Univerza v Ljubljani
Fakulteta za elektrotehniko

Seminarska naloga

Izdajanje in upravljanje z overili

9.maj 2006 Avtor: Tine Stegel

KAZALO:

Slike:

1 Asimetrična kriptografija

Asimetrična kriptografija temelji na uporabi para ključev javnega in zasebnega ključa. Če podatke šifriramo z enim ključem, jih lahko dešifriramo samo s pripadajočim komplementarnim ključem. Taka ključa imenujemo par asimetričnih ključev.

Slika 1: Asimetrični par ključev

Asimetrična kriptografija je mnogo počasnejša od simetrične, zato se v praksi uporablja hibridni pristop. Pri elektronski pošti je celotno sporočilo zašifrirano s pomočjo naključnega simetričnega ključa, nato pa je sam ključ zašifriran še z javnim ključem prejemnika.

Sama uporaba asimetrične kriptografije v infrastrukturi javnih ključev nam zagotavlja celovitost, zaupnost, nezatajljivost sporočila in preverjanje identitete pošiljatelja. Če sporočilo zašifriramo z javnim ključem prejemnika, ga lahko samo ta prejemnik dešifrira s svojim zasebnim ključem. Ravno obratno velja pri digitalnem podpisu, ko pošiljatelj podpiše sporočilo s svojim zasebnim ključem, prejemnik pa na podlagi njegovega javnega ključa preveri, če je to sporočilo res podpisano s strani pošiljatelja in če med prenosom ni bilo spremenjeno.

Tipični predstavniki kriptografije z javnimi ključi so algoritmi RSA, DSS, DH ali El-Gamal. Javni in zasebni ključi so precej večji od simetričnih (klasičnih) ključev; tipične dolžine znašajo 512, 768, 1024 ali 2048 bitov. Ključ dolžine 512 bitov ne nudi veliko varnosti, saj ga je z dovolj hitrimi računalniki mogoče razbiti v sprejemljivo kratkem času (zgolj ocena: če bi 512-bitni ključ hoteli razbiti v enem letu, bi rabili 10-100 procesorjev Pentium II). Primerna dolžina za osebno uporabo je vsaj 1024 bitov; 2048-bitni ključi se uporabljajo recimo na strežnikih, ki podpisujejo digitalna potrdila.

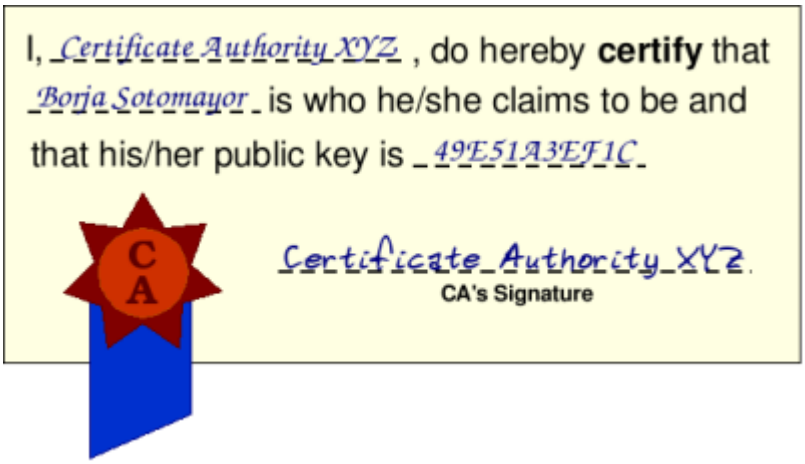
Metoda RSA temelji na predpostavki, da je razmeroma lahko najti dve veliki praštevili, če pa poznamo samo njun zmnožek, je težko najti faktorja. Vzemimo primer s 3-številčnima praštevilomа: 191 x 283 = 54053. Če hočemo faktorirati to število, ga moramo deliti z vsemi praštevili do 191 oziroma v splošnem do njegovega kvadratnega korena. V praksi pa so ta števila več kot stoštevilčna.

Znani so tudi asimetrični algoritmi, ki temeljijo na eliptičnih krivuljah (ECC - elliptic curve cryptosystems). Ideja je znana že od leta 1985. Najdlje na tem področju je kanadska firma Certicom. V primerjavi z RSA zadoščajo krajši ključi, zato kaže, da bodo v bodočnosti ti algoritmi prevladali vsaj pri uporabi v manj zmogljivih napravah.

2 Digitalno potrdilo

2.1 Opis

Digitalno potrdilo predstavlja enolično povezavo med imetnikom potrdila in javnim ključem asimetričnega kodiranja. Potrdilo vsebuje vse osnovne podatke o imetniku in javni ključ. Če ne gre za zaprt sistem uporabnikov, so digitalna potrdila javno objavljena, kar omogoča ugotovitev ter preverjanje identitete podpisnika na osnovi njegovega javnega ključa.



Slika 2: Ilustracija digitalnega potrdila

Stopnjo odgovornosti in tveganja v elektronskem poslovanju lahko stranke rešujejo s kvalificiranimi ali nekvalificiranimi digitalnimi potrdili.

Nekvalificirana potrdila temeljijo na pogodbenem razmerju strank, kjer gre za dogovor med strankami, ki poslujejo po že utečenih poteh. Pri elektronskem poslovanju strank, ki še niso poslovale ena z drugo, pa je smiselna vključitev tretje osebe, ki izdaja kvalificirana potrdila.

Kvalificirana potrdila temeljijo na natančno predpisanem uradnem postopku identifikacije imetnika. Možnost zlorabe je minimalna, saj je podan prepričljiv dokaz o identiteti podpisnika. Takšno identifikacijo lahko izvajajo overitelji in pa v njihovem imenu tudi pooblaščene prijavne službe.

Digitalno potrdilo je tako imetnikova osebna izkaznica v elektronskem poslovanju. Potrdila izdajajo različni overitelji, vendar pa vsi ne zagotavljajo enake stopnje varnosti. Tako lahko uporabniki izbirajo stopnjo varnosti, ki jo potrebujejo za področje svojega poslovanja.

Digitalna potrdila nudijo dve osnovni možnosti za zasebnost v elektronskem poslovanju in komuniciranju:

- šifriranje podatkov, ki zagotavlja zaupnost, in
- digitalni podpis, ki predstavlja sodobno alternativo klasičnemu podpisu, zagotavlja pa:
    - identiteto imetnika digitalnega potrdila
    - nezatajljivost lastništva poslanih e-podatkov, in
    - celovitost (integriteto) sporočila, kar pomeni, da samo dela podatkov ni mogoče spremeniti ali drugače popraviti brez (vednosti) podpisnika.

2.2 Vsebina potrdila

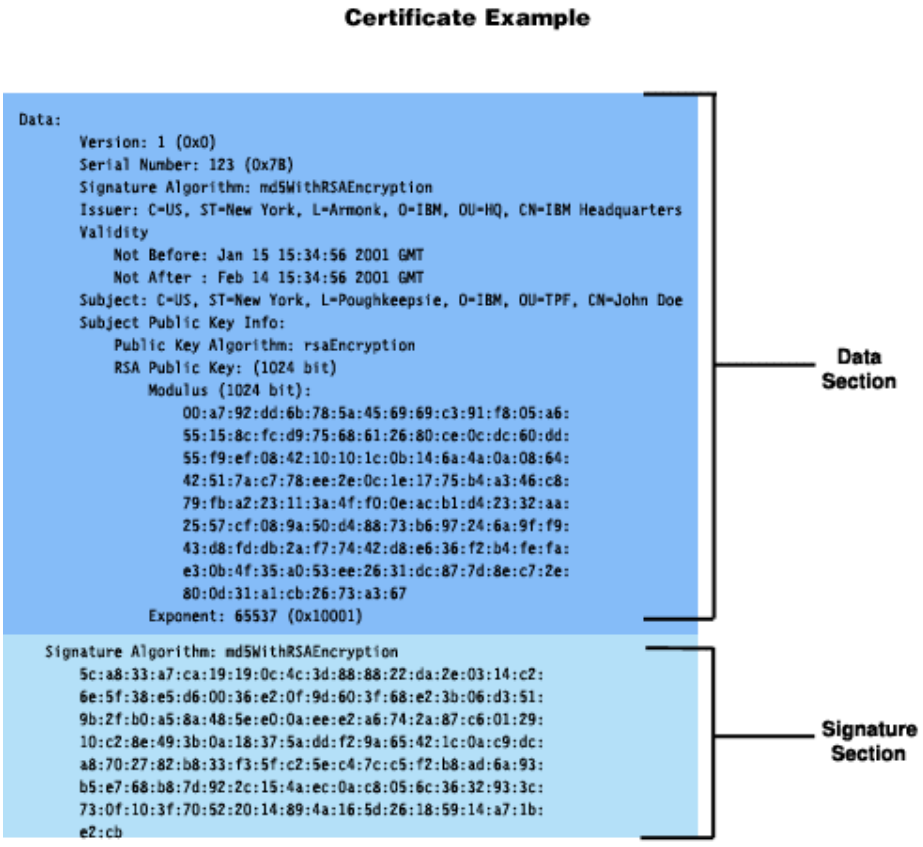
V nadaljevanju je predstavljena oblika digitalnega potrdila po standardu ISO/IEC X.509V3 oziroma njegova vsebina.

Podatkovni del:

- verzija standarda, ki ga potrdilo podpira (zdaj do verzije 3)
- serijska številka potrdila, ki jo enolično določi overitelj
- algoritmi in parametri kodiranja (npr. SHA1 in RSA)
- ime izdajatelja (overitelj javnih ključev)
- datuma veljavnosti potrdila (časovni interval)
- prejemnik digitalnega potrdila (njegovo ime, drugi podatki o njem)
- podatki o njegovem javnem ključu:
    - algoritem
    - parametri
- javni ključ
- enolična oznaka uporabnika (samo v verzijah 2 in 3)
- opcijske razširitve (dodatne informacije)

Podpisni del:

- algoritem digitalnega podpisa
- digitalen podpis teh podatkov (uporabljen je zasebni ključ overitelja)

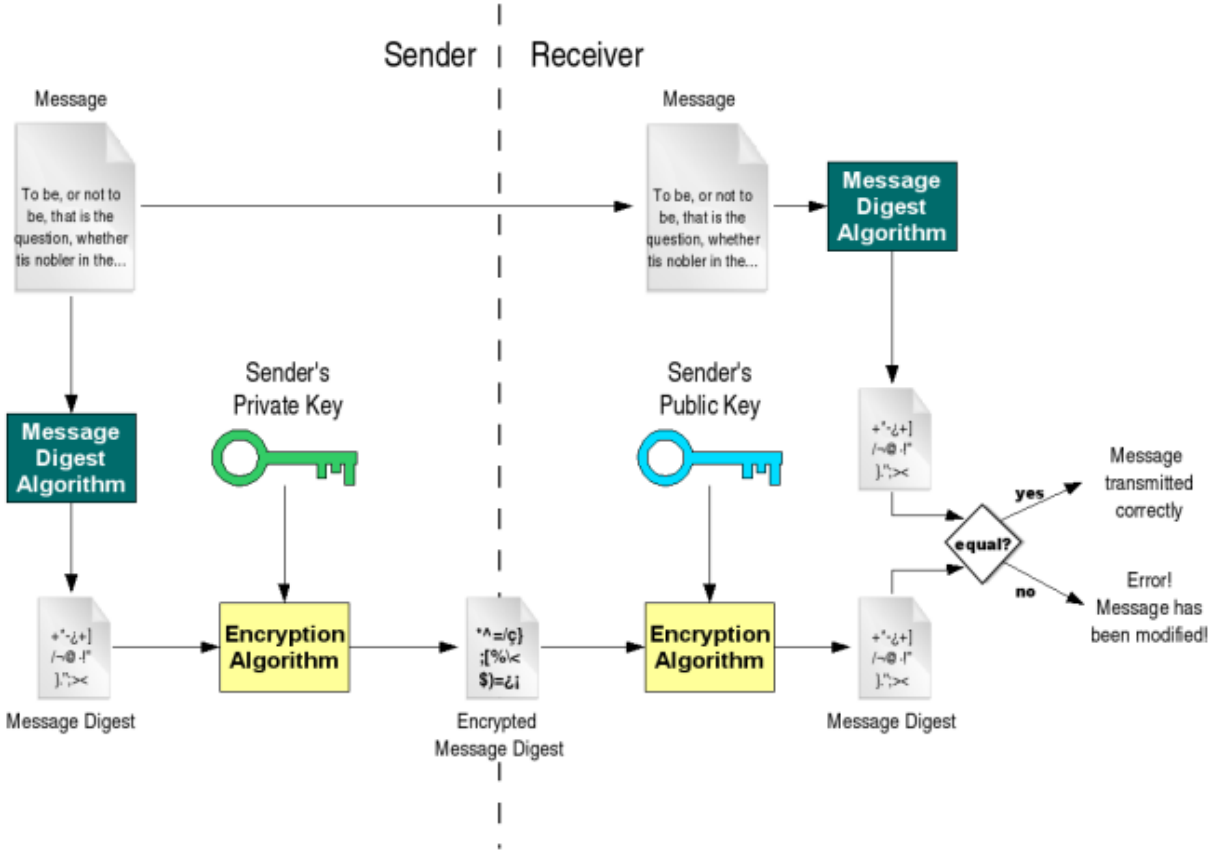


Slika 3: Primer vsebine potrdila

2.3 Možnosti uporabe

2.3.1 Digitalni podpis

Osnovna funkcija digitalnega podpisa je v dokazovanju identitete podpisnika elektronskega dokumenta in zagotavljanju celovitosti podatkov oziroma zaščite pred spreminjanjem vsebine e-dokumentov. Digitalni podpisi temeljijo na asimetrični kriptografiji, zato potrebujemo par ključev - zasebnega za podpisovanje in javnega za preverjanje veljavnosti podpisov.

