PKI IN VARNA EL. POŠTA

Modeli zaupanja

Modeli zaupanja

- neposredno zaupanje
- splet zaupanja
- hierarhično zaupanje
  - infrastruktura javnih ključev
  - overitelji

Težave: avtentičnost ključa

- Janez želi Micki poslati šifrirano sporočilo
- uporabi Mickin javni ključ
- Kaj se zgodi, če Marcel Janezu podtakne svoj ključ in ga Janez uporabi, kot da pripada Micki?
  - iz ključa ni možno ugotoviti lastnika

Težave: odpoklic ključa

- Marcel je ukradel Janezov zasebni ključ iz njegovega trdega diska
- Janez ugotovi, da je bil ključ kompromitiran
- Kako naj Janez obvesti uporabnike njegovega ključa, da ga ne uporablja več?
  - ta podatek ni razviden iz ključa

Težave: zanikanje dejanj

- namen elektronskega podpisa je preprečiti zanikanje dejanj
  - ne moremo zanikati, da smo v preteklosti podpisali dokument
- prvi pogoj je, da lahko samo lastnik ključa elektronsko podpiše podatke
  - zato mora ostati zasebni ključ tajen
- Kako preprečimo Marcelu, da zanika, da je zasebni ključ njegov?

Težave: zagotavljanje ustreznih pravil

- V Kriptografija d.o.o. so navdušeni nad asimetrično kriptografijo, zato naj ima vsak zaposleni svoj ključ
  - vsak naj ima samo en par ključev
  - vsi ključi naj bodo v centraliziranem imeniku
  - vsak ključ naj ima primerno dolžino
  - vsak ključ je nujno zamenjati po določenem času
  - če zaposleni zapusti podjetje, je treba ključ umakniti iz uporabe
  - Kako zagotovimo spoštovanje pravil podjetja?

Model zaupanja

- ker naštetih problemov ni možno rešiti samo z asimetrično kriptografijo, potrebujemo dodatno infrastrukturo
- pri tem so pomembna razmerja zaupanja
- Janez pošilja sporočilo Micki in Zdenku, ki ga ne pozna
- Kako lahko zaupa javnim ključem?

Neposredno zaupanje

- Micka potrdi avtentičnost ključa neposredno
  - osebno ga prinese na ključku
  - pošlje po elektronski pošti in potrdi zgoščevalno vrednost po telefonu
  - …
- pri odpoklicu ključa moramo obvestiti vse uporabnike ključa
- preprečevanje zanikanja dejanj je težavno
- zagotavljanje upoštevanja politike je težavno
- težko je vzpostaviti zaupanje z neznanim uporabnikom - Zdenko?

Splet zaupanja (Web of Trust)

1. Janez zaupa Micki z neposrednim zaupanjem in želi poslati sporočilo Zdenku
   - Micka že pozna Zdenka in neposredno zaupa njegovemu javnemu ključu
2. Micka zato podpiše ključ Zdenka in ga pošlje Janezu
   - na podoben način lahko Janez vzpostavi komunikacijo z Žanom, ki se pozna z Zdenkom

- Tako spontano vendar neurejeno nastane splet zaupanja!

Splet zaupanja: izmenjava ključev

- da se izogne napakam Micka podpiše ne samo Zdenkin javni ključ temveč tudi njegovo ime
- takšno podatkovno strukturo imenujemo tudi **digitalno potrdilo**
- vsebuje lahko tudi druge podatke:
  - čas veljavnosti
  - serijsko številko
  - …

Splet zaupanja: slabosti

- za shranjevanje ključev je smiselno vzpostaviti namenski strežnik
- odpoklic ključa je zapleten
  - obvestiti vse, ki bi lahko uporabljali ključ
  - lahko je neizvedljivo
- preprečevanje zanikanja dejanj je lažje, vendar iz pravnega stališča ni zadovoljivo
- zagotavljanje spoštovanja pravil organizacije je zahtevno

Hierarhično zaupanje

- splet zaupanja lahko izboljšamo, če določimo overitelja - Certificate Authority (CA)
  - neodvisen izdajatelj digitalnih potrdil
- varen način izdajanja digitalnih potrdil zahteva posebno infrastrukturo

Hierarhično zaupanje: prednosti

- odpoklic digitalnega potrdila je enostaven
- boljša izhodišča pri preprečevanju zanikanja dejanj
- centralizirano zagotavljanje skladnosti z lokalno politiko

- zato je to bolj zapleten in hkrati bolj učinkovit model zaupanja

Komponente PKI

Kaj je PKI?

