CENTER VLADE REPUBLIKE SLOVENIJE
ZA INFORMATIKO

VARNOSTNI VIDIKI APLIKACIJ Z UPORABO DIGITALNIH POTRDIL SIGEN-CA IN SIGOV-CA

PRIPOROČILA ZA APLIKACIJE

Verzija: 1.0

1. avgust 2003

STANJE DOKUMENTA

Namen dokumenta:	Uporabnikom digitalnih potrdil SIGEN-CA in SIGOV-CA
Kratek naziv projekta:	Varnostni vidiki aplikacij z uporabo digitalnih potrdil SIGEN-CA in SIGOV-CA
Vsebina:	Glej "Vsebina"
Status:	Končna
Verzija:	1.0
Datum verzije:	1. avgust 2003
Avtor:	Overitelj na Centru Vlade RS za informatiko
Kontaktni podatki:	Naslov: Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija Tel.: (+386) 01 4788 600 Fax.: (+386) 01 4788 649 Url.: http://www.gov.si/ca E-pošta: sigen-ca@gov.si, sigov-ca@gov.si

VSEBINA

1. UVOD

Pričujoči dokument povzema evropska priporočila za izvedbo aplikacij e-storitev, ki zahtevajo najvišji nivo varnosti, ki ga lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil. Priporočila temeljijo na uporabi kvalificiranih digitalnih potrdilih Overitelja na Centru Vlade RS za informatiko, katerega delovanje določa Politika delovanja Overitelja na CVI. Dokument predstavlja del Priporočil za aplikacije e-storitev z varnostnimi zahtevami z uporabo kvalificiranih digitalnih potrdil:
Varnostni vidiki aplikacij z uporabo digitalnih potrdil izdajateljev SIGEN-CA in SIGOV-CA.

2. OVERITELJ NA CENTRU VLADE RS ZA INFORMATIKO

Overitelj na Centru Vlade RS za informatiko (CVI) izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001), evropskimi direktivami ter drugimi veljavnimi predpisi. Politika delovanja overitelja na CVI določa namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost overitelja na CVI ter zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji.

Overitelja na CVI (http://www.gov.si/ca*)* predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGEN-CA (angl. *Slovenian General Certification Authority*) za državljane in pravne osebe (http://www.sigen-ca.si),
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) za upravo Republike Slovenije (http://www.sigov-ca.gov.si).

Oba izdajatelja sta mednarodno registrirana, medsebojno priznana ter tehnološko in zakonsko enako veljavna.

Vse o digitalnih potrdil SIGOV-CA in SIGEN-CA, njihov profili, profil registrov preklicanih potrdil so podani s politikami delovanja overitelja, zbrano pa je tudi v Priporočilih za aplikacije e-storitev z varnostnimi zahtevami z uporabo kvalificiranih digitalnih potrdil, v dokumentu *Profil kvalificiranih digitalnih potrdil in registra preklicanih potrdil izdajateljev SIGEN-CA in SIGOV-CA.*

2.1. Pravni vidik e-podpisa in kvalificiranih digitalnih potrdil

Po Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ima elektronski podpis pravno veljavo, če je overjen s t.i. kvalificiranim digitalnim potrdilom (*člen 15: "Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.*"). Tak elektronski podpis oz. z njim podpisana pogodba v e-obliki je tako enakovredna lastnoročnemu podpisu na dokumentu v papirni obliki.

Varen elektronski podpis je elektronski podpis, ki izpolnjuje nekaj, v zakonu taksativno naštetih zahtev. Tako mora biti izključno povezan s podpisnikom in je tako iz njega mogoče zanesljivo ugotoviti podpisnika. Hkrati mora biti podpis tehnološko zasnovan tako, da je povezan s podatki, na katere se nanaša, in bi bila opazna vsaka sprememba teh podatkov ali povezave z njimi, ki se bi zgodila po

podpisu. Podpisnik pa mora podpis oblikovati s pomočjo sredstev za varno elektronsko podpisovanje pod svojim izključnim nadzorom. Sredstva za varno elektronsko podpisovanje se od običajnih sredstev za elektronsko podpisovanje razlikujejo v tem, da izpolnjujejo posebne pogoje glede varnosti in zanesljivosti, ki jih določa ZEPEP. Varen elektronski podpis pa mora biti overjen še s kvalificiranim potrdilom. Takšno potrdilo ima enake značilnosti kot običajno potrdilo, le da zakon zanj podrobneje predpisuje njegovo vsebino ter način izdaje, uporabe in preklica. Prav tako so z zakonom in uredbo predpisani posebni, strožji pogoji glede overiteljev, ki izdajajo takšna kvalificirana potrdila (Uradni list RS, št. 77/2000 in 2/2001).

Overitelj na CVI izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z ZEPEP in Uredbo, evropskimi direktivami ter drugimi veljavnimi predpisi.

3. POMEN VARNOSTI E-STORITEV

Pri elektronskem načinu opravljanja storitev je velik poudarek na zagotavljanju ustrezne varnosti pri dostopu do posameznih aplikacij oziroma uvedbi takšne infrastrukture, ki bo nudila zaupnost e-storitev in s tem varno elektronsko poslovanje (varni protokoli, varna infrastruktura, varnostna politika vseh vpletenih ...). Pomembno je, da storitve, ki se vršijo na elektronski način, zagotovijo enak ali celo višji nivo varnosti in zaupanja kot storitve, ki se opravljajo na klasičen način. Omogočiti je potrebno mehanizme za nedvoumno ugotavljanje identitete, zaupnost pri izmenjavi občutljivih podatkov, avtenticiran dostop do podatkovnih baz, obstajajo pa tudi številne aplikacije, ki so povezane z elektronskimi podpisi oziroma potrebujejo le-te za delovanje. Ponudnik aplikacije na elektronski način (transakcije, izpolnjevanje obrazcev,...) mora natančno proučiti vidike tveganja in na podlagi tega določiti potrebne varnostne ukrepe. Najvišji nivo varnosti lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil, ki omogočajo:

- **avtentikacijo**: zagotoviti nedvoumno identifikacijo uporabnika kot tudi strežnika oz. aplikacije, do katere uporabnik dostopa,
- **avtorizacijo** oz. nadzor nad dostopom: zagotoviti uporabniku avtoriziran dostop do podatkov/storitev in pod kakšnimi pogoji.
- **nezatajljivost:** z digitalnim podpisom s podporo za nezatajljivost zagotoviti nezmožnost zanikanja izvora podatkov ter vključenost v opravljanje storitev, preprečiti možnost ponarejanja opravljenih storitev,
- **celovitost podatkov:** z digitalnim podpisom podatkov zagotoviti celovitost izmenjanih podatkov, kar pomeni, da podatki niso bili kakorkoli spremenjeni od svojega nastanka in da o tem ciljni uporabnik ne bi bil obveščen,
- **zaupnost:** z ustreznimi postopki šifriranja zagotoviti zaupnost povezave med uporabnikom in strežnikom, prav tako pa mora biti zagotovljena zaščita podatkov, ki se ob tem izmenjajo.