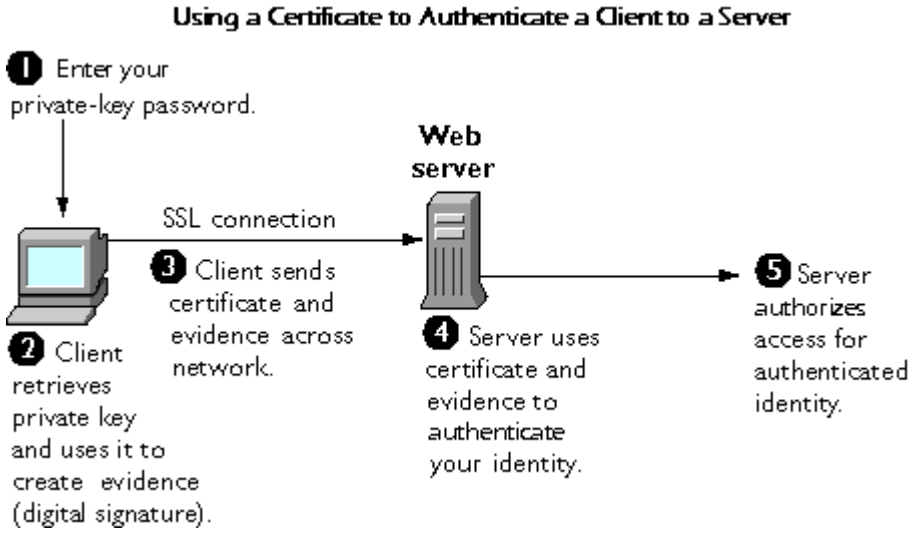


Slika 4: Metoda digitalnega podisa

Digitalno podpisovanje je pravzaprav izdelava prstnega odtisa podatkov, ki je vedno unikaten - vsakemu dokumentu pripada samo en prstni odtis. Pri digitalnem podpisovanju dokumenta se vhodni podatki pretvorijo z zgoščevalno funkcijo, katere rezultat je prstni odtis dokumenta. Ko prstni odtis dokumenta zakripiramo z zasebnim ključem, dobimo digitalni podpis dokumenta.

Dokument digitalno podpišemo s svojim zasebnim ključem, medtem ko podpis preverjamo z javnim ključem podpisnika. Ključa sta med seboj tako povezana, da podpis dokumenta, ki smo ga naredili z zasebnim ključem, lahko preverimo samo z javnim ključem iz para.

Spodnji primer prikazuje avtentikacijo med spletnim uporabnikom in strežnikom.



Slika 5: Avtentikacija uporabnik-strežnik

2.3.2 Kriptiranje

Sama uporaba asimetrične kriptografije v infrastrukturi javnih ključev nam zagotavlja celovitost, zaupnost, nezatajljivost sporočila in preverjanje identitete pošiljatelja. Če sporočilo zašifriramo z javnim ključem prejemnika, ga lahko samo ta prejemnik dešifrira s svojim zasebnim ključem. Ravno obratno velja pri digitalnem podpisu, ko pošiljatelj podpiše sporočilo s svojim zasebnim ključem, prejemnik pa na podlagi njegovega javnega ključa preveri, če je to sporočilo res podpisano s strani pošiljatelja in če med prenosom ni bilo spremenjeno.

Slika 6: Kriptiranje z uporabo potrdila

2.3.3 Varni časovni žig (Time-stamping)

V splošnem je varni časovni žig digitalni zapis, ki zagotavlja podpis dokumenta z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način.

2.3.3.1 Postopek časovnega žigosanja

Ko želimo v neki aplikaciji časovno žigosati nek elektronski dokument oziroma podatke, pošljemo strežniku TSA z zgostitveno funkcijo narejen "povzetek" (hash) dokumenta oziroma podatkov. To je niz bitov fiksne dolžine (običajno 160 bitov), ki enolično določa dokument. Strežnik temu povzetku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem - to je časovni žig. S tem je dokazano, da je elektronski dokument obstajal pred časom, navedenim v časovnem žigu, poleg tega pa se da preveriti, da se od časa žigosanja ni spremenil (naredimo ponovni povzetek dokumenta in se mora ujemati s tistim, ki je del časovnega žiga). Postopek je opisan v RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP).

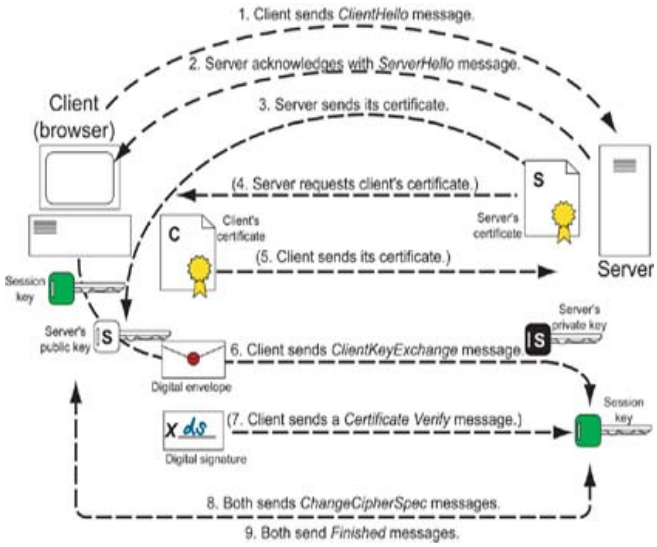
Slika 7: Postopek časovnega žigosanja

2.3.4 SSL (Secure Sockets Layer)

SSL je protokol, ki zagotavlja zasebnost in celovitost podatkov v komunikaciji med dvema aplikacijama, ki sta povezani z TCP/IP povezavo. Podatki, ki se prenašajo, so zakriptirani s simetričnim algoritmom (DES ali RC4). Sistem javnih ključev se uporabi za izmenjavo simetričnih ključev in podpisovanje podatkov. Za kriptiranje algoritem uporabi javni ključ destinacijske aplikacije, ki ga dobi v javno objavljenem digitalnem potrdilu. Za podpisavanje pa uporabi aplikacija svoj privatni ključ.

Protokol se uporablja pri:

- spletnih strežnikih, ki omogočajo varne povezave do spletnih brskalnikov
- povezavi med LDAP strežniki in LDAP uporabniki
- Host-on-Demand V2 za zagotavljanje varne povezave med uporabnikom in gostiteljem



Slika 8: Potek SSL varne povezave

SSL uporablja digitalna potrdila za izmenjavo ključev, indentifikacijo strežnika in opcijsko tudi identifikacijo uporabnika.

2.4 Varnost

Avtentikacija in kriptiranje z digitalnim potrdilom temeljita na podatkih, ki so dostopni samo uporabniku. To sta privatni ključ in geslo, ki privatni ključ ščiti na mediju, kjer je shranjen. Tehnologija digitalnih potrdil ne rešuje problemov fizične varnosti kot so:

- dostop nepooblaščenih oseb do računalnika ali podatkov,
- odpoved strojne ali programske opreme in
- raznih naravnih nesreč.

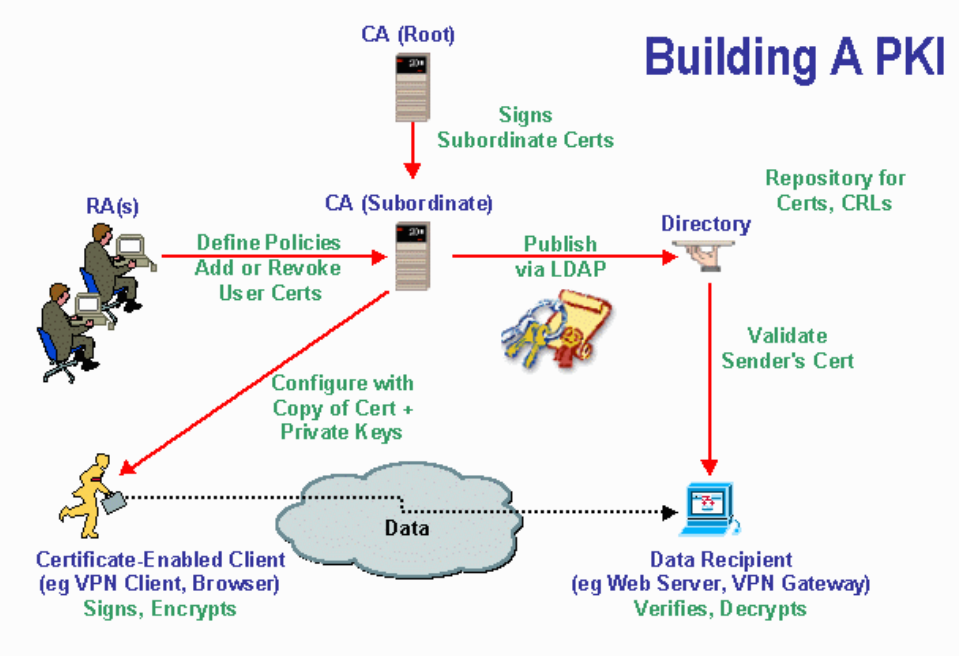
Varna shramba privatnega ključa in njegovo arhiviranje je pomembna naloga vsakega lastnika potrdila.

3 Infrastruktura javnih ključev (PKI - Public-Key Infrastructure)

Infrastruktura javnih ključev vključuje pravno, tehnično in organizacijsko infrastrukturo za izdajo, upravljanje in preklic potrdil, ki podpirajo avtentikacijo, šifriranje, celovitost in nezataljivost v elektronskem poslovanju.

Infrastrukturo javnih ključev določajo postopki in oprema za:

- generiranje in hranjenje ključev,
- overjanje imetnikov ključev in izdajanje digitalnih potrdil javnih ključev,
- objavljanje digitalnih potrdil (imeniki),
- preklicevanje digitalnih potrdil,
- časovno označitev postopkov.



Slika 9: infrastruktura javnih ključev (PKI)

3.1 Overitelj (Certification Authority - CA)

Overitelj (Certification Authority - CA) igra osrednjo vlogo v infrastrukturi javnih ključev. Predstavlja ustanovo, ki ji zaupajo uporabniki digitalnih potrdil in digitalnih podpisov.

Overitelj prejema zahteve za izdajo digitalnih potrdil, izvaja ustrezno identifikacijo bodočih imetnikov, izdaja digitalna potrdila in skrbi za register izdanih potrdil, saj so informacije o izdanih potrdilih javnega značaja (razen v zaprtih sistemih). Overitelj prav tako skrbi za preklic digitalnih potrdil in informacije o preklicih osvežuje v registru preklicanih potrdil, ki je prav tako javnega značaja.

Overitelj, ki izdaja kvalificirana potrdila, zanesljivo ugotovi ter preveri identiteto in druge pomembne lastnosti osebe, ki naroča izdajo potrdila. Takšno identifikacijo lahko izvajajo overitelji, v njihovem imenu pa tudi pooblaščene prijavne službe, ki prav tako preverijo identiteto prosilca in originalno

dokumentacijo za izdajo kvalificiranega potrdila ter jo na varen način posredujejo overitelju. Vso potrebno dokumentacijo za izdajo kvalificiranih digitalnih potrdil je tako mogoče oddati na sedežu overitelja, s pomočjo notarjev in v pooblaščenih prijavnih službah.

Overitelj (agencija za certificiranje) je pravna oseba, ki je pooblaščena za izdajo digitalnih potrdil ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

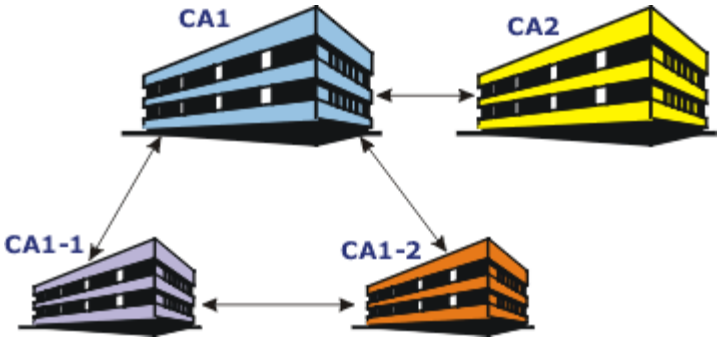
Vsak overitelj objavi svoj javni ključ in dokumente o overiteljskih politikah (Certification Policies), ki opisujejo različne podprte postopke, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ. Celoten proces izdajanja posameznih skupin digitalnih potrdil natančno določa overiteljska politika.