- Public Key Infrastructure (PKI) označuje združenje ljudi, opreme, dogovorov in postopkov za ustvarjanje, upravljanje, hranjenje in podeljevanje digitalnih certifikatov
- povezovanje javnega in privatnega ključa z uporabnikom
- pridobitev digitalnega podpisa

Komponente PKI

- centralne komponente PKI s skupno besedo imenujemo center zaupanja
- velikokrat se za center zaupanja uporablja kar izraz CA - overitelj, čeprav je to ožji pojem
- Komponente:
  - Overitelj (Certification Authority – CA)
  - Registrator (Registration Authority – RA)
  - Strežnik digitalnih potrdil (Validation Authority – VA)
  - Digitalno potrdilo (certificate) – standard X.509

Overitelj (CA)

- Certification Authority (CA)
- overitelj je temeljna komponenta centra zaupanja:
  - izdeluje digitalna potrdila
  - varnostno kritična komponenta
  - najbolj pomembno je varovanje zasebnega ključa overitelja
  - računalnik, na katerem se izvaja CA običajno ni priključen v omrežje

Registrator (RA)

- Registration Authority (RA):
  - je administrativni center, kjer lahko uporabniki vložijo zahtevke za izdajo digitalnega potrdila
  - RA posreduje zahtevke CA, da lahko izdela digitalna potrdila
  - teoretično bi lahko zahtevke sprejemal neposredno CA, kar se iz varnostnih razlogov ne uporablja

Strežnik digitalnih potrdil

- imenovan tudi validation authority (VA)
- VA:
  - vsebuje vsa digitalna potrdila, ki jih izdela CA
  - sodeluje pri odpoklicu potrdil
  - lahko je del centra zaupanja ali deluje ločeno

Digitalno potrdilo (certificate)

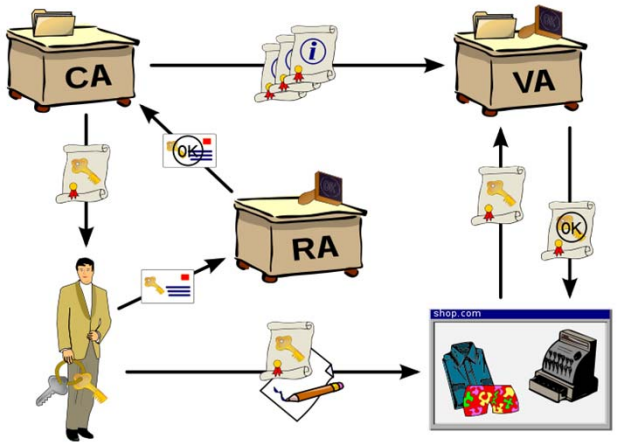
- Standard X.509
  - specificira format certifikata z javnim ključem
  - obvezna uporaba CA
  - Certificate Revocation List (CRL)
- Povezava ključa z lastnikom

Struktura digitalnega potrdila (X.509)

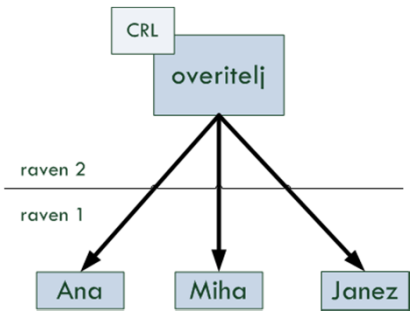
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=ZA, ST=Western Cape,
L=Cape Town,
O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Validity
Not Before: Aug 1 00:00:00 1996 GMT
Not After : Dec 31 23:59:59 2020 GMT
Subject: C=ZA, **ST=Western** Cape,
L=Cape Town,
O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
3a:c2:b5:66:22:12:d6:87:0d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: md5WithRSAEncryption
07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
70:47