3.1. Splošna varnost

V varnostne rešitve e-storitev morajo biti poleg zgoraj naštetih osnovnih vidikov, ki jih lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil, vpeti tudi ostali splošni pogoji zagotavljanja varnosti:

- zaščita sistema s požarno pregrado,
- sistem za spremljanje vdorov,
- sistem za alarmiranje,
- varnostno kopiranje dokumentov,
- protivirusna zaščita,
- zagotovitev visoke razpoložljivosti sistema,

- opozarjanje in izobraževanje uporabnikov o varnem ravnanju.

Splošne pogoje varnosti mora ponudnik storitve upoštevati v skladu s svojo interno varnostno politiko oz. v skladu z mednarodnimi standardi, npr. ISO 17799.

Razvijalci oz. ponudniki novih e-storitev morajo varnostno logiko vgraditi v vsako novo aplikacijo, kar je povezano s stroški, časom, reorganizacijo in vključitvijo v obstoječe sisteme. Vgraditev varnostnih vidikov je zahteven postopek, zato je smiselno njihovo enovito reševanje na podlagi splošno privzetih standardov in priporočil.

3.2. Koraki pri implementaciji aplikacij in razvojna orodja

Po proučitvi varnostnih zahtev in drugih splošnih vidikov varnosti, morajo razvijalci aplikacij skrbno izbrati razvojno okolje in orodja, ki omogočajo vgraditev ustreznega nivoja varnosti (z uporabo digitalnih potrdil SIGEN-CA in SIGOV-CA), pri tem pa upoštevati tudi povezljivost z obstoječimi rešitvami.

4. VARNOSTNI VIDIKI E-STORITEV Z UPORABO DIGITALNIH POTRDIL

Osnovne vidike varnosti, ki se nanašajo na nedvoumno ugotavljanje istovetnosti vseh sodelujočih v storitvi, nadzor nad dostopom, zaupnost, celovitost, podporo za nezatajljivost, zagotovimo s tehnologijo kvalificiranih digitalnih potrdil. Vse te varnostne funkcije so v nadaljevanju podane nanašajoč se na infrastrukturo kvalificiranih digitalnih potrdil Overitelja na CVI. Vrste digitalnih potrdil, njihov profil, profil registra preklicanih potrdil so podani s politikami delovanja overitelja, zbrane pa so tudi v Priporočilih za aplikacije e-storitev z varnostnimi zahtevami z uporabo kvalificiranih digitalnih potrdil, v dokumentu *Profil kvalificiranih digitalnih potrdil in registra preklicanih potrdil izdajateljev SIGEN-CA in SIGOV-CA.*

Uporabniki digitalnih potrdil Overitelja na CVI morajo upoštevati tehnična in ostala določila Overitelja (politike delovanja Overitelja na CVI, http://www.gov.si/ca).

4.1. Splošna priporočila

4.1.1 Funkcionalnost

1. Aplikacije oz. lastniki aplikacije morajo v skladu z zahtevami poslovnega vidika in tveganj opravljanja storitev na elektronski način upoštevati oz. vgraditi naslednje mehanizme:
   - celovitost opravljanja storitve v celotnem življenjskem ciklu storitve oz. dokumentov, ki pri tem nastanejo,
   - digitalni podpis, kjer je to potrebno, in tudi njegovo verodostojno verifikacijo,
   - zaupnost oz. šifriranje občutljivih podatkov pri izmenjavi oz. hrambi,
   - celovit in nezatajljiv postopek opravljanja avtentikacije, avtorizacije in ostalih akcij v zvezi s storitvijo,
   - beleženje vseh dogodkov in varno hranjenje podatkov o tem,
   - zagotovitev varnega arhiva v skladu s poslovnimi zahtevami.

2. Za aplikacijo mora biti jasno določena uporaba in medsebojna razmerja med vključenimi strankami. Lastnik aplikacije le-ta določi z varnostno politiko e-podpisa (angl. *Signature Policy*). Več o tem v poglavju 5 in prilogi A.

3. Aplikacija mora glede na pogoje pridobitve digitalnih potrdil in ostale lastnosti v zvezi z posameznimi vrstami digitalnih potrdil (npr. čas veljavnosti, podpora za 2 para ključev,...) določiti pogoje uporabe aplikacije, t.j. vrsto digitalnih potrdil.

4.1.2 Tehnična priporočila

1. Aplikacije morajo znati uporabljati digitalna potrdila shranjena v skladu z zahtevami Overitelja na CVI, t.j. na pametnih karticah oz. na disku ali v bazah brskalnikov – glej [1] pogl. 3. V zvezi s tem je potrebna interoperabilnost s standardi za dostop do ključev in digitalnih potrdil:
   - PKCS#11,
   - PKCS#12,
   - Entrust Profile,
   - MS CAPI.

2. Kadarkoli aplikacija preverja digitalno potrdilo, mora preveriti:
   - veljavnost digitalnega potrdila,
   - veljavnost podpisnega zasebnega ključa ("PrivateKeyUsagePeriod"),
   - ustrezen register preklicanih potrdil (CRL),
   - izdajatelja (izdajateljevo potrdilo),
   - uporabo potrdila, politiko overitelja, varnostno politiko e-podpisa.

3. Aplikacije morajo upoštevati objavljene profile digitalnih potrdil in CRL.

4. Aplikacija mora poskrbeti za ažuren dostop do CRL. Le-ta se izvede na podlagi reference za dostop do CRL iz potrdila ("*CRL Distribution Points*") ali drugače objavljenih podatkov (npr. javno objavljen dostop do CRL) – glej [1] pogl. 2 (namesto CRL lahko aplikacija preverja status potrdila preko protokola OCSP, *storitev trenutno ni dostopna*).

5. Podpora za uporabo kriptografskih algoritmov naj bo v skladu s priporočili v pričujočem dokumentu v pogl. 7 oz. v skladu z mednarodnimi in drugimi priporočili (npr. ETSI). Priporočamo uporabo produktov in kriptografskih algoritmov odprtih standardov.