Glede na zahtevnost postopka preverjanja identitete tistega, ki mu bo izdal digitalno potrdilo, overitelj lahko izdaja digitalna potrdila na različnih nivojih zaupanja. Lahko npr. določi, da se mora posameznik osebno zglasiti in predložiti osebni dokument, lahko pa podeli digitalno potrdilo na osnovi zahtevka, poslanega po elektronski pošti. Jasno je, da je mogoče bolj zaupati digitalnemu potrdilu, podeljenemu po prvem postopku kot po drugem. Poskrbeti mora, da so imetniki digitalnih potrdil enolično določeni (posameznik ima lahko več javnih ključev in torej tudi digitalnih potrdil) in za poseben seznam preklicanih digitalnih potrdil (torej tistih digitalnih potrdil, ki so iz različnih vzrokov neveljavni).

Pomembno je tudi, da overitelj poskrbi za varnost svojega zasebnega ključa, saj bi bila sicer potrdila, ki jih je izdal, brez pomena - še več, lahko bi prišlo do poneverb, ki bi jih prepozno opazili. Hraniti ga morajo na dobro zaščitenem računalniku.

Slika 10: Medsebojno zaupanje prek overitelja

Podobno je overitelj ustanova, ki ji lahko zaupajo tudi ostali overitelji ali posamezniki in posredno s tem tudi lastnikom vseh digitalnih potrdil, ki jih je overitelj izdal in potrdil. Tako se lahko različni overitelji povezujejo na različne načine, bodisi horizontalno, kjer se medsebojno overijo in s tem omogočijo varno in zanesljivo komunikacijo med lastniki digitalnih potrdil obeh ustanov (npr. podobno kot pri medsebojnem priznanju potnih listov med državama) ali vertikalno, ko nek overitelj pooblasti neko drugo ustanovo za izdajanje digitalnih potrdil v njegovem imenu, kar je seveda potrebno pri upravljanju z velikim številom digitalnih potrdil, poleg tega pa se z medsebojnim priznavanjem veča nabor e-storitev, ki so možne s posameznimi digitalnimi potrdili.



Slika 11: Medsebojno zaupanje med overitelji

Metoda digitalnih potrdil temelji na zaupanju v certifikat oziroma v zaupanje v overitelja, ki je potrdilo izzdal. Vsak posameznik se sam odloči, kateri overitelji so vredni zaupanja. Njegova infrastruktura javnih ključev (PKI) vsebuje seznam zaupanja vrednih overiteljev in njihovih javnih ključev, s katerimi preverja overiteljeve digitalne podpise. Nekateri overitelji so v svetu dobro poznani, zato so v nekatere aplikacije že vključeni. Primer sta VeriSign in GlobalSign, ki sta že vključena v spletne brskalnike.

3.2 RA (Registration Authority)

Registration Authority (registracijska pisarna overitelja) je podrejeni overitelj (agencija za registracijo ali pooblaščena prijavna služba). RA predstavlja vezni člen med overiteljem in končnimi uporabniki ter vključuje preverjanje identitete in komuniciranje s končnimi uporabniki.

RA je odgovorna za shranjevanje in preverjanje vseh podatkov, ki jih overitelj potrebuje. Njena najpomembnejša naloga je preverjanje identitete prosilca za izdajo potrdila. To se največkrat izvede s pregledom osebnega dokumenta. RA ponavadi ni dostopna preko spleta, ampak se morajo prosilci tam zglasiti osebno. Ko je avtentikacija potrebnih podatkov opravljena, RA te podatke posreduje overitelju, ki prosilcu izda digitalno potredilo.

3.3 Javni imenik potrdil (Directory Service)

Javni imenik je javno dostopna točka, ki vsebuje overiteljski seznam izdanih potrdil. Uporabniki preko imenika preverjajo veljavnost tujih potrdil ter pridobivajo tuje javne ključe za dekriptiranje zaščitenih vsebin.

Imenik potrdil mora opravljati dve nalogi:

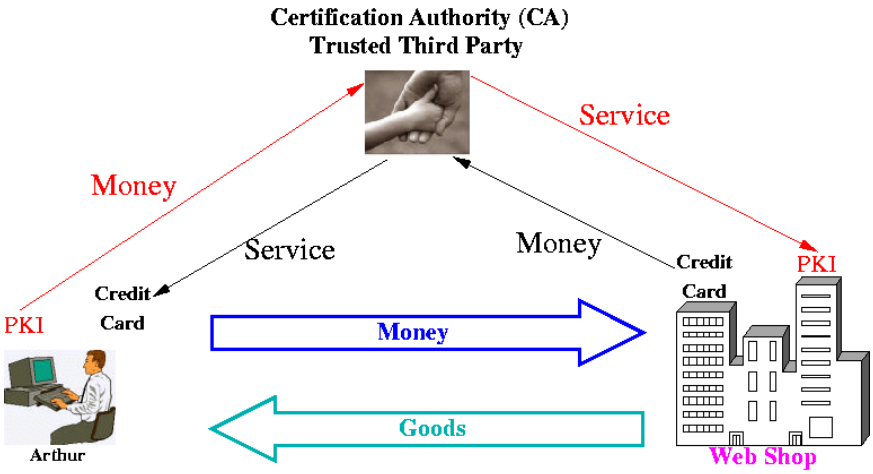
- objava javnih ključev in drugih infomacij o potrdilih
- objava seznama preklicanih potrdil (CLR)

3.4 Uporabnik

Uporabnikova programska oprema (npr. brskalnik) omogoča sodelovanje z vsemi elementi infrastrukture javnih ključev. Programska oprema glede na parametre, ki jih nastavi uporabnik, odloča o uporabi digitalnih potrdil ter presoja o zaupanju sprejetih podatkov, ki so zaščiteni s tujimi potrdili. Uporabnik ni nujno lastnik potrdila, saj uporablja PKI oziroma objavljene javne ključe tudi za vsa druga njemu tuja potrdila.

Uporabnik se mora odločiti, katerim overiteljem eksplicitno zaupa, ter temu ustrezno nastaviti programsko opremo. Avtentikacija in veljavnost tujih potrdil se nato postopoma preverja glede na relacije v verigi zaupanja oziroma križnega potrjevanja overiteljev.

Uporabniki potrdil so pravzaprav generatorji in uporabniki spletnih storitev, ki potrebujejo varno komunikacijo. Ostali elementi infrastrukture javnih ključev pa uporabnikom to varno komunikacijo zagotavljajo.



Slika 12: Varna spletna storitev

Pojem uporabnika lahko uporabimo tudi pri medsebojnem sodelovanju dveh overiteljev. Pri tem overitelja izdata drug drugemu potrdilo, ki ga uporabljata za nadaljno varno komunikacijo (križno potrjevanje).

4 Sporazumi glede varnosti in uporabnosti potrdil

4.1 Overiteljska politika (Certificate Policy – CP)

S tem, ko overitelj izda digitalno potrdilo, uporabnikom potrdila da na voljo izjavo o povezavi določenega javnega ključa z lastnikom potrdila. Do kakšne mere bo uporabnik zaupal izjavi overitelja, je odvisno od samega uporabnika. Ker so digitalna potrdila namenjena različni uporabi ter morajo tako zadostiti tudi različnim kriterijem varnosti, se le ta lahko izdajajo po različnih postopkih in praksah. Za potrdila, ki zagotavljajo visoko varnost, se mora upoštevati vse varnostne mehanizme, medtem ko za manj varnostno zahtevne storitve včasih ni potrebna niti osebna avtentikacija.

Standard X.509 definira overiteljsko politiko kot seznam pravil in postopkov izdajanja, ki s svojo stopnjo zahtevnosti definirajo ciljno skupino uporabnikov potrdil s podobnimi varnostnimi zahtevami. Vsako izdano potrdilo lahko vsebuje indentifikator overiteljske politike (Object Identifier), ki definira politiko, katero je upošteval overitelj pri njegovem izdajanju. Na podalgi tega parametra se uporabnik odloči ali bo potrdilu zaupal pri določeni spletni storitvi ali ne.

Overiteljska politika mora biti prepoznavna in enoumno določena tako s strani overitelja kot tudi s strani uporabnika digitalnega potrdila. Vsak overitelj zato poleg digitalnih potrdil javno objavi tudi indentifikatorje overiteljskih politik ter njihove podrobne tekstovne specifikacije. Na ta način lahko vsak uporabnik prebere pravila ter se odloči, katera politika ustreza njegovim varnostnim zahtevam.

Zbirka politik, ki jih overitelj podpira, je osnova za ocenjevanje mere zaupanja do overitelja. Ko si overitelji izdajajo medsebojna digitalna potrdila, v tej zbirki ocenijo in določijo katerim politikam zaupajo. Tako overitelj zaupa vsem potrdilom sodelujočega overitelja, ki so bila izdana in upravljanja po pravilih in postopkih zaupanih politik.

4.1.1 Primeri overiteljskih politik

Za primer vzemimo organizacijo International Air Transport Association (IATA), ki se odloči definirati overiteljske politike za uporabo potrdil v letalski industriji. Uporabljena bo kombinacija lokalne PKI pod nadzorom IATA ter PKI-ji posameznih drugih letalskih ogranizacij oziroma podjetij. IATA se odloči za dve različni politiki. Prva politiko imenuje IATA General-Purpose, drugo pa IATA Commercial-Grade.

Politika IATA General-Purpose je namenjena za zaščito rutinskih podatkov zaposlenih v industriji (običajna elektronska pošta) in za avtentikacijo TCP/IP povezav med spletnimi brskalniki in strežniki pri dostopanju do splošnih infomacij. Pari ključev so lahko ustvarjeni, shranjeni in upravljani z uporabo cenovno ugodne programske opreme, kot naprimer spletnih brskalnikov. Pod to politiko je IATA določila, da se digitalno potrdilo lahko izda vsem zaposlenim v organizaciji in vsem članicam organizacije (ostalim letalskim družbam), ki dostavijo podpisan dopis oziroma zahtevek za digitalno potrdilo za njihovo kontaktno osebo.

Politika IATA Commercial-Grade je namenjena zaščiti finančnih transakcij in zavezujočih pogodbenih obveznosti med letalskimi družbami. Pod to politiko IATA zahteva, da se pari ključev ustvarijo in shranijo v odobreni kriptografski strojni opremi (approved cryptographic hardware tokens). Potrdila in kriptografska strojna oprema so dostopna samo zaposlenim v letalski industriji, ki so pristojni za dostop do teh občutljivih podatkov. Ti določeni posamezniki se morajo osebno zglasiti v varnostni službi organizacije IATA, pokazati veljaven osebni dokument ter podpisati zavezujočo izjavo, da bodo ustrezno varovali kriptografsko strojno opremo ter uporabljali potrdila le v dovoljenih primerih. Potrdilo jim je izdano šele po izpolnjenih varnostnih pogojih.

4.1.2 Priporočena struktura overiteljske politike

RFC 2527 definira spodaj navedene osnovne točke overiteljske politike. Omenjena struktura dokumenta ni obvezna, se pa njena uporaba namerno spodbuja, saj je enako strukturirane politike različnih overiteljev lažje primerjati.