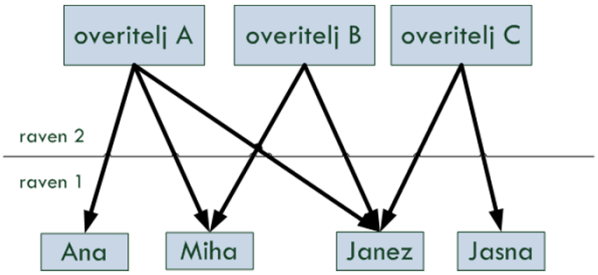
Kompomente PKI



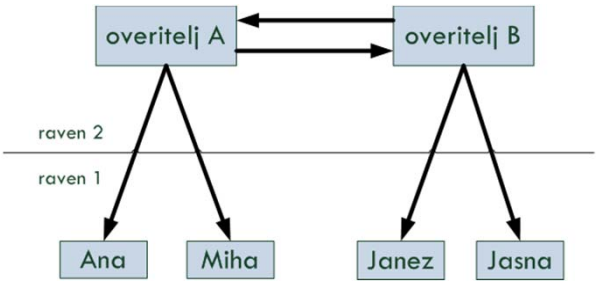
Dvonivojska hierarhija



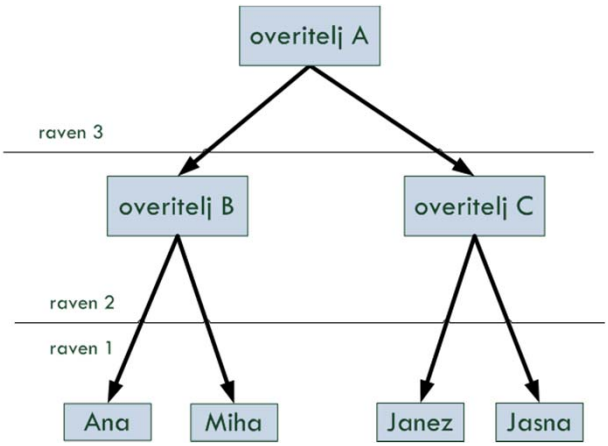
Splet overiteljev



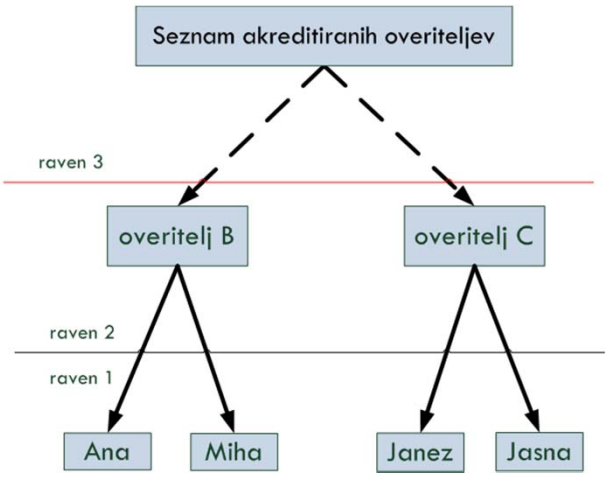
Medsebojno overjanje



Hierarhija overiteljev



Akreditirani overitelji v Sloveniji



Register overiteljev

- Vodi MVZT
- Overitelji:
  - MJU (SIGEN-CA, SIGOV-CA)
  - Halcom d.d. – HALCOM-CA
  - NLB d.d. – NLB klik
  - Pošta Slovenija d.o.o. – PostarCA
- http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/REGISTER_ver20__04.09.2007X.pdf

Predpisi

- ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu (2000)
  - hranjenje dokumentov v elektronski obliki
  - elektronski podpis veljaven tudi, če ne temelji na kvalificiranem potrdilu
  - elektronski podpis=lastnoročen podpis

Elektronski podpis

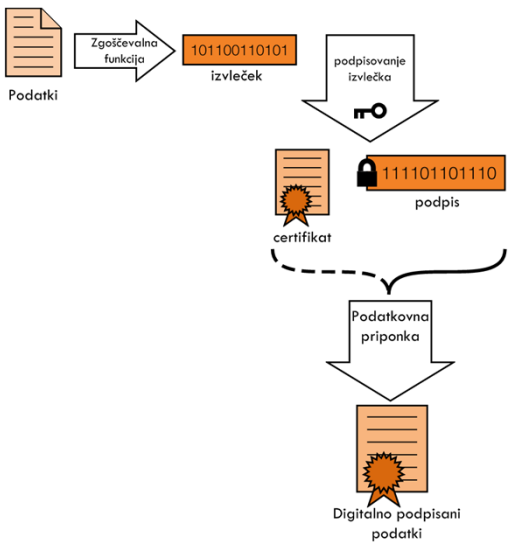
Overjanje sporočil

- ohranjanje celovitosti sporočila
- preverjanje identitete pošiljatelja (overjanje)
- preprečevanje pretvarjanja za drugo osebo