6. Skalabilnost infrastrukture: potrebno je upoštevati pogostnost dostopov in zagotoviti ustrezno infrastrukturo.

7. Aplikacija mora omogočiti uporabniku, da preveri zagotavljanje avtentičnosti in celovitosti aplikacije.

4.1.3 Uporabniška prijaznost

1. Aplikacija mora zagotoviti prijazne in jasne uporabniške vmesnike. Posamezni koraki morajo biti jasno določeni in transparentni uporabniku. Aplikacija mora nuditi ustrezno podporo "Pomoč" in zagotoviti tudi ustrezno drugačno podporo (pomoč po telefonu, e-pošti,....). Tekst v pogovornih oknih mora biti uporabniško razumljiv in jasen.

2. Uporabnik mora biti vedno jasno obveščen o namenu vnosa gesla in drugih podatkov ter o morebitnih tveganjih (s politiko uporabe e-podpisa in tudi sprotno preko pogovornih oken).

3. Aplikacija mora avtomatično uporabniku ponuditi ustrezno digitalno potrdilo, z ustreznim namenom ("Key Usage").

4. Če aplikacija nudi možnost uporabe v načinu "off-line", potem mora ustrezne kontrole izvesti takoj, ko se uporabnik poveže v način "on-line".

5. Aplikacija ne sme uporabnika obremeniti s prepogostimi vnosi gesel oz. informacijah o varnosti. Pogostnost potrebnega prijavljanja z vnosom gesla uporabnika lahko celo zmanjšuje varnost aplikacije, saj se s tem zmanjša uporabnikova pozornost.

6. Aplikacija mora podpirati uveljavljena okolja uporabnikov, npr. uporabo različnih brskalnikov, operacijskih sistemov ipd.

7. V kolikor tehnologija dopušča, je potrebno zagotoviti optimalno varno okolje na strani uporabnika že s privzetimi nastavitvami.

8. Uporabniški vmesniki morajo biti verodostojni:
   - pri vnosu gesel (pod znaki `*´ mora biti dejansko šifrirano geslo),
   - ko uporabnik izvede odjavo, mora aplikacija dejansko prekiniti povezavo.

Aplikacije morajo v skladu z zahtevami svojega poslovnega vidika storitve upoštevati oz. imeti vgrajene naslednje funkcionalnosti:
- avtentikacija,
- avtorizacija,
- zaupnost,
- e-podpisovanje za zagotovitev nedvoumnega izvora, podpore za nezatajljivosti in celovitosti.

4.2. Avtentikacija

S prehodom v elektronski svet so se pojavile zahteve za nove mehanizme za povečanje zaupanja v prepoznavnost vseh vključenih strani. Potrebno je ugotoviti istovetnost vsakega posameznika, da ne bi prišlo do razkritja kakršnekoli informacije nepooblaščeni osebi. Prijava z uporabo uporabniškega imena in gesla je "programska prijava". Najvišji nivo varnosti pri ugotavljanju istovetnosti zaenkrat zagotavljajo kvalificirana digitalna potrdila z uporabo pametnih kartic.

4.2.1 Tehnična priporočila

1. Aplikacija mora podpirati avtentikacijo vseh vključenih na podlagi digitalnih potrdil.

2. Na podlagi digitalnega potrdila je potrebno preveriti (avtentikacija SSL):
   - veljavnost potrdil ("Valid From", "Valid To"),
   - veljavnost podpisa izdajatelja potrdila,
   - da digitalno potrdilo ni preklicano (preverjanje CRL).

3. Aplikacija mora uporabiti digitalno potrdilo z ustreznim namenom ("Key Usage" – *Digital Signature* ali "extendedKeyUsage": *ClientAuth* (slednja opcija zaenkrat ni implementirana v digitalnih potrdilih Overitelja na CVI).

4. Če je aplikacija zasnovana več-nivojsko, se morajo podatki o opravljeni avtentikaciji ustrezno, celovito in varno prenesti na ostale nivoje.

5. Spletne aplikacije naj si zagotovijo interoperabilnost z upoštevanjem standardov:
   - SSL 3.0
   - TLS
   - IPsec
   - S/MIME

- PKSC#7 oz. CMS,
- idr.

4.3. Druga priporočila

1. Aplikacija mora zavrniti uporabnika z neustreznim digitalnim potrdilom (npr. potrdilo neustreznega izdajatelja).

2. Aplikacija mora uporabnika obvestiti o uspešni prijavi in mora tudi ponuditi možnost, da postopek zavrne.

3. Aplikacija mora uporabniku prikazati v berljivi obliki vse ključne podatke o opravljeni avtentikaciji (identiteto, izdajatelja, ...).

4. Potrebno je upoštevati pogostnost dostopov in zagotoviti ustrezno infrastrukturo.

4.4. Avtorizacija

Ko na podlagi avtentikacije ugotovimo istovetnost uporabnika oz. identiteto, za katero se uporabnik predstavlja, moramo temu uporabniku določiti ustrezna dovoljenja, potrebne vire oz. tisto, kar uporabnik pričakuje. Vse vključene strani morajo jasno vedeti, kaj za svoje delo potrebujejo, uporabnikom moramo dati informacijo, "kje in kdaj" dobijo, kar potrebujejo s čim manjšo porabo vseh obstoječih virov. Vsakega uporabnika moramo obravnavati kot edinstveno "osebo" s svojimi potrebami. Paziti moramo, da uporabnika ne obremenjujemo z zahtevnostjo celotnega sistema, mora pa biti s samo storitvijo zadovoljen.

4.4.1 Priporočila

1. Glede na poslovne značilnosti storitve, je potrebno v aplikaciji določiti vzpostaviti shemo dostopnih pravic v smislu:
   - logične kontrole na podlagi identitete na podlagi avtentikacije,
   - kontroliran dostop tako do strežnika kot do uporabniškega vmesnika.

2. Dostopne pravice se lahko določi na podlagi različnih podatkov na različne načine. Omejitev je lahko določena na podlagi (glej Profil kvalificiranih digitalnih potrdil in registra preklicanih potrdil izdajateljev SIGEN-CA in SIGOV-CA, 1. del pričujočih priporočil):
   - vrste digitalnih potrdil (npr. dovoljeno samo imetnikom zaposlenim pri poslovnih subjektih – posamezna vrsta se loči na podlagi serijske številke oz. dela razločevalnega imena ali OID politike),
   - skupine uporabnikov, ki pripadajo določenim poslovnim subjektom,
   - posameznikom,
   - ipd.