1. INTRODUCTION
1.1 Overview
1.2 Document name and identification
1.3 PKI participants
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 Subscribers
1.3.4 Relying parties
1.3.5 Other participants
1.4 Certificate usage
1.4.1. Appropriate certificate uses
1.4.2 Prohibited certificate uses
1.5 Policy administration
1.5.1 Organization administering the document
1.5.2 Contact person
1.5.3 Person determining CPS suitability for the policy
1.5.4 CPS approval procedures
1.6 Definitions and acronyms
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES
2.1 Repositories
2.2 Publication of certification information
2.3 Time or frequency of publication
2.4 Access controls on repositories
3. IDENTIFICATION AND AUTHENTICATION (11)
3.1 Naming
3.1.1 Types of names
3.1.2 Need for names to be meaningful
3.1.3 Anonymity or pseudonymity of subscribers
3.1.4 Rules for interpreting various name forms
3.1.5 Uniqueness of names
3.1.6 Recognition, authentication, and role of trademarks
3.2 Initial identity validation
3.2.1 Method to prove possession of private key
3.2.2 Authentication of organization identity
3.2.3 Authentication of individual identity
3.2.4 Non-verified subscriber information
3.2.5 Validation of authority
3.2.6 Criteria for interoperation
3.3 Identification and authentication for re-key requests
3.3.1 Identification and authentication for routine re-key
3.3.2 Identification and authentication for re-key after revocation
3.4 Identification and authentication for revocation request
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)
4.1 Certificate Application
4.1.1 Who can submit a certificate application
4.1.2 Enrollment process and responsibilities
4.2 Certificate application processing
4.2.1 Performing identification and authentication functions
4.2.2 Approval or rejection of certificate applications
4.2.3 Time to process certificate applications
4.3 Certificate issuance
4.3.1 CA actions during certificate issuance
4.3.2 Notification to subscriber by the CA of issuance of certificate
4.4 Certificate acceptance
4.4.1 Conduct constituting certificate acceptance
4.4.2 Publication of the certificate by the CA
4.4.3 Notification of certificate issuance by the CA to other entities
4.5 Key pair and certificate usage
4.5.1 Subscriber private key and certificate usage
4.5.2 Relying party public key and certificate usage
4.6 Certificate renewal
4.6.1 Circumstance for certificate renewal
4.6.2 Who may request renewal
4.6.3 Processing certificate renewal requests
4.6.4 Notification of new certificate issuance to subscriber
4.6.5 Conduct constituting acceptance of a renewal certificate
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities
4.7 Certificate re-key
4.7.1 Circumstance for certificate re-key
4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities
4.8 Certificate modification
4.8.1 Circumstance for certificate modification
4.8.2 Who may request certificate modification
4.8.3 Processing certificate modification requests
4.8.4 Notification of new certificate issuance to subscriber
4.8.5 Conduct constituting acceptance of modified certificate
4.8.6 Publication of the modified certificate by the CA
4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Certificate revocation and suspension
4.9.1 Circumstances for revocation
4.9.2 Who can request revocation
4.9.3 Procedure for revocation request
4.9.4 Revocation request grace period
4.9.5 Time within which CA must process the revocation request
4.9.6 Revocation checking requirement for relying parties
4.9.7 CRL issuance frequency (if applicable)
4.9.8 Maximum latency for CRLs (if applicable)
4.9.9 On-line revocation/status checking availability
4.9.10 On-line revocation checking requirements
4.9.11 Other forms of revocation advertisements available
4.9.12 Special requirements re key compromise
4.9.13 Circumstances for suspension
4.9.14 Who can request suspension
4.9.15 Procedure for suspension request
4.9.16 Limits on suspension period
4.10 Certificate status services
4.10.1 Operational characteristics
4.10.2 Service availability
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities
4.7 Certificate re-key
4.7.1 Circumstance for certificate re-key
4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities
4.8 Certificate modification
4.8.1 Circumstance for certificate modification
4.8.2 Who may request certificate modification
4.8.3 Processing certificate modification requests
4.8.4 Notification of new certificate issuance to subscriber
4.8.5 Conduct constituting acceptance of modified certificate
4.8.6 Publication of the modified certificate by the CA
4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Certificate revocation and suspension
4.9.1 Circumstances for revocation
4.9.2 Who can request revocation
4.9.3 Procedure for revocation request
4.9.4 Revocation request grace period
4.9.5 Time within which CA must process the revocation request

9.4.5 Notice and consent to use private information
9.4.6 Disclosure pursuant to judicial or administrative process
9.4.7 Other information disclosure circumstances
9.5 Intellectual property rights
9.6 Representations and warranties
9.6.1 CA representations and warranties
9.6.2 RA representations and warranties
9.6.3 Subscriber representations and warranties
9.6.4 Relying party representations and warranties
9.6.5 Representations and warranties of other participants
9.7 Disclaimers of warranties
9.8 Limitations of liability
9.9 Indemnities
9.10 Term and termination
9.10.1 Term
9.10.2 Termination
9.10.3 Effect of termination and survival
9.11 Individual notices and communications with participants
9.12 Amendments
9.12.1 Procedure for amendment
9.12.2 Notification mechanism and period
9.12.3 Circumstances under which OID must be changed
9.13 Dispute resolution provisions
9.14 Governing law
9.15 Compliance with applicable law
9.16 Miscellaneous provisions
9.16.1 Entire agreement
9.16.2 Assignment
9.16.3 Severability
9.16.4 Enforcement (attorneys' fees and waiver of rights)
9.16.5 Force Majeure
9.17 Other provisions

4.2 Sporazum med sodelujočima stranema (Relying Party Agreements)

Sporazum med sodelujočima stranema je sporazum med overiteljem in naročnikom digitalnega potrdila. Njegov namen je definirati dolžnosti, odgovornosti in pogoje med overiteljem in naročnikom, ki se zanaša na pravilno in varno delovanje celotnega sistema PKI. Primer: sporazum lahko zahteva, da naročnik pred vsako uporabo potrdila preveri ali je bilo potrdilo vmes že preklicano. Dejansko izvajanje teh sporazumov je zaradi njihove narave težko nadzirati ali zakonsko prisiliti.

Pogoji, ki so običajno vključeni v sporazume so:

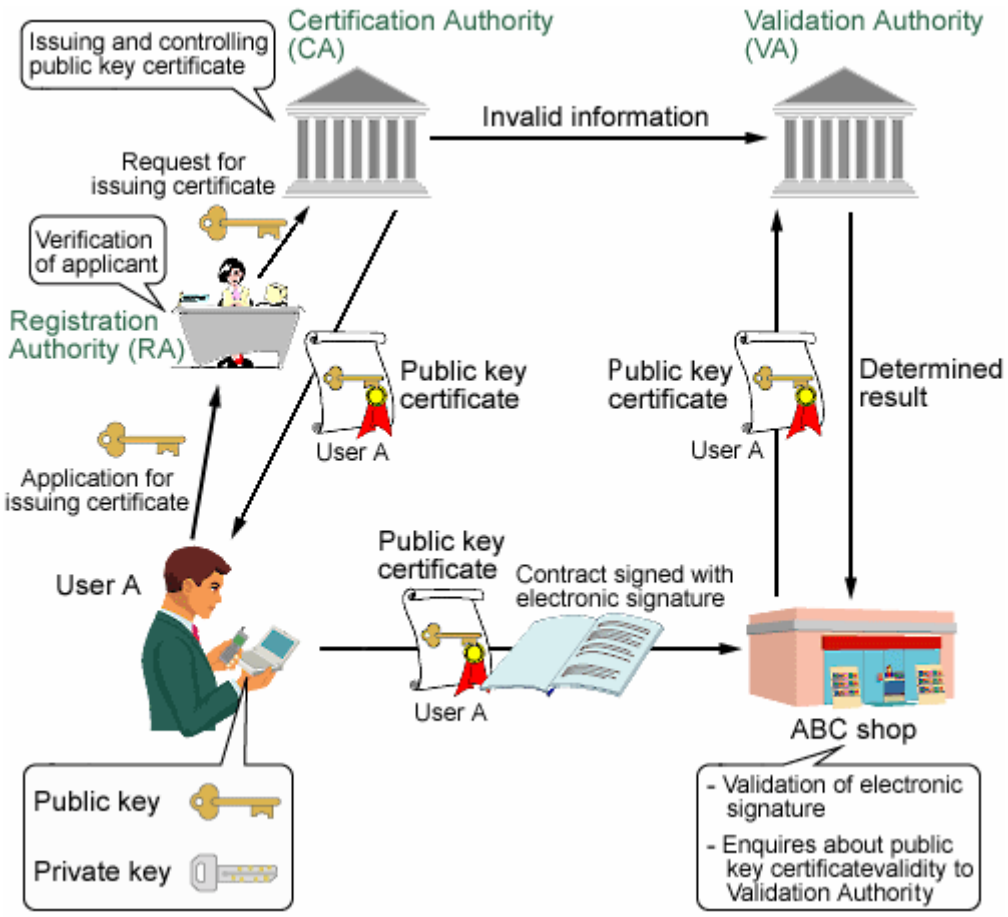
- Pravilna/dovoljena uporaba potrdil. Ta obsega tip uporabe (podpis ali kriptiranje) ter seznam specifičnih aplikacij oziroma postopkov, kjer je uporaba potrdil specifično dovoljena ali prepovedana.
- Identiteta posameznikov oziroma organizacij, s katerimi je dovoljeno sodelovanje. (Primer – Organizacija, ki sama podpisuje in izdaja digitalna potrdila, omeji uporabo potrdil na zaposlene v organizaciji in njihove stranke)
- Zahteva za pravilno izvajanje kriptografskih operacij z uporabo programske in strojne opreme, ki ustreza varnostnemu standardu.
- Omejitve glede zanesljivosti.

5 Izdajanje potrdil

5.1 Lokacija izdelave asimetričnih ključev

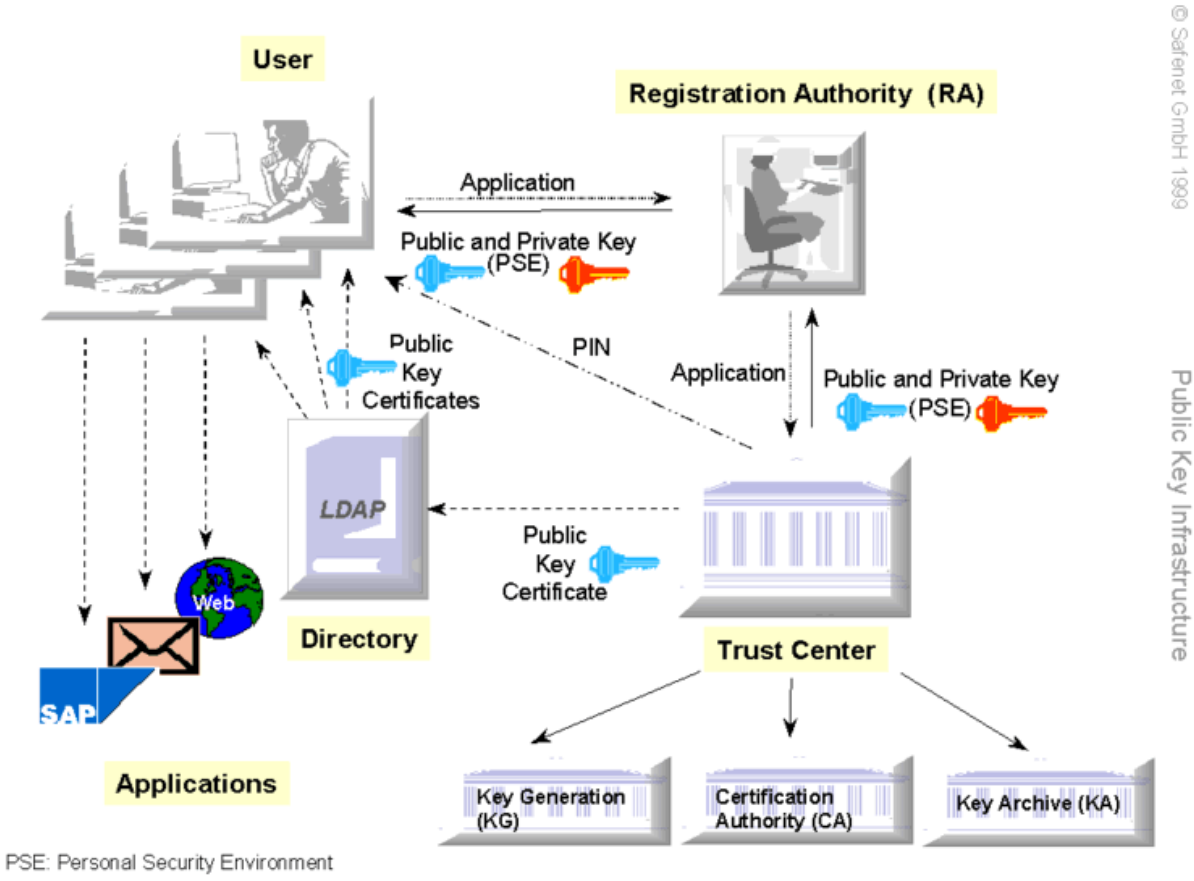
Če je par ključev generiran na strani naročnik, le ta obdrži privatni ključ ter ga varno spravi in opcijsko tudi arhivira v svojem lokalnem sistemu. Overitelju pošlje svoj javni ključ, ki ga le ta poveže z naročnikovo identiteto, ki jo avtenticira s primernimi standardnimi ali nestandardnimi postopki. Digitalno potrdilo, ki vsebuje tudi naročnikov javni ključ, pa overitelj objavi v svojem imeniku. Prednost tega postopka je v tem, da privatni ključ naročnika pozna le naročnik sam.

Primer: Pridobitev kvalificiranega digitalnega potrdila za elektronsko podpisovanje in kriptiranje podatkov.



Slika 13: Naročnik generira par ključev

Če je par ključev generiran na strani overitelja, mora le ta poleg avtentikacije naročnika, naročniku tudi varno dostaviti naročnikov privatni ključ. Naročnikov privatni ključ torej poznata najmanj overitelj in naročnik, do njega pa lahko pri dostavi teoretično pride tudi kak napadalec. Prednost tega postopka je, da overitelj pozna naročnikov privatni ključ, ki ga lahko arhivira za kasnejšo uporabo.



Slika 14: Overitelj generira par ključev

Primer: Neko podjetje postavi svojo infrastrukturo javnih ključev, kjer želi zagotoviti varnost podatkov glede na okolje izven podjetja. Znotraj podjetja med zaposlenimi, ki si zaupajo, pa visoka stopnja varnosti in anonimnosti ni več potrebna. Podjetje lahko dostavlja privatne ključe preko lokalnega omrežja oziroma z osebnim stikom preko različnih prenosnih medijev (USB ključ, CD...)

5.2 Izdajanje prvih potrdil

Postopek izdajanja prvih potrdil je omejen na prvi stik naročnika z overiteljem. Overitelj namreč ne ve s kom ima opravka.