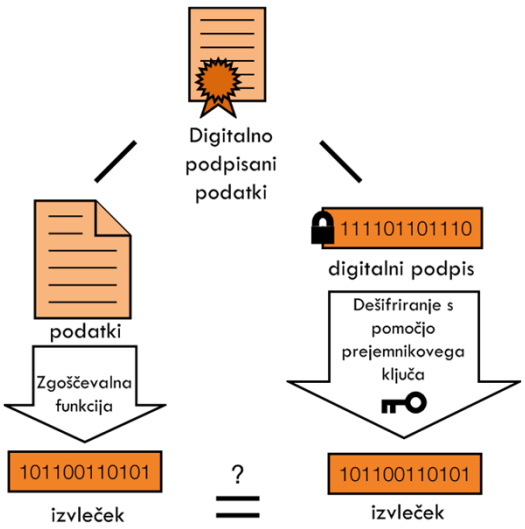
Digitalni podpis

- zagotavlja zaščito pred ponarejanjem
- zagotavlja povezavo s podpisnikom
- se ne da prenesti na drugi dokument
- mora odkriti spremembe v podpisanem dokumentu

Digitalno podpisovanje



Preverjanje digitalnega podpisa



Algoritmi digitalnega podpisovanja

- možnost uporabe algoritma RSA
- podpisnik dekriptira izvorni dokument z zasebnim ključem
- prejemnik izvede RSA šifriranje z javnim ključem.
  Če je sporočilo enako izvornemu, je podpis veljaven

- algoritmov za elektronski podpis je še manj kot asimetričnih algoritmov
- ostale različice temeljijo na diskretnih logaritmih (DL):
  - Digital Signature Algorithm (DSA)

Napadi

- klasični napadi na uporabljene asimetrične algoritme
- izdelava sporočila, ki ustreza že obstoječemu podpisu
- problem predstavitve - napadalec s spremembo programske opreme prepriča uporabnika da podpiše nekaj drugega kot vidi na zaslonu

RSA vs. DSA

- RSA omogoča šifriranje in podpisovanje
- RSA je 10x hitrejši
- za RSA je običajno ključ dolžine 1024 bitov;
  DSA lahko zagotovi enako varnost s krajšim ključem
- DSA mora izdelati naključno število za vsak podpis;
  RSA naključni ključ
- DSA je možno prilagoditi za uporabo z z eliptičnimi krivuljami, da so hitrejši

VARNA E-POŠTA

Varna elektronska pošta

- ELEKTRONSKA POŠTA S POVEČANO ZASEBNOSTJO
- Kombinacija
  - Prikrivanja
  - Protokolov
  - Podatkovne celovitosti

Varna elektronska pošta

- Nevarnosti, ki ogrožajo elektronsko pošto:
  - Prestrezanje sporočil (zaupnost, prekinitev dostopa)
  - Prestrezanje sporočil in delni odgovor
  - Spreminjanje vsebine sporočila
  - Spreminjanje izvora sporočila
  - Ponarejanje sporočila
  - Preklic prenosa sporočila

Varna elektronska pošta

- Z zaščito želimo zagotoviti
  - Zaupnost sporočila
  - Celovitost sporočila
  - Overitev pošiljateljev
  - Ne-zavrnitev (non-repudiation) - pošiljatelj ne more zanikati dejstva, da je sporočilo poslal

Načini zaščite

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- OpenPGP (Pretty Good Privacy)

- Pogojno:
  - TLS (Transport Layer Security)
  - Identity based encryption
  - Mail sessions encryption

S/MIME

Kaj je S/MIME?