3. Po uspešni avtentikaciji se identiteta uporabnika prenese v ustrezno shemo dostopnih pravic.

4. Pri vzpostavitvi sheme se lahko upošteva ustrezen podatek o nedvoumni identiteti uporabnika:
   - razločevalno ime uporabnika digitalnega potrdila,
   - serijsko številko digitalnega potrdila,

- osebne podatke vezane na serijsko številko potrdila (dobljeni preko prevajalne tabela MULTI ali od uporabnik),
- specifične podatke v potrdilu, ki so podani kot razširitve ("extension") potrdila.

4.5. Zasebnost

Odnos vključenih strank je grajen na temelju medsebojnega zaupanja, saj je le tako lahko zaupna in občutljiva informacija zaščitena in pravilno obravnavana. Zavedati se moramo, da se poudarek na zasebnosti pri elektronskem poslovanju povečuje, saj so transakcije izpostavljene javnemu omrežju, katerega pa ni enostavno nadzorovati. V trenutku, ko uporabnik pritisne tipko ali klikne z miško in s tem sproži potrditev, mora biti takšna informacija zaščitena pred nepooblaščenim dostopom ali uporabo.

4.5.1 Priporočila

1. Aplikacije morajo podpirati vzpostavitev varnega kanala med uporabnikom in strežnikom, v kolikor je to poslovna, zakonska ali varnostna zahteva.

2. Aplikacije morajo podpirati šifriranje vsebine oz. dokumentov, ki nastanejo z opravljanjem storitve, v kolikor je to poslovna, zakonska ali varnostna zahteva.

3. Aplikacija mora uporabiti digitalno potrdilo z ustreznim namenom ("Key Usage" – *keyEnchipherment* ali *dataEnchipherment*).

4. Spletne aplikacije naj si zagotovijo interoperabilnost z upoštevanjem standardov:
   - SSL 3.0
   - TLS
   - IPsec
   - S/MIME
   - PKSC#7 oz. CMS,
   - idr.

5. Preverjanje potrdila (kot v razd. 4.1.2, 2. alinea).

4.6. Verifikacija/Elektronski podpis

Pri klasičnem poslovanju se zaključek dela potrdi s stiskom roke in podpisom ustreznega dokumenta. Pri elektronskem načinu je ključnega pomena zagotavljanje sledečih vidikov varnosti:

- zagotavljanje nezatajljivosti je eden poglavitnih vidikov varnosti in omogoča nezmožnost zanikanja izvora podatkov oz. postopkov ter vključenost v storitev,
- elektronski podpis, ki predstavlja digitalno alternativo klasičnemu podpisu, zagotavlja pa nedvoumno istovetnost vseh sodelujočih strani in je osnova podpore zagotavljanju nezatajljivosti,
- točen čas izvedbe transakcije, ki določeno transakcijo oz. dokument postavi v določen čas in s tem potrjuje, da je dokument ali podatek obstajal, oziroma nastal pred tem časom,
- zaupanje vseh vključenih strani, da je transakcija, ki vsebuje občutljivo informacijo, celovita, torej prava in nespremenjena.

4.6.1 Priporočila

1. E-podpis mora biti izveden v skladu z načelom WIPIWIS (*angl.* **W**hat **I**s **P**resented **I**s **W**hat **I**s **S**igned) in zavestno s strani podpisnika. Podpisnik mora biti vnaprej obveščen o postopku podpisa. Nezavestna izvedba e-podpisa mora biti onemogočena (razen v primerih avtomatskega podpisa strežnika oz. aplikacije).

2. Aplikacija mora vzpostaviti zaupanje uporabnika do podpisanih podatkov. Uporabniku mora biti nedvoumno prikazano, kateri podatki se podpisujejo.

3. V vsaki fazi postopka, ki zahteva digitalni podpis podatkov, je potrebno pred naslednjo fazo uspešno preveriti veljavnost digitalnega podpisa.

4. Verifikacija podpisa se izvede:
   - v realnem času, to je takoj po podpisu, oziroma v času, ko se smatra, da so vsi podatki za verifikacijo, oziroma njihov status, še nespremenjeni (začetno preverjanje),
   - po preteku daljšega časovnega obdobja (več ur, dni, let, ...), ko nekateri ali vsi podatki za verifikacijo nimajo več istega statusa kot ob podpisu (običajno preverjanje).

5. Verifikacija vključuje:
   - veljavnost podpisnikovega digitalnega potrdila (ni potekel, ni v CRL, overil ga je ustrezni izdajatelj),
   - veljavnost podpisa na podatkih,
   - veljavnost časovnega žiga ali oznake, kjer je potrebno zagotoviti varno beleženje vrednosti in digitalnih podpisov.

   Uporabniku morajo biti prikazani v berljivi obliki vsi ključni podatki o opravljeni verifikaciji podpisa.

6. Aplikacija mora v odvisnosti od poslovnih značilnosti omogočati podpis več podpisnikov (npr. možnost verižnega podpisovanja).

7. Aplikacija mora uporabiti digitalno potrdilo z ustreznim namenom ("Key Usage" – *Digital Signature*) ter politiko overitelja.

8. Aplikacije morajo znati izvesti časovne žige oz. oznake in opraviti tudi njihovo verifikacijo.

9. Za podporo nezatajljivosti opravljene storitve je potrebno glede na varnostne in poslovne zahteve pripraviti:
   - dokazilo, kdo je dokument pripravil (angl. *origin*),
   - dokazilo, da je bil dokument poslan (angl. *submission*),
   - dokazilo, da je dokument prispel (angl. *delivery*),
   - dokazilo, da je bil dokument pravilno prejet (angl. *receipt*).

10. Podpis mora vsebovati še sledeče atribute (v skladu s politiko uporabe e-podpisa – glej 5):
    - kdo je podpisal dokument,
    - časovno oznako,
    - format dokumenta,
    - sklicno številko,
    - namen podpisa,
    - ipd.

Vse o formatu varnega elektronskega podpisa in aplikacijah za podpisovanje in verifikacijo podpisa v skladu s priporočili ETSI in CEN je podano v poglavju pogl. 6 in prilogah B, C in D.

4.7. Priporočila za arhiviranje digitalno podpisanih dokumentov

Za elektronsko podpisane dokumente, ki nastanejo ob opravljanju vrste storitev, se lahko zahteva hranjenje oz. arhiviranje tudi za dobo, ki je daljša od dobe veljavnosti digitalnih potrdil. V teku so aktivnosti na področju normativne ureditve problema hranjenja in ohranjanja digitalno podpisanih dokumentov pri nas in v svetu. V prihodnjem letu se pričakuje sprememba Direktive 1999/93/EC, ki ureja področje e-podpisa v EU. Nekatere članice že opozarjajo na nujnost ureditve dolgotrajnega ohranjanja elektronsko podpisanih dokumentov, ki je v trenutno veljavni direktivi pomanjkljivo obdelana. Izdana pa so bila že priporočila glede same formata e-podpisa dokumentov arhivskih vrednosti, ki bi pripomogel k ohranjanju avtentičnosti, celovitosti in pravni veljavnosti digitalnih podpisov (več o tem v nadaljevanju).

Za e-podpisane dokument je potrebno upoštevati, kakšne so zahteve za hrambo takega dokumenta:

- zahtevan čas hrambe,
- dostopnost,
- razpoložljivost,
- uporabnost dokumenta,
- pravna veljavnost dokumenta,
- itd.

4.7.1 Priporočila

1. Shranjevanje vsebine v enotnem predpisanem in prenosljivem formatu (priporočena je uporaba XML) ter omogočanje dostopa do dokumentov ter ohranjanje njihove berljivosti.

2. Shranjevanje konteksta dokumentov v enotnem predpisanem in prenosljivem formatu - priporočena je uporaba XML.

3. Shranjevanje arhivskih dokumentov iz delovnega okolja, kjer dokumenti nastanejo oz. kjer so za to ustrezne zahteve.

4. Izvedba formata e-podpisa v skladu s priporočili ETSI za ohranjanje veljavnosti za daljše obdobje z dodanimi ustreznimi podatki za verifikacijo e-podpisa, z izvajanjem periodičnega časovnega žigosanja itd.

5. Zapis v arhivu mora vsebovati vse podatke, ki so potrebni za preverjanje verodostojnosti e-podpisa.

6. Skladno z zahtevami se morajo ustrezno beležiti vsi dostopi do dokumentov (glej razd. 4.8).

Več o formatu podpisa za dolgotrajno hrambo v pogl. 6 in prilogi B.

4.8. Beleženje dogodkov

Vse faze v izvajanju postopka storitve oz. dostopu do podatkov oz. dokumentov morajo biti zabeležene in dostopne za kasnejši vpogled.

4.9. Zgled shematskega poteka aplikacije

4.9.1 Visok nivo varnostnih zahtev: *Oddaja e-podpisanega dokumenta s povratnico*

V nadaljevanju je podan shematski potek aplikacije z visokim nivojem varnosti, kjer uporabnik oddaja e-podpisan dokument (spletni obrazec) ob tem, da uporabnik prejme povratnico.

Izhodišča za primer z visokim nivojem varnosti:
- tako uporabnik kot strežnik uporabljata digitalno potrdilo,
- spletni obrazec je dostopen samo avtoriziranim uporabnikom (z ustreznimi serijskimi številkami potrdila),
- za dokument mora biti zagotovljena podpora za nezatajljivost (zahteva za e-podpis),
- ob izmenjavi mora biti zagotovljena zasebnost (vsa komunikacija med uporabnikom in strežnikom poteka po protokolu HTTPS), šifriranje samega pa dokumenta ni potrebno,
- obrazec se arhivira,
- vse faze postopka se beležijo in varno shranjujejo.

Shematski potek oddaje e-obrazca:
1. Uporabnik se poveže na ustrezni spletni naslov. Vzpostavi se seja SSL.

2. Izvede se *avtentikacija*. Uporabnik in strežnik se medsebojno preverita.

3. Izvede se *avtorizacija*. Na podlagi uspešne *avtentikacije* in ustreznosti uporabnika v shemi dostopnih pravic aplikacija ponudi uporabniku pripadajočo stran s spletnim obrazcem. Evidenčni podatki in podatki o uporabniku se vnesejo v obrazec, ki se nato posreduje uporabniku.

4. Uporabnik vnese v obrazec manjkajoče podatke in jih posreduje strežniku.

5. Strežnik oz. aplikacijo opravi kontrolo podatkov (semantično in sintaktično preverjanje), doda ostale potrebne podatke (sklicno številko, čas, format,...), oblikuje obrazec, ki bo e-podpisan, izvede nad tem *e-podpis* in dokument posreduje uporabniku.

6. Uporabnik opravi *verifikacijo e-p*odpisa in izvede *e-podpis* ter obrazec posreduje na strežnik.

7. Strežnik verificira uporabnikov e-podpis, dokumentu doda časovni žig in pripravi potrdilo o prejemu dokumenta. Le-tega e-podpiše in pošlje uporabniku. Dokument in povratnico shrani v bazo zalednih aplikacij za kasnejšo obdelavo ter v arhiv.

8. Uporabnik preveri e-podpis na povratnici in jo skupaj z oddanim dokumentom shrani na svojem računalniku za morebitno kasnejšo uporabo.

9. Seja se zaključi.

4.9.2 Nizek nivo varnostnih zahtev: *Varen vnos podatkov*

V primeru vnosa podatkov preko spletnega obrazca, kjer se za same podatke ne zahteva podpora za nezatajljivost, velja naslednje:

Izhodišča:
- tako uporabnik kot strežnik uporabljata digitalno potrdilo,
- spletni obrazec je dostopen samo avtoriziranim uporabnikom (z ustreznimi serijskimi številkami potrdila),
- za podatke oz. dokument se ne zahteva, da so e-podpisani),
- ob izmenjavi mora biti zagotovljena zasebnost (vsa komunikacija med uporabnikom in strežnikom poteka po protokolu HTTPS), šifriranje obrazca ni potrebno,

- vse faze postopka se beležijo in varno shranjujejo.

Shematski potek oddaje e-obrazca:
1. Uporabnik se poveže na ustrezni spletni naslov. Vzpostavi se seja SSL.

2. Izvede se *avtentikacija*. Uporabnik in strežnik se medsebojno preverita.

3. Izvede se *avtorizacija*. Na podlagi uspešne *avtentikacije* in sheme dostopnih pravic aplikacija ponudi uporabniku ustrezno stran s spletnim obrazcem za vnos podatkov. Evidenčni podatki in podatki o uporabniku se skladno z zahtevami storitve v obrazec.

4. Uporabnik vnese v obrazec preostale manjkajoče podatke in jih posreduje strežniku.

5. Strežnik oz. aplikacijo opravi kontrolo podatkov (semantično in sintaktično preverjanje), doda ostale potrebne podatke (sklicno številko, čas, ...). Podatki se shranijo v bazi aplikacije.

6. Seja se zaključi.

5. VARNOSTNA POLITIKA UPORABE E-PODPISA IN OVERJANJA PODPISA

Medsebojna razmerja, odgovornosti, pravna razmerja in tehnične pogoje vseh vključenih v storitev (podpisnika-stranke, tretje osebe itd.), je potrebno določiti v varnostni politiki uporabe e-podpisa Le-ta mora biti nedvoumna in dostopna vsem strankam, ki kreirajo e-podpis in ga tudi overjajo.

Politika e-podpisa je lahko vključena v podpisani dokument:
- implicitno, če je v podpisanem dokumentu navedeno, da drugi dokument kot npr. zakon, pogodba, navaja, da mora biti določena politika podpisa uporabljena za določen tip podatkov.
- eksplicitno, če je v podpisu navedena eksplicitna referenca na politiko podpisa.

Oseba, ki overja podpis, mora pred overjanjem vedeti določila politike podpisa. Le-ta mora biti dostopna v tekstovni obliki ali predstavljena na način, ustrezen za avtomatsko procesiranje s strani sistema.

Iz politike podpisa mora biti popolnoma jasno, pod katerimi pogoji se sprejme podpis, pod katerimi se podpis kreira. Politika podpisa mora vključevati:
- enoumno identifikacijsko oznako politike podpisa,
- ime izdajatelja politike podpisa,
- datum izdaje politike podpisa,
- področje uporabe politike podpisa,
- politiko za overjanje podpisa (SVP, angl. *Signature Validation Policy*,), ki vključuje pravila za določanje/overjanje overitvene poti (angl. *Certification Path* – CP), pravila za uporabo CRLjev, OCSP-jev; časovnih žigov in oznak,
- podatke za overjanje podpisa, ki jih priloži podpisnik, podatke za overjanje podpisa, ki jih zbere oseba/sistem, ki overja podpis.

Lahko pa tudi vključuje:
- obdobje, do kdaj se lahko podpisuje po tej politiki,
- pravila za uporabo različnih funkcij podpisnikov,
- omejitve za podpisne algoritmi in dolžine ključev,
- dodatna pravila politike podpisa, ki so potrebna za dosego namena podpisa.

V prilogi A pričujočega dokumenta je podan povzetek priporočil ETSI za politiko uporabe e-podpisa in njegove verifikacije (ETSI *Signature Policies Report* - TR 102 041 (februar 2002)), [2]. Osnutek

priporočila za storitve, kjer se zahteva več podpisnikov, je dostopen preko spletnih strani ETSI - *Signature Policy for Extended Business Model* –TR 102 045 STF 209-T1 (nov. 2002).

6. FORMAT VARNEGA ELEKTRONSKEGA PODPISA

Za storitve, ki zahtevajo najvišji nivo varnosti, je potrebno za pravno veljavnost podatkov, ki se izmenjujejo na elektronski način, potrebno zagotoviti avtoriziran dostop do teh podatkov ter njihovo avtentičnost in celovitost. Zagotavljanje nezataljivosti je eden poglavitnih vidikov varnosti in omogoča nezmožnost zanikanja izvornosti podatkov oz. postopkov ter vključenost v storitev. Nezatajljivost je zagotovljena z uporabo več mehanizmov na vseh nivojih. Uporabljeni so tehnični mehanizmi in postopki skladno z ZEPEP, Direktivo EU za elektronski podpis (Directive 1999/93/EC) in priporočili ETSI in CEN. Bistveni elementi zagotavljanja nezatajljivosti so elektronski podpis, časovni žig oz. varna časovna oznaka na elektronsko podpisanih dokumentih ter varno arhiviranje vseh potrebnih podatkov za dolgoročno veljavnost in preverjanje elektronskih podpisov.

Elektronski podpis je nujen pri zagotavljanju nezatajljivosti, vendar mora biti za to zagotovljenih več pogojev. Varovanje zasebnega ključa na strani podpisnika kot tudi na strani aplikacije mora biti ustrezno, odgovornosti vključenih v storitev pa določena v varnostni politiki uporabe elektronskega podpisa (glej pogl. 5). Potrebno je ustrezno preverjanje veljavnosti digitalnega podpisa. Več o samih aplikacijah za sam e-podpis in njegovo verifikacijo v prilogah C in D.

Osnovna oblika varnega elektronskega podpisa (*v nadaljevanju* elektronski podpis), ki ustreza ZEPEP in Direktivi EU za elektronski podpis (Directive 1999/93/EC), pomeni uporabo asimetričnih algoritmov za šifriranje (npr. RSA) s podpisnikovim zasebnim ključem nad sledečimi podatki

1. zgoščena vsebina (angl. *hash code*): "seštevek" sporočila, ki povezuje digitalni podpis s podatki, ki se jih podpisuje. Zgoščena vsebina nastane iz podatkov z uporabo zgoščevalne funkcije (npr. SHA-1) s sledečimi lastnostmi:
   - rezultat zgoščene vsebine nad istimi podatki je vedno enak (kar zagotavlja tudi enako uporabo za uspešno verifikacijo),
   - iz zgoščene vsebine ni mogoče restavrirati sporočila,
   - vsaka sprememba v sporočilu povzroči spremembo "seštevka" sporočila.
2. kvalificirano digitalno potrdilo, ki nedvoumno in enolično pripada zasebnemu ključu podpisnika.

Osnovna oblika elektronskega podpisa zadošča za uporabo v kratkem časovnem obdobju od samega nastanka digitalnega podpisa, ko smo z veliko gotovostjo prepričani, da se razmere v zvezi stanjem potrdila niso spremenile. Za uspešno verifikacijo morajo biti na razpolago:

1. vsa potrdila, uporabljena za podpis, t.j. podpisnikovo digitalno potrdilo in potrdilo izdajateljev (oz. veriga potrdil izdajateljev),

2. statusi uporabljenih digitalnih potrdil, ki dokazujejo, da so bila potrdila veljavna in niso bila preklicana, pridobljena pa na podlagi:
   - registra preklicanih potrdil (CRL, angl. *certificate revocation list*) ali
   - sprotnega odgovora o stanju potrdila (OCSP, angl. *on-line certificate status protocol*),

3. varen časovni žig ali varna časovna oznaka, ki pomeni nedvoumen dokaz o obstoju digitalnega podpisa ob določenem času in vključuje:
   - zgoščeno vsebino digitalnega podpisa,
   - zaupanja vredno časovno označbo,
   - identiteto izdajatelja časovnega žiga.

Povzetek formata e-podpisa, ki je podan v prilogi B, je v skladu s priporočili *Electronic Signature Formats* - ETSI TS 101 733 v 1.3.1, feb. 2002 (za notacijo ASN.1 (angl. *Abstract Syntax Notation 1*)) in *XML Advanced Electronic Signatures (XAdES)* - ETSI TS 101 903, feb. 2002.

7. PRIPOROČILA UPORABE KRIPTOGRAFSKIH ALGORITMOV

Aplikacija naj bo pripravljena tako, da je možno določiti algoritme, dolžine ključev in protokole, ki jih uporablja, ter jih zamenjati, če se pokaže, da niso več zadostno varni. Priporočamo uporabo znanih in preverjenih kriptografskih algoritmov:

1. za zgoščevalno funkcijo SHA-1 ali ripemd-160,
2. za šifriranje trojni DES ali AES s 128-bitnim ključem,
3. za izmenjavo ključa RSA s 1024-bitnim modulom ali Diffie-Hellman s 1024-bitnim praštevilskim ključem,
4. za digitalni podpis RSADSS s 1024-bitnim ključem ali DSA s 1024-bitnim ključem.

Podrobnejše specifikacije tudi ostalih uveljavljenih algoritmov so v prilogi E, pri tem smo pri algoritmih za digitalni podpis upoštevali priporočilo ETSI SR 002 176 v1.1.1 (marec 2003).

8. TERMINOLOGIJA IN POJMI

V pripravi (objavljeno v dokumentu ver. 1.1)

9. LITERATURA

[1] Priporočila Overitelja na CVI za aplikacije e-storitev z varnostnimi zahtevami z uporabo kvalificiranih digitalnih potrdil – 1.del, *Profil kvalificiranih digitalnih potrdil in registra preklicanih potrdil izdajateljev SIGEN-CA in SIGOV-CA,* marec 2003.

[2] Domača stran ETSI (ang. *European Telecommunications Standards Institute*) http://www.etsi.org.

[3] Domača stran EESSI (ang. *European Electronic Signature Standardization Initiative)*, http://www.ict.etsi.fr/eessi/Documents/.

[4] Domača stran CEN/CWA (fr. *Comite European de Normalisation)*, http://www.cenorm.be.

[5] *XML-Signature Core Syntax and Processing,* W3C/IETF 08-2001, avgust 2001.

DODATEK

STANDARDI IN PRIPOROČILA EU

Področje elektronskega poslovanja je pravno formalno urejeno na več nivojih. V okviru držav EU zakonodajno področje elektronskega poslovanja urejajo ustrezne direktive evropskega parlamenta in komisije združenih narodov. Poleg teh pa ima večinoma tudi vsaka članica EU svojo nacionalno zakonodajo. Zaradi interoperabilnosti elektronskega poslovanja in zaradi lažjega izpolnjevanja standardov, ki urejajo to področje in izhajajo iz Direktive1999/93/EC, bo potrebno nacionalno zakonodajo vsaj do določene mere uskladiti z evropsko. Enako velja tudi za Slovenijo, kjer je Zakon o elektronskem poslovanju in elektronskem podpisu že usklajen z Direktivo 1999/93/EC in z določili Modelnega zakona Komisije OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju in enotnimi pravili za elektronske podpise ter z določili primarne evropske zakonodaje.

Evropska komisija je pooblastila institucijo EESSI (angl. *European Electronic Signature Standardization Initiative*) za analizo področja za določitev potrebnih standardov. V okviru EESSI delujeta instituciji ETSI in CEN, katerih delovanje je opisano v nadaljevanju.

ETSI

ETSI (angl. *European Telecommunications Standards Institute*) je neprofitna organizacija, katere poslanstvo je priprava telekomunikacijskih standardov za področje Evrope, ki bodo služili kot smernice razvoja telekomunikacijskih storitev v prihodnje. To so predstavniki uprave, operaterji, podjetja, ponudniki storitev, raziskovalne ustanove in uporabniki. ETSI igra pomembno vlogo pri razvoju širokega spektra standardov in tehnične dokumentacije, ki predstavlja evropski prispevek k svetovni standardizaciji na področju telekomunikacijske in informacijske tehnologije. ETSI je uradno priznan s strani Evropske komisije in sekretariata EFTA. V nadaljevanju je naštetih nekaj ETSI priporočil s področja elektronskega poslovanja, ko so tudi predmet tega dokumenta:

- *Signature Policies Report* - TR 102 041 (februar 2002),
- *XML Advanced Electronic Signatures (XAdES)* - TS 101 903 (februar 2002),
- *Electronic Signature Formats* - TS 101 733 v 1.3.1 (februar 2002),
- *XML format for signature policies* - TR 102 038 (april 2002),
- *Signature Policy for Extended Business Model* –TR 102 045 STF 209-T1 (nov. 2002) – *v pripravi,*
- *Time stamping profile* - TS 101 861 v1.2.1 (marec 2002).

Priporočila in ostali dokumenti ETSI so dostopni preko spletne strani http://www.etsi.org.

CEN

CEN (fr. *Comite European de Normalisation*) je organizacija, ki pripravlja evropske standarde s področij informatike, ki pa ne sodijo v področji elektrotehnike in telekomunikacij. CEN je ustanovila t.i. sistem standardizacije informacijske družbe (angl. *Information Society Standardization System* oz. CEN/ISSS), prek katerega se odvijajo delavnice, ki so odprtega tipa. Rezultati teh delavnic so objavljeni pod oznako CWA (angl. *CEN Workshop Agreements*).

Delavnica CEN/ISSS E-SIGN je odgovorna za del EESSI delovnega programa, ki se nanaša na kvalitativne in funkcijske standarde za sredstva za elektronsko podpisovanje in sredstva za overjanje elektronskega podpisa ter tudi za kvalitativne in funkcijske standarde za overitelje digitalnih potrdil. Doslej so bili pod okriljem CEN/ISSS s področja predmeta tega dokumenta pripravljeni naslednji dokumenti:

- *CWA14172-4 EESSI Conformity Assessment Guidance – Part: 4: Signature Creation Application and Procedures for Electronic Signature Verification,*

- *CWA14172-5 EESSI Conformity Assessment Guidance – Part: 5: Secure signature creation devices,*
- *CWA14171 Procedures for Electronic Signature Verification,*
- *CWA 14170 Security Requirements for Signature Creation Systems,*
- *CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+',*
- *CWA 14168 Secure Signature-Creation Devices, version 'EAL 4'.*

A. POLITIKA UPORABE E-PODPISA IN OVERJANJA PODPISA

(ETSI TR 102 041, 02-2002)

Pričujoči dokument povzema opis priporočil za politiko uporabe e-podpisa, ki so podrobneje predstavljene v dokumentu **ETSI *Signature Policies Report* - TR 102 041 (feb. 2002**), ki je dostopen na spletnih straneh ETSI, [2]. Osnutek priporočila za storitve, kjer se zahteva več podpisnikov, je dostopen preko spletnih strani **ETSI - *Signature Policy for Extended Business Model* –TR 102 045 STF 209-T1 (nov. 2002).**

Ko želita dve neodvisni stranki overiti določen e-podpis, morata uporabljata ista pravila, da bi dobili iste rezultate. Taka pravila vsebuje politika podpisa, mora pa biti nedvoumna in dostopna vsem strankam, ki kreirajo podpis in ga tudi overjajo.

S tem so povezane zahteve po dostopnosti politike podpisa in njeni nedvoumnosti. Politika podpisa je lahko vključena v podpisani dokument:

- **implicitno**, če je v podpisanem dokumentu navedeno, da drugi dokument kot npr. zakon, pogodba, navaja, da mora biti določena politika podpisa uporabljena za določen tip podatkov.
- **eksplicitno**, če je v podpisu navedena eksplicitna referenca na politiko podpisa.

Oseba, ki overja podpis, mora pred overjanjem poznati določila politike podpisa. Priporočeni so trije načini objave politike podpisa, ki zagotavljajo, da je uporabljena politika podpisa res prava:

- preko varnega kanala (Web+SSL.; ni praktično za dolgoročno overjanje),
- preko shrambe (angl. *repository*) registriranih politik podpisa (izvaja tretja oseba; omogoča običajno overjanje; politike se hranijo dokler obstaja potreba po njihovi uporabi),
- preko trajnih medijev (zgoščenke, ...).

Iz politike podpisa mora biti popolnoma jasno, pod katerimi pogoji se sprejme podpis.

A 1. Vsebina politike e-podpisa

Politika podpisa mora vključevati:

- enoumno identifikacijsko oznako politike podpisa,
- ime izdajatelja politike podpisa,
- datum izdaje politike podpisa,
- področje uporabe politike podpisa,
- politiko za overjanje podpisa (SVP, angl. *Signature Validation Policy*,).

Področje uporabe opiše pričakovano uporabo in pogoje, ki se nanašajo na elektronski podpis. Vsebuje različne pravne in pogodbene določbe.

Politika za overjanje podpisa določa tehnična pravila, ki jih morata upoštevati podpisnik in oseba ali sistem, ki overja podpis za obdelavo elektronskega podpisa. Politika za overjanje podpisa je lahko v tekstovni obliki ali predstavljena na način, ustrezen za avtomatsko procesiranje s strani sistema. Politika za overjanje podpisa vključuje definicijo komponent elektronskega podpisa, ki jih mora pripraviti podpisnik in podatke, ki jih potrebuje oseba/sistem, ki overja

podpis za običajno overjanje. Poleg tega vsebuje pravila za uporabo storitev različnih ponudnikov varnih storitev (angl. Trust Service Provider-TSP, CA, strežniki OCSP, Attribute Authorities, Time Stamping Authorities).

Politika za overjanje podpisa tako vključuje:
- pravila za določanje/overjanje overitvene poti (angl. *Certification Path* – CP),
- pravila za uporabo CRLjev, OCSPjev, časovne oznake in žiga,
- podatke za overjanje podpisa, ki jih priloži podpisnik,
- podatke za overjanje podpisa, ki jih zbere oseba/sistem, ki overja podpis.

Lahko pa tudi vključuje:
- obdobje, do kdaj lahko podpisujemo po tej politiki,
- pravila za uporabo različnih funkcij podpisnikov,
- omejitve za podpisne algoritme in dolžine ključev,
- dodatna pravila politike podpisa, ki so potrebna za dosego namena podpisa.

B. FORMAT VARNEGA ELEKTRONSKEGA PODPISA

(ETSI TS 101 733 v 1.3.1, 02-2002,)

V tem poglavju je podan opis **formata varnega e-podpisa v skladu s priporočili ETSI *Electronic Signature Formats* – TS 101 733 v 1.3.1, feb. 2002 z elementi za podporo zagotavljanja nezatajljivosti.**

Elektronski podpis lahko obstaja v različnih oblikah vključujoč:

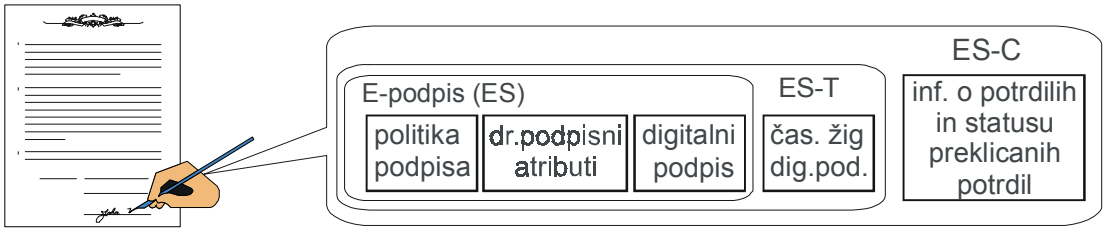
1. **osnovni elektronski podpis, ES** (angl. *electronic signature*): vključuje elektronski podpis in ostale osnovne informacije, priložene s strani podpisnika; za pravno veljavnost pa vključuje še druge potrebne atribute podpisa:
   - referenca na politiko elektronskega podpisa (OID, ki enolično določa politiko uporabe elektronskega podpisa, glej pogl. 5); ki določa tehnične zahteve in pravna razmerja med podpisom in tretjo osebe ter ostale potrebne atribute digitalnega podpisa,
   - podpisani podatki;
   - digitalni podpis (generiran s podpisnikovim zasebnim ključem);
   - drugi podpisani atributi (definirani v politiki uporabe elektronskega podpisa in so lahko obvezni ali neobvezni):
     - oznaka namena podpisa (angl. *commitment type*);
     - enolična razločevalna oznaka digitalnega potrdila podpisnika;
     - vloga podpisnika (angl. *role attribute*);
     - lokacija podpisnika;
     - datum in ura podpisa;
     - format podpisanih podatkov
     - …

   Ta oblika nudi osnovno identifikacