta kriptografija nam zagotavlja celovitost, zaupnost in preverjanje identitete pošiljatelja, saj sporočilo lahko dekodira le prejemnik na podlagi svojega javnega ključa).

3.2.OVERITELJI (CA)

Igrajo osrednjo vlogo glede javnih ključev. Predstavljajo ustanovo, ki ji zaupajo vsi uporabniki digitalnih potrdil in digitalnih podpisov. Overitelj prejme zahtevo za izdajo digitalnega potrdila, izvede ustrezno identifikacijo bodočih imetnikov, izda digitalno potrdilo in skrbi za register izdanih potrdil, saj so informacije o izdanih potrdilih javnega značaja (razen v zaprtih sistemih). Overitelj prav tako skrbi za preklic potrdil in to tudi objavi v registru preklicanih potrdil, ki je prav tako javen. Kvalificirana potrdila imajo za sabo ugotovitev identitete in drugih pomembnih lastnosti osebe, ki naroča izdajo potrdila. V imenu overitelja lahko to naredi tudi prijavna služba, ki je pooblaščena, svoje ugotovitve pa pošlje overitelju.

4.ZAKLJUČEK

V tej seminarski nalogi smo spoznali, kaj sta digitalno potrdilo in digitalni podpis in njuno delovanje. Preverili smo, na kakšen način nastajajo tovrstni »dokumenti« in kdo jih izdaja, potrjuje, ter kdo jih lahko ima, in kaj za njihovo nemoteno delovanje in uporabo potrebuje. Razvoj le teh bo verjetno še močnejši, saj so odličen način za varno dostopanje do zaupnih podatkov.

LITERATURA IN VIRI

http://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art012 (22.9.2014)
http://en.wikipedia.org/wiki/Cryptographic_hash_function (15.9.2014)

http://en.wikipedia.org/wiki/One-way_functionhttp://en.wikipedia.org/wiki/One-way_function (15.9.2014)

http://postarca.posta.si/predstavitev-storitve/1481/Opis-digitalnih-potrdil (15.9.2014)

http://searchsecurity.techtarget.com/definition/digital-certificate (15.9.2014)

http://upload.wikimedia.org/wikipedia/commons/thumb/2/2b/Digital_Signature_diagram.svg/800px-Digital_Signature_diagram.svg.png (15.9.2014)
http://www.webopedia.com/TERM/D/digital_certificate.html (15.9.2014)

KAZALO SLIK

KAZALO KRATIC

OS: operacijski sistem
PIN: ang. personal identification number
PKI: public key infrastructure
CA: certification authority