- Standard MIME je omogočal pošiljanje slike, zvokovnih datotek, programov in ostalih priponk (MIME – Multipurpose Internet Mail Extension)
- MIME ne zagotavlja varnosti
- S/MIME je varna verzije MIME
- Zagotavlja
  - Zaupnost
  - Overjanje
  - Celovitost

S/MIME: lastnosti

- Uporablja
  - Simetrično šifriranje
  - Kriptografijo javnega ključa
  - Zgoščevalne funkcije
  - Digitalna potrdila po standardu X.509
  - PKI – infrastrukturo javnih ključev
- Uporaba vseh omenjenih tehnik za zagotavljanje praktične, učinkovite in varne el. pošte

S/MIME: lastnosti

- Algoritmi v uporabi:
  - RC2, TripleDES (simetrični algoritmi)
  - RSA (asimetrični algoritem),
  - MD5 oz. SHA-1 (zgoščevalni algoritmi)

S/MIME: zagotavljanje zaupnosti

- Janez program za el. pošto:
  - kreira naključen ključ (sejni ključ), uporaben za asimetrično šifriranje
  - Šifrira sporočilo s pomočjo simetrične šifre in sejnega ključa
  - Šifrira sejni ključ s pomočjo asimetrične kriptografije in Mickinega javnega ključa
  - Kreira paket: šifriranega sporočila, šifriranega sejnega ključa, Janezovega X.509 digitalnega potrdila, imen uporabljenih algoritmov
- Janez program za el. pošto pošlje paket Micki – to je S/MIME el. sporočilo

S/MIME: zagotavljanje zaupnosti

- Mickin program za el. pošto sprejme sporočilo
- Mickin program za el. pošto:
  - Uporabi njen zasebni ključ in ustrezne PKC algoritme za dešifriranje sejnega ključa
  - Uporabi sejni ključ in ustrezne algoritme za dešifriranje el. sporočila

S/MIME: overjanje

- Janez program za el. pošto:
  - Uporabi zgoščevalni funkcijo in oblikuje izvleček el. sporočila
  - Šifrira izvleček s pomočjo PKC algoritma in svojega zasebnega ključa
  - Kreira paket: izvornega sporočila, šifriranega izvlečka, Janezovega X.509 certifikata, imen uporabljenih algoritmov
- Janez program za el. pošto pošlje paket Micki – to je S/MIME el. sporočilo

S/MIME: overjanje

- Mickin program za el. pošto sprejme sporočilo
- Mickin program za el. pošto:
  - Preveri Janezovo X.509 digitalno potrdilo, s preverjanem podpisa certifikacijske agencije (CA)
  - Pridobi Janezov javni ključ iz digitalnega potrdila
  - Uporabi Janezov javni ključ, da dešifrira izvleček
  - Neodvisno izračuna izvleček poslanega sporočila s pomočjo iste zgoščevalne funkcije
  - Primerja izvlečka in s tem preveri pošiljatelja ter celovitost sporočila

S/MIME: zagotavljanje zaupnosti in overjanje

- Sporočilo overimo po postopku opisanem na prejšnjih dveh prosojnicah
- Paket, ki ga tvorimo pri overjanju zavarujemo s postopkom zagotavljanja zaupnosti
- Varovan paket pošljemo prejemniku
- Prejemnik
  - uporabi svoj zasebni ključ, da pridobi javni ključ
  - uporabi sejni ključ, da dešifrira preostanek sporočila in pridobi sporočilo za overjanje
  - s prej opisanim postopkom overi sporočilo

PGP

PGP (Pretty Good Privacy)

- Praktični standard za varno e-pošto
  - Razvil Phil Zimmerman
  - Na razpolago v različnih OS
- Zagotavlja:
  - Zaupnost
  - Celovitost
  - Overjanje
- Ni avtoritete, ki bi podpisovala ključe
- Obstoječi uporabniki podpišejo za nove

PGP (Pretty Good Privacy)

- Vse PGP funkcije se izvedejo v enem programu
- Vsak uporabnik ima javni in privatni ključ
- Privatni ključ zaščiten z geslom
- Javni ključ lahko podpiše več že obstoječih uporabnikov
- Uporabno za prikrivanje, razkrivanje in podpisovanje sporočil

PGP (Pretty Good Privacy)

- Vprašanje legalnosti
  - Legalno uporabno po vsem svetu
  - Nekomercialna uporaba v ZDA/Kanadi z licenčno MIT verzijo
  - Komercialna uporaba v ZDA/Kanadi z licenčno Viacryptverzijo
  - Nekomercialna uporaba zunaj ZDA legalna z mednarodno verzijo (ki ni prišla iz ZDA)
  - Komercialna uporaba izven ZDA zahteva licenco za IDEA
  - Vprašanje, kdo je prvi izvozil PGP iz ZDA

OpenPGP

- Komercializacija PGP-ja
  - Odprt standard za PGP
  - Najbolj znana implementacija GPG (GNU Privacy Guard)