5.2.1 Stopnje varnosti

Pri izdajanju potrdila se mora upoštevati dogovorjena overiteljska politika. Ta lahko zahteva različno visoko stopnjo varnosti, kar se odraža v različno varnih postopkih:

- avtentikacije naročnika potrdila,
- avtentikacije overitelja,
- dostave privatnega ali javnega ključa,
- shrambe in arhiviranja ključev.

5.2.2 Avtentikacija naročnika

Možnih načinov avtentikacije naročnika je zelo veliko, ker si lahko vsak overitelj poljubno izbere sebi prirejen postopek. Omenili bomo le nekaj najbolj pogostih načinov.

Najbolj varna avtentikacija naročnika je osebna zglasitev naročnika pri prijavni službi overitelja (RA). Svojo identiteto naročnik dokaže z veljavnim osebnim dokumentom. RA nato o uspešni avtentikaciji naročnika obvesti overitelja, ki glede na pridobljene podatke izda digitalno potrdilo. Tak postopek avtentikacije je značilen za zakonsko določena kvalificirana potrdila in vsa druga potrdila, ki zahtevajo visoko varnost.

Overitelj v nekem podjetju lahko prebere podatke o bodočih lastnikih potrdil kar iz svojega seznama zaposlenih.

Kadar identiteta naročnika ni pomembna (anonimnost), se lahko logična identiteta oziroma lastništvo privatnega ključa (Proof of Posession) dokaže s podpisanim javnim ključem. Rezultat zgoščevalne funkcije na javnem ključu naročnik zakriptira s svojim privatnim ključem.

5.2.3 Avtentikacija CA ali RA

Avtentikacija je za overitelje, ki jim naročnik oziroma uporabnik eksplicitno zaupa, neposredna s samo-podpisanim potrdilom overitelja. Uporabi se javni ključ za preverjanje pristnosti overiteljevega podpisa.

Če ciljni overitelj ni v seznamu overiteljev, ki jim naročnik ali uporabnik eksplicitno zaupa, se avtentikacija izvaja postopno po verigi zaupanja, dokler naročnik ne prejme potrdila korenskega overitelja, ki mora biti v naročnikovem seznamu zaupanja vrednih overiteljev.

5.2.4 Izmenjava ključev začetne komunikacije

Izmenjava asimetričnih ključev se največkrat izvede po kakem nestandardnem (ang. out-of-band) postopku. Za primer navedimo banko, ki se s svojim komitentom dogovori o izdelavi digitalnega potrdila. Komitent se osebno zglasi na banki, kjer zahteva izdajo potrdila. Banka mu nato pošlje en del kriptirnega ključa preko navadne pošte in drugi del kriptirnega ključa po elektronski pošti. Komitent nato doma preko spletnega brskalnika s pomočjo kriptirnih ključev vzpostavi varno TCP/IP povezavo, po kateri se izmenjajo asimetrični ključi digitalnega potrdila.

6 Upravljanje potrdil

6.1 Lastniki potrdil

Lastniki lahko vplivajo na preklic, obnovo ali novo izdajanje potrdila. Primeri, ki zahtevajo preklic digitalnega potrdila so:

- odpoved naročnikove strojne ali programske opreme ter s tem izguba privatnega ključa,
- pozabljeno geslo, ki varuje privatni ključ in
- sum zlorabe privatnega ključa.

6.2 Overitelji

6.2.1 Obnovitev potrdil

Pri izdajanju digitalnega potrdila overitelj potrdilu dodeli datum poteka veljavnosti. Poznamo dva glavna razloga za časovni okvir veljavnosti.

Obnovitev poteklega potrdila omogoča overitelju, da ponovno preveri identiteto in primernost osebe oziroma subjekta. S tem postopkom overitelj avtomatično počisti seznam potrdil (ukinjeni subjekti, oseba zamenja službo, preminule osebe...).

Če ima napadalec na razpolago dovolj kriptiranih sporočil, dovolj časa ali dovolj procesorskih zmogljivosti, lahko ogrozi varnost privatnega ključa. Obnovitev potrdila omogoča predvideno in planirano varnostno zamenjavo asimetričnih ključev.

Časovni okvir veljavnosti potrdila je določen v overiteljski politiki. Pri določanju dolžine časovnega okvirja je potrebno premisliti naslednje parametre:

- Dolžina ključev (daljši ključi otežijo kriptoanalizo)
- Varnost kriptirnega algoritma
- Namen uporabe (potrdila za kritične aplikacije naj bi imela krajšo veljavno dobo)

Obnovitev potrdila je postopek, kjer overitelj izda novo potrdilo, ki nadomesti poteklega. Obnovitev potrdila lahko opcijsko vključuje tudi zamenjavo ključev, če to zaheva varnostna politika overitelja. Vsak overitelj ima svoj postopek obnovitve potrdila, objavljen na spletnih straneh.

6.2.2 Distribucija novih digitalnih potrdil

6.2.2.1 Distribucija novih uporabniških potrdil

Postopki distribucije obnovljenih potrdil se razlikujejo glede na izvor potrdil in glede na to ali so se pri obnovi zamenjali tudi asimetrični ključi.

Obnovitev uporabniških potrdil brez zamenjave ključev se lahko izvede še pred njihovim potekom veljavnosti s pomočjo podpisanega elektronskega sporočila ali preko varne TCP/IP povezave. Podpis ali vzpostavitev SSL povezave sta mogoča, ker je staro potrdilo še vedno veljavno. Če staro potrdilo poteče ali je razveljavljeno, mora naročnik ponoviti začetni postopek pridobitve potrdila.

Pri obnovitvi uporabniških potrdil z zamenjavo ključev mora biti poskrbljeno za avtentikacijo novega javnega ključa. To lahko uporabnik zagotovi z dokazom o lastništvu starega privatnega ključa (ang. Proof of Posession) ali pa s ponovnim osebnim obiskom v prijavni službi (RA), kjer potrdi svojo identiteto.

Overitelj ima vedno možnost ponovitve začetnega postopka, torej istega postopka, ko je naročnik pri overitelju prvič zahteval potrdilo. Avtomatična obnovitev potrdila je mogoča pred iztekom veljavnosti ali razveljavitve starega potrdila. Nov javni ključ naročnik namreč podpiše s še veljavnim starim ključem, overitelj pa mu nato izda novo potrdilo.

6.2.2.2 Distribucija novih overiteljskih potrdil (Root CA)

Pri obnovitvi overiteljevega potrdila in ključev je potreben poseben postopek, kjer overitelj za neko časavno obdobje objavi 3 svoja potrdila, ki jih tudi sam podpiše:

- nov overiteljev javni ključ podpisan s starim overiteljevim privatnim ključem,
- star overiteljev javni ključ podpisan z novim overiteljevim privatnim ključem,
- nov overiteljev javni ključ podpisan z novim overiteljevim privatnim ključem.

Ko ima overitelj ta potrdila javno objavljena, ni več potrebe po shranjevanju starega privatnega ključa. Drugi običajen postopek je, da overitelj vključi rezultat zgoščevalne funkcije naslednjega overiteljevega javnega ključa v trenutno overiteljevo potrdilo. Rezultat zgoščevalne funkcije se kasneje uporabi za avtentikacijo novega overiteljevega javnega ključa.

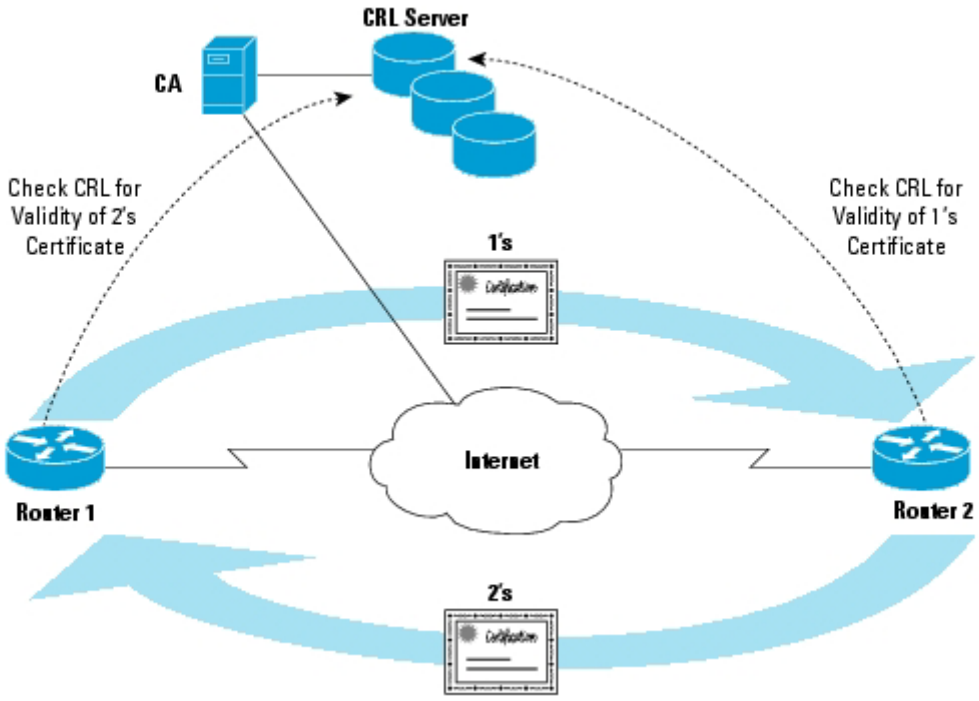
6.2.3 Obveščanje o neveljavnih potrdilih (Certificate Revocation List - CRL)

Register preklicanih potrdil vsebuje seznam potrdil, ki so bili preklicani s strani izdajatelja pred pretekom roka veljavnosti.

Če pride do zlorabe, če naročnik pozabi geslo za uporabo svojega zasebnega ključa ali pa se je pokvarila naprava, kjer je ključ hranil, je potrebno ustvariti nov par ključev in dobiti novo digitalno potrdilo, staro pa preklicati. Vsa digitalna potrdila, ki so iz različnih razlogov neveljavna, objavljajo overitelji na posebnih seznamih, ki jih tudi digitalno podpišejo.Za te sezname se je uveljavila kratica CRL (Certificate Revocation List). Seznami se objavljajo na spletnih strežnikih overiteljev ali pa v imenikih po standardu X.500, kjer so dostopni prek protokola LDAPv3. Preverjanje CRL mora biti omogočeno neprekinjeno. Da bi bilo dostopanje do CRL čim hitrejše, se je uveljavilo več načinov: ko število preklicanih potrdil preseže neko mejo, se CRL razdelijo na več vstopnih točk v direktoriju; dodatno se objavljajo samo nova preklicana potrdila od nekega časa dalje (delta CRL). V CRL je najavljeno, kdaj bo najkasneje objavljen nov CRL (čez nekaj ur, en dan, en teden, ...). Aplikacija, ki uporablja digitalna potrdila nekega overitelja, mora znati vključiti zadnji veljavni CRL overitelja v

ustreznih obdobjih. Overitelj lahko izda nov CRL pred najavljenim časom, zato morajo aplikacije preverjati veljavnost upoštevanega CRL pogosteje, kot bi sklepali iz objavljenega časa v CRL.

Zaradi problema določanja časa za vključitev CRL in ker so spletne povezave vedno hitrejše, se razvija sistem sprotnega preverjanja veljavnosti digitalnega potrdila: delovna skupina PKIX pri IETF pripravlja OCSP (Online Certificate Status Protocol). Do zdaj je bil izdan RFC 2560. Aplikacija pošlje zahtevo za preverjanje statusa potrdila direktno "pooblaščenemu" strežniku, ki mu pravijo "Certificate Status Responder", in ustavi vse transakcije, dokler ne dobi odgovora. Protokol OCSP že uporabljajo banke, ki so vključene v sistem Identrus.

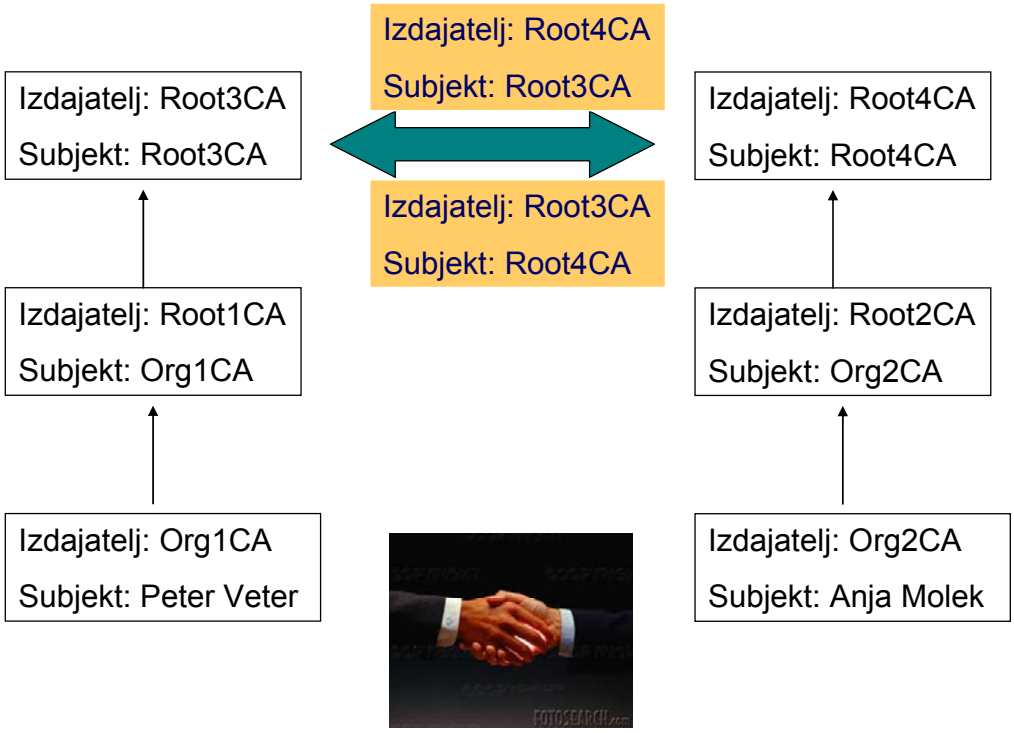


Slika 15: Register preklicanih potrdil

7 Povezovanje različnih PKI

7.1 Križno potrjevanje

Križno potrjevanje povečuje področje zaupanja z dodajanjem področja dodatnega overitelja, ki sicer ni v uporabnikovem seznamu zaupanja, mu pa zaupa uporabnikov overitelj. Zaupanje se ustvari z medsebojno izmenjavo potrdil s prej dogovorjeno overiteljsko politiko.



Slika 16: Križno potrjevanje

Za primer vzemimo dve podjetji, ki imata vsak svojega overitelja. Podjetji se dogovorita, da bosta uporabljala in potrjevala potrdila, ki jih je izdal partnerjev overitelj. Overitelja si drug drugemu izdata digitalno potrdilo, s čimer lahko jamčita avtentikacijo tudi drugih izdanih potrdil nasprotnega overitelja.

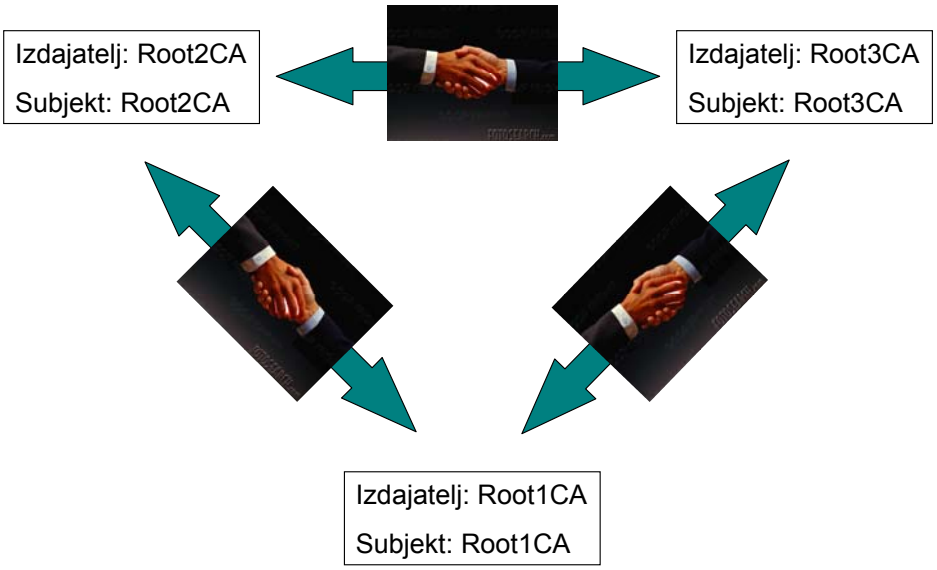
Pojem križnega potrjevanja je razdeljen na dva postopka. Prvi je vzpostavitev medebojnega zaupanja z medsebojno podelitvijo potrdil. Drugi pa je pogosto preverjanje veljavnosti posameznih navadnih in križnih potrdil v celotni verigi zaupanja. Prav tako kot navadna potrdila imajo tudi križna potrdila rok veljavnosti in možnost preklica.

7.2 Načini vzpostavljanja medsebojnega zaupanja različnih PKI

Poznamo dva načina povečevanja področja zaupanja z združevanjem različnih PKI:

7.2.1 Peer-to-peer zaupanje

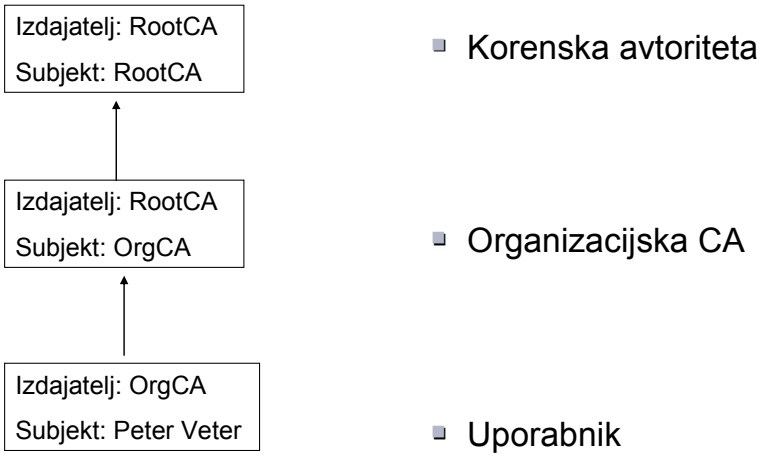
Peer-to-peer zaupanje je vzpostavljeno med dvema ali večimi overitelji z varno izmenjavo javnih ključev oziroma križnim potrjevanjem, kjer se ključi uporabijo za preverjanje identitete elektronskega podpisa na dostavljenih potrdilih. Vsak overitelj izda drugemu overitelju potrdilo, s čimer doseže, da lahko njegovi uporabniki po novem zaupajo tudi drugemu overitelju.



Slika 17: Trije overitelji križno potrjeni

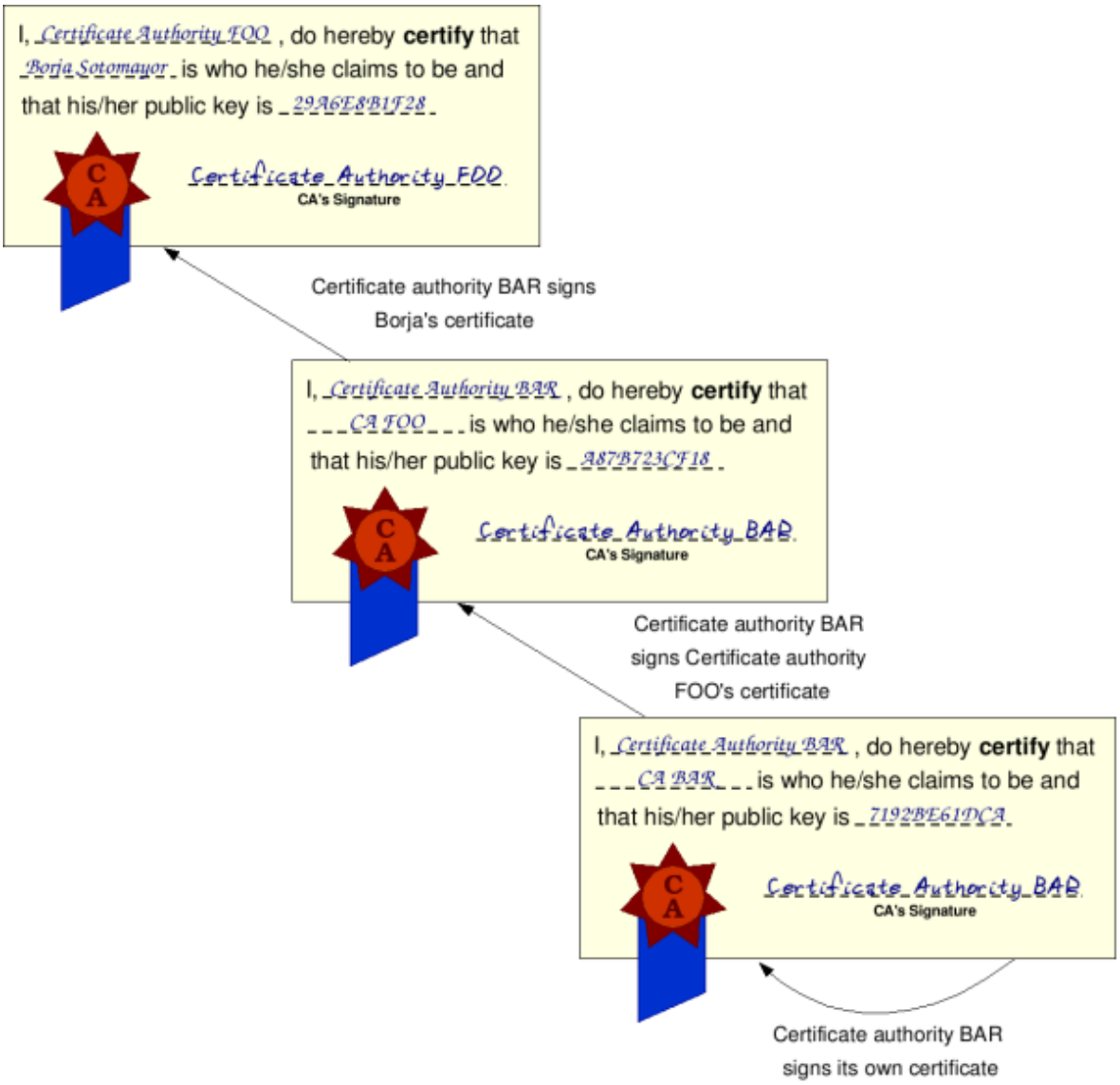
7.2.2 Hierarhično zaupanje

Hierarhično zaupanje je doseženo z vzpostavitvijo verige zaupanja med overitelji. V verigi zaupanja so overitelji hierarhično razporejeni po pomembnosti oziroma stopnji zaupanja. Na vrhu verige je t.i. korenska avtoriteta (root CA) oziroma overitelj, ki mu eksplicitno zaupa celotna veriga. Avtentičnost overiteljev se potrjuje od ciljnega overitelja navzgor, dokler se ne avtenticira zadnji člen verige zaupanja (korenski overitelj). Ker se na ta način lahko avtenticira vsak člen verige, privzamemo, da si lahko overitelji medsebojno zaupajo.



Slika 18: Hierarhično zaupanje

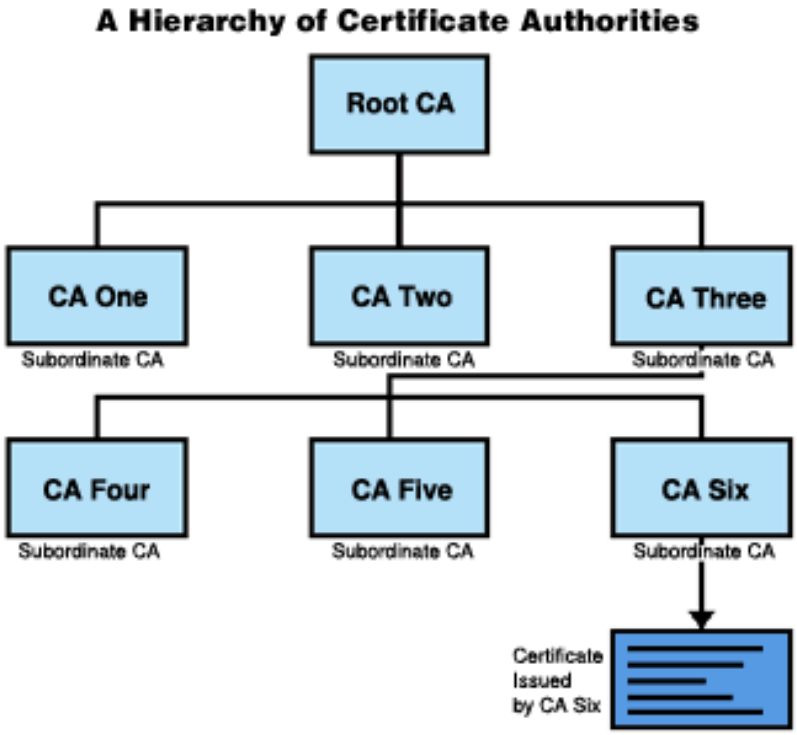
Spodnji primer nazorno ilustrira postopno verižno avtentikacijo posameznih overiteljev oziroma potrdil. Vsak overitelj v verigi zaupanja potrebuje potrditev višje ležečega overitelja, le korenski overitelj, ki mu eksplicitno zaupajo vsi člani verige, potrdi samega sebe s t.i. samo-podpisom svojega potrdila (self-signed certificate).



Slika 19: Ilustracija poteka križnega potrjevanja

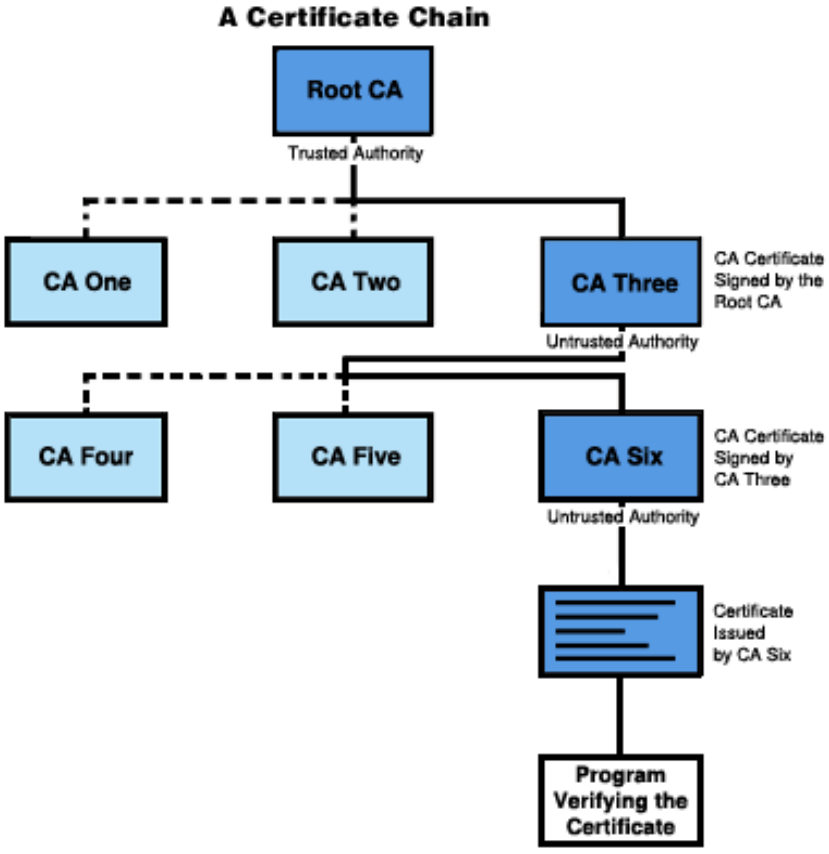
Veliko aplikacij, ki pošilja uporabniško digitalno potrdilo ciljnemu prejemniku, pošlje poleg uporabniškega potrdila tudi vsa druga potrdila, ki so potrebna za potrditev zahtevanega potrdila po verigi zaupanja vse do korenskega overitelja.

V primeru potreb po večjem številu različnih overiteljskih politik oziroma geografski razpršenosti uporabnikov, se uporablja drevesno strukturo povezovanja overiteljev, kot prikazuje spodnja slika.

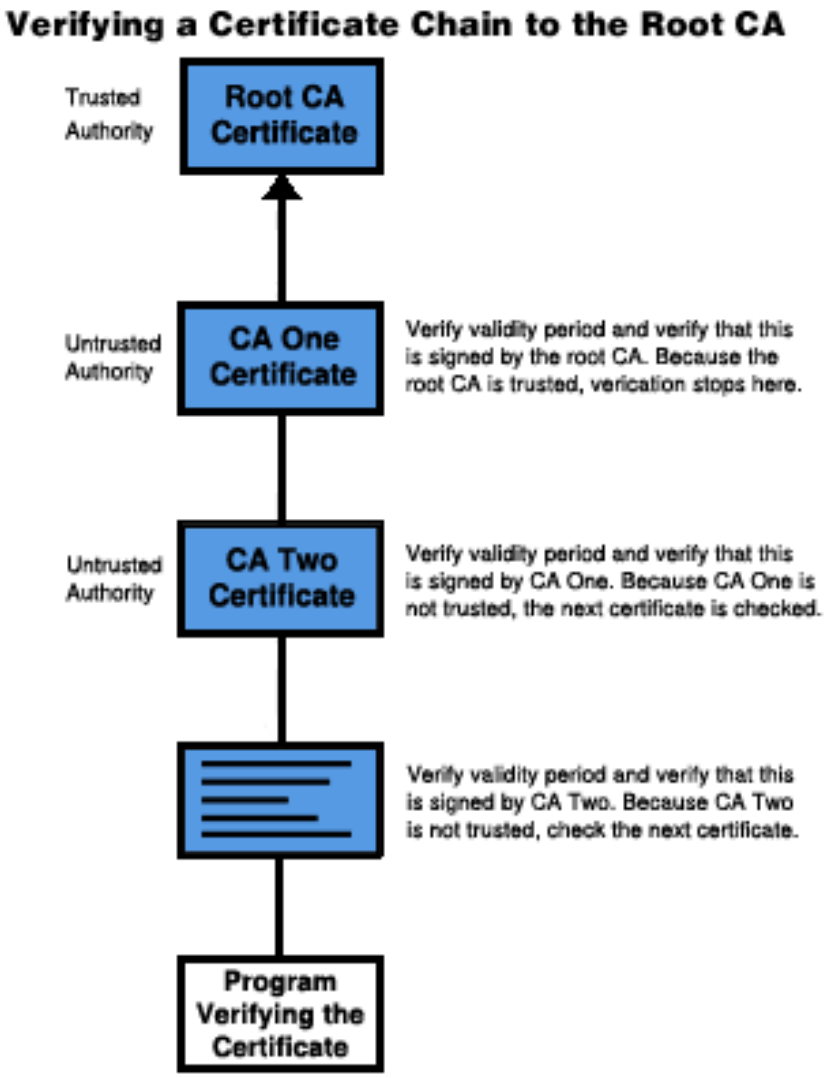


Slika 20: Hierarhična drevesna struktura overiteljev

Drevesna struktura overiteljev je sestavljena iz več različnih verig zaupanja, ki se stekajo k korenskemu overitelju.



Slika 21: Posamezna veriga v drevesni strukturi overiteljev



Slika 22: Potek preverjanja potrdila po hierarhični verigi zaupanja

Predstavljen postopek preveri potrdilo ciljnega overitelja pri tem pa uporabi celotno verigo overiteljev, dokler ne pride do overitelja, ki mu uporabnik zaupa.

1. Uporabnik locira potrdilo overitelja 1.
2. Uporabnik preveri potrdilo overitelja 1 pri overitelju 2, ki je to potrdilo izdal.
3. Če uporabnik zaupa overitelju 2, se postopek konča. V drugem primeru pa preverja potrdila naslednjih overiteljev vse do korenskega overitelja.

8 Uporaba overiteljev v podjetjih

Pri organizaciji in uvajanju digitalnih potrdil v poslovanje podjetja imajo organizacije na voljo dve možnosti. Lahko se odločijo in same izdajajo kvalificirana potrdila, kar pomeni da znotraj podjetja oblikujejo agencijo za certificiranje ter s tem postanejo enakovredne ostalim CA (horizontalna mreža overiteljev). Druga možnost, ki jo imajo podjetja na voljo je, da storitve delegirajo komercialnim overiteljem in postanejo del vertikalne mreže overiteljev (angl. outsourcing).

Pri vertikalni mreži overiteljev se podjetje izogne visokim začetnim stroškom in organizaciji, ki je potrebna, da so digitalna potrdila kvalificirana, če sklene pogodbo z overiteljem, ki potem v imenu naročnika s svojo informacijsko tehnologijo omogoča naročniku, da izdaja, upravlja in preklicuje certifikate. Zakon o elektronskem poslovanju in elektronskem podpisu, ki je bil v Sloveniji sprejet junija 2000 namreč zahteva visoko stopnjo zaščite prostora overitelja, ki lahko takšna kvalificirana izdaja. Posamezna podjetja, kot so npr. banke so potem prijavne službe, odgovorna za registracijo in preverjanje identitete končnih uporabnikov ter personalizacijo digitalnih potrdil. S tem postanejo podrejeni overitelji.

9 Digitalna potrdila v Sloveniji

9.1 Uporaba digitalnih potrdil v Sloveniji

Uporaba digitalnih potrdil za strežnike za to, da se omogoči zašifrirana povezava z brskalnikom po protokolu SSL, je uveljavljena pri praktično vseh, ki se ukvarjajo s prodajo po internetu. S tem dosežemo to, da podatkov, ki jih je vtipkal uporabnik, ne more kdo prestreči, ker je povezava zašifrirana, poleg tega pa uporabnik lahko preveri digitalno potrdilo strežnika in iz tega sklepa, ali se je priključil na pravi strežnik.

Uporabo potrdil v brskalnikih za overjanje svojih komitentov sta prvi začeli uporabljati NLB (1999) v aplikaciji Klik in SKB v aplikaciji SKBNet. Vsaka banka ima svojo službo za izdajanje digitalnih potrdil in tako potrdilo je uporabno samo za dostop do bančnih aplikacij ustrezne banke. Je pa možno nekatera potrdila, ki so jih izdale banke, uporabljati za dostop do aplikacij državne uprave (n.pr. potrdilo NLB za oddajo dohodnine). Zanimiva je letošnja odločitev Abanke (2006), da preneha izdajati svoja potrdila za Abanet, omogoči pa uporabo potrdil Posta®ca, v bodoče pa tudi potrdil SIGEN-CA in HALCOM-CA.

Tudi slovenska vlada uresničuje načrt o e-poslovanju javne uprave. V okviru tega nastaja PKI za javno upravo, saj je bil leta 2001 ustanovljen overitelj digitalnih potrdil na Centru Vlade za informatiko. Po reorganizaciji leta 2004 je naloge Centra Vlade za informatiko prevzelo na novo ustanovljeno Ministrstvo za javno upravo, v okviru katerega zdaj deluje overitelj digitalnih potrdil:

SIGOV-CA, ki deluje od 17.januarja 2001, izdaja kvalificirana digitalna potrdila za institucije javne uprave,
SIGEN-CA, ki deluje od 9.julija 2001, izdaja kvalificirana digitalna potrdila za državljane ter za pravne in fizične osebe, registrirane za opravljanje dejavnosti.
Z uporabo digitalnih potrdil se da urediti že kar nekaj stvari prek interneta - seznam je na spletni strani e-uprave.

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati bodoči imetnik. Izpolnjen zahtevek se odda na prijavno službo (seznam je objavljen na spletni strani http://www.sigen-ca.si/prijavne-slu.htm).

SIGEN-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega bodočega imetnika kvalificiranega digitalnega potrdila in ju bodoči imetnik potrebuje za prevzem svojega potrdila, ki ga opravi na svoji delovni postaji v skladu z navodili izdajatelja SIGEN-CA. Bodoči imetnik prejme referenčno številko po elektronski pošti, avtorizacijsko kodo pa po priporočeni pošti na svoj stalni ali drug izbran naslov.
Spletno kvalificirano digitalno potrdilo je povezano z enim parom ključev, ki se tvori z imetnikovo programsko ali strojno opremo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa. Javni ključ se pošlje izdajatelju SIGEN-CA, ki izda potrdilo, katerega sestavni del je javni ključ. Spletno potrdilo se shrani pri imetniku, dostopno pa je tudi v javnem imeniku potrdil.
SIGEN-CA poleg podatkov, ki so vključeni v digitalno potrdilo, hrani ostale potrebne podatke o imetniku za namen elektronskega poslovanja v skladu z veljavnimi predpisi.
Imetnik mora skrbno varovati zasebne ključe in svoje kvalificirano digitalno potrdilo ter ravnati v skladu s politiko, obvestili izdajatelja SIGEN-CA in veljavno zakonodajo.

9.2 Slovenski overitelji, ki delujejo v skladu z zakonskimi zahtevami

Overitelji so fizične ali pravne osebe, ki izdajajo potrdila (v elektronski obliki, ki povezujejo podatke za preverjanje elektronskega podpisa z določeno osebo, imetnikom potrdila, ter potrjujejo njeno identiteto) ali opravljajo druge storitve v zvezi z overjanjem ali elektronskimi podpisi, saj je varen elektronski podpis, ki je overjen s kvalificiranim potrdilom, glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima enako veljavnost in dokazno vrednost.

Za opravljanje svoje dejavnosti overitelj ne potrebuje posebnega dovoljenja. Mora pa najmanj 8 dni pred pričetkom opravljanja svoje dejavnosti le-to prijaviti ministrstvu, pristojnemu za informacijsko družbo (v nadaljevanju: ministrstvo).

Določeni overitelji, ki delujejo v skladu z zakonskimi zahtevami, izdajajo t. i. kvalificirana potrdila, ki izpolnjujejo predpisane zahteve, kot npr.: navedba, da gre za kvalificirano potrdilo; ime ali firma in država stalnega prebivališča ali sedeža overitelja; ime oziroma psevdonim imetnika potrdila ali naziv oziroma psevdonim informacijskega sistema z navedbo imetnika potrdila, pod katerega nadzorom je, z obvezno navedbo, da gre za psevdonim; dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo; podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila; začetek in konec veljavnosti potrdila; identifikacijska oznaka potrdila; varen elektronski podpis overitelja, ki je potrdilo izdal; morebitne omejitve v zvezi z uporabo potrdila; morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja.

Overitelji, ki dokažejo, da izpolnjujejo vse z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi predpisane pogoje za svoje delovanje, lahko zahtevajo, da jih akreditacijski organ (Agencija za telekomunikacije) vpiše v register akreditiranih overiteljev.

Spodaj so navedeni pogoji, ki jih mora izpolnjevati kvalificiran slovenski overitelj.

1. ZAKONODAJA

- Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00, 30/01 – ZODPM-C, 25/04, 98/04 – uradno prečiščeno besedilo (ZEPEP-UPB1))
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01)
- Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Slovenije (Uradni list RS, št. 99/01)

2. POGOJI

- Prostor in oprema
  - Overiteljevi prostori in infrastruktura morajo biti v skladu s pravili stroke ustrezno elektronsko in fizično varovani pred nepooblaščenimi vdori.
  - Zagotovljena mora biti uporaba zanesljivih sistemov in opreme, ki so zaščiteni pred spreminjanjem in ki zagotavljajo tehnično in kriptografsko varnost postopkov, v katerih se uporabljajo.
  - Informacijsko telekomunikacijska infrastruktura, ki je povezana v drugo informacijsko telekomunikacijsko omrežje, mora biti varovana z zanesljivimi varnostnimi mehanizmi (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada in podobno), ki preprečujejo nedovoljene dostope prek tega omrežja in omejujejo dostop samo po protokolih, ki so nujno potrebni za upravljanje s kvalificiranimi potrdili, vsi drugi protokoli pa morajo biti onemogočeni
  - Programska oprema mora ustrezati svetovno uveljavljenim varnostnim in tehničnim standardom (FIPS 140-1 za kriptografske module, priporočljivo EAL5 oziroma najmanj EAL3 Skupnih meril - Common Criteria /ISO 15408/, priporočila izvedenske skupine Evropske iniciative za standardizacijo elektronskih podpisov - EESSI in drugo).
  - Programska oprema, ki generira podatke za elektronsko podpisovanje, mora zagotavljati najmanjšo možnost poneverbe teh podatkov z uporabo trenutno razpoložljivih tehnologij.
  - Šteje se, da strojna in programska oprema ter postopki izpolnjujejo predpisana merila in pogoje, če so v skladu s standardi, merili ali pogoji, ki so splošno priznani v Evropski uniji in objavljeni v Uradnem listu Evropskih skupnosti.
  - Informacijski sistem overitelja za upravljanje kvalificiranih potrdil mora biti sestavljen zgolj iz strojne in programske opreme, ki je potrebna za upravljanje kvalificiranih potrdil.
- Usposobljenost
  - Zaposlene najmanj 3 osebe z univerzitetno izobrazbo, od tega najmanj 2 osebi z univerzitetno diplomo tehnične oziroma naravoslovne smeri, najmanj 2 osebi pa morata imeti tudi 2 leti delovnih izkušenj s področja delovanja overiteljev ali sorodnega področja.
  - Zaposlen univerzitetni diplomirani pravnik z opravljenim pravniškim državnim izpitom (lahko tudi na podlagi sklenjene ustrezne svetovalne pogodbe).
  - Vse prej naveden osebe morajo imeti posebna strokovna znanja glede upravljanja in poznavanja tehnologije, varnostnih postopkov in pravnih zahtev s področja elektronskega poslovanja in delovanja overiteljev, pridobljena na strokovnih usposabljanjih.

- Zaposleni v prijavni službi morajo biti usposobljeni za zanesljivo ugotavljanje istovetnosti oseb.
- Overitelj, ki izdaja kvalificirana potrdila – zaposleno osebje s potrebnim strokovnim znanjem, izkušnjami in usposobljenostjo na področju opravljanih storitev, zlasti na področju upravljanja ter poznavanja tehnologije elektronskega poslovanja in ustreznih varnostnih postopkov.
- Osebje se mora ravnati po administrativnih in upravljavskih postopkih, skladnih z uveljavljenimi pravili stroke.
- Zaposleni ne smejo poleg svojega dela opravljati enakih oziroma podobnih del, kot jih opravljajo na svojem delovnem mestu, pri drugih overiteljih, če to niso podrejeni overitelji, ali opravljati del, ki niso združljiva z njihovimi delovnimi zadolžitvami in odgovornostmi pri overitelju. Izjema je opravljanje samostojnega znanstvenega in pedagoškega dela, delo v kulturnih, umetniških, športnih, humanitarnih in drugih podobnih društvih in organizacijah ter delo na publicističnem področju.

- Ostalo
  - Zagotovljeno mora biti ustrezno fizično varovanje strojne opreme overitelja in nadzor fizičnega dostopa do lastnega informacijskega sistema za upravljanje kvalificiranih potrdil.
  - Ob začetku opravljanja dejavnosti ali ob njeni spremembi mora overitelj seznaniti ministrstvo s svojimi notranjimi pravili glede elektronskega podpisovanja in overjanja ter s svojimi postopki in infrastrukturo.
  - Notranja pravila overiteljev, ki izdajajo kvalificirana potrdila, morajo vsebovati javni in zaupni del. Bistvene določbe notranjih pravil, ki vplivajo na odnos med overiteljem in imetniki od njega izdanih kvalificiranih potrdil ter tretjimi osebami, ki se zanašajo na ta potrdila, morajo biti vsebovane v javnem delu notranjih pravil. Le-ta mora biti javno dostopen v elektronski obliki na internetu in na trajnem nosilcu podatkov v elektronski ali klasični obliki (glede minimalne vsebine notranjih pravil glej Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje).
  - Overiteljev informacijski sistem za upravljanje kvalificiranih potrdil mora imeti vgrajene zadostne varnostne mehanizme, ki preprečujejo zlorabo s strani zaposlenih in omogočajo jasno ločitev nalog na predpisana področja (t. j. področje upravljanja s kvalificiranimi potrdili, področje upravljanja z informacijskim sistemom overitelja in področje varovanja in kontrole).
  - Overitelj mora zagotoviti zaupnost in enkratnost uporabe podatkov za generiranje kvalificiranega potrdila.
  - Overitelj, ki izdaja kvalificirana potrdila, mora zavarovati svojo škodno odgovornost. Najnižji znesek zavarovalne vsote, za katero overitelj, ki izdaja kvalificirana potrdila, zavaruje svojo škodno odgovornost, je 50 milijonov SIT.
  - Dokler zavarovalnice na trgu Republike Slovenije ne ponudijo možnosti sklenitve tovrstnega zavarovanja, se šteje, da overitelj, ki izdaja kvalificirana potrdila, izpolnjuje predpisani pogoj, če:
    - pridobi drug ustrezen finančni instrument (npr. bančno garancijo), s katerim se finančna institucija zaveže, da bo v primeru škodnega dogodka oškodovancu v imenu overitelja izplačala odškodnino v višini, ki ne sme biti manjša od prej navedenega predpisanega zneska, ali

- ◊ vrednost obveznosti prostega premoženja overitelja ali pravne osebe, ki solidarno jamči za overiteljevo odgovornost, znaša najmanj trikratnik prej navedenega predpisanega zneska.

3. VLOGA

- V elektronski ali papirnati obliki na predpisanem obrazcu "Podatki o overitelju" (Priloga 1).
  - ◊ Vloga mora vsebovati podatke o overitelju oziroma osebi, ki opravlja naloge overitelja ter za vsako prijavljeno storitev naslednje podatke: naziv in vrsta storitve, vrsta potrdil in elektronskega podpisa oziroma časovnega žiga.
- Če bo overitelj izdajal kvalificirana potrdila, mora vloga vsebovati tudi podatke o številu, izobrazbi in usposobljenosti overiteljevih zaposlenih.
- Vloga tujega overitelja za vpis v register mora vsebovati še podatke o izpolnjevanju pogojev glede veljavnosti njegovih potrdil v Republiki Sloveniji. Vloga mora biti v slovenskem jeziku. Overitelj lahko določena podatke (glej 3. člen pravilnika) navede tudi v angleškem jeziku.

4. OBVEZNE PRILOGE K VLOGI

- Za vsako prijavljeno storitev:
  - ◊ javni del notranjih pravil in druga pomembna dokumentacija glede storitve,
  - ◊ podatki o imeniku potrdil in registru preklicanih potrdil, če obstajata,
  - ◊ podatki o tehnoloških značilnostih potrdila ali časovnega žiga,
  - ◊ podatki o tehnoloških značilnostih ter načinu in pogostnosti osveževanja imenika in registra preklicanih potrdil, če obstajata,
  - ◊ podatki o službi za preklic ali drugi dežurni službi overitelja,
  - ◊ podatki o prijavnih službah overitelja,
  - ◊ seznam podatkov, ki so vsebovani v potrdilu ali časovnem žigu,
  - ◊ podatki o namenu ali omejitvi uporabe potrdil ali storitve,
  - ◊ podatki o postopku in načinu preverjanja identitete imetnikov potrdil,
  - ◊ rok veljavnosti izdanih potrdil,
  - ◊ opis overiteljeve infrastrukture in postopkov s pripadajočo tehnično dokumentacijo, ki mora omogočati ocenitev skladnosti z zahtevami veljavnih predpisov za vsako prijavljeno storitev,
  - ◊ začetek opravljanja storitve,
  - ◊ konec opravljanja storitve,
  - ◊ drugi pomembni podatki glede prijavljene storitve.
- Če bo overitelj izdajal kvalificirana potrdila - dokazilo o sklenjenem obveznem zavarovanju za overiteljeve zaposlene.
- Priložena dokumentacija k vlogi tujega overitelja za vpis v register je lahko v slovenskem ali angleškem jeziku, po predhodnem soglasju direktorja direkcije pa je lahko tudi v drugem jeziku.

5. OSTALA DOKAZILA

6. UPRAVNA TAKSA IN STROŠKI

- Upravna taksa v znesku 4.250 SIT (250 točk, po tar. št. 1 in 3 Zakona o upravnih taksah)

7. PRISTOJNI ORGAN ZA IZDAJO ODLOČBE

- Ministrstvo za informacijsko družbo

8. OSTALO

- Minister v osmih dneh od vložitve popolne vloge z odločbo odloči o vpisu overitelja v register.
- Overitelj mora kakršnokoli spremembo podatkov v vlogi ali v priloženi dokumentaciji takoj prijaviti ministrstvu v elektronski obliki na predpisanem obrazcu "Prijava predloga spremembe vpisa v registru" (Priloga 2).
- Če overitelj preneha z delovanjem ali je njegovo delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj ter če overitelj ne prekliče svojega potrdila, mora ministrstvo takoj zagotoviti preklic potrdil overitelja.
- Ministrstvo vodi elektronski javni register vseh overiteljev v Republiki Sloveniji. Na njihovo zahtevo se vanj vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Republiki Sloveniji. Register overiteljev varno elektronsko podpiše ministrstvo, nakar se kvalificirano potrdilo ministrstva objavi v Uradnem listu Republike Slovenije.
- Tudi v register akreditiranih overiteljev se na njihovo zahtevo vpišejo tuji overitelji, če izpolnjujejo predpisane pogoje za veljavnost njihovih potrdil v Republiki Sloveniji.
- Javni elektronski register prostovoljno akreditiranih overiteljev vodi akreditacijski organ (dokler Agencija za telekomunikacije ne prevzame predpisanih nalog, opravlja naloge iz njene pristojnosti Center vlade za informatiko).
- Register akreditiranih overiteljev varno elektronsko podpiše akreditacijski organ, nakar se kvalificirano potrdilo akreditacijskega organa objavi v Uradnem listu Republike Slovenije.
- Akreditacijski organ lahko priporoči spremembo notranjih pravil akreditiranega overitelja oziroma prenehanje nadaljnje uporabe neprimernih postopkov in infrastrukture. Če overitelj teh priporočil ne upošteva, ga akreditacijski organ z odločbo izbriše iz registra akreditiranih overiteljev.
- Kvalificirana potrdila overitelja s sedežem v Evropski uniji so enakovredna domačim kvalificiranim potrdilom.
- Kvalificirana potrdila overiteljev s sedežem v tretjih državah so enakovredna domačim, če:
  - ◊ overitelj izpolnjuje predpisane pogoje in je prostovoljno akreditiran v Republiki Sloveniji ali eni izmed držav članic Evropske unije;
  - ◊ domači overitelj, ki izpolnjuje predpisane pogoje, jamči za taka potrdila enako, kot bi bila njegova;
  - ◊ tako določa dvostranski ali večstranski sporazum med Republiko Slovenijo in drugimi državami ali mednarodnimi organizacijami;
  - ◊ tako določa dvostranski ali večstranski sporazum med Evropsko unijo in tretjimi državami ali mednarodnimi organizacijami.

10 Viri

[1] RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), IETF, September 2005
http://www.ietf.org/rfc/rfc4210.txt

[2] RFC 3647, Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework, IETF, November 2003
http://www.ietf.org/rfc/rfc3647.txt

[3] http://www.ibm.com

[4] http://www.pki-page.info

[5] http://www.entrust.com

[6] http://www.si-ca.si/

[7] http://www.opengroup.org

[8] http://mid.gov.si

[9] http://en.wikipedia.org

[10] http://www.halcom-ca.si/

[11] http://msdn.microsoft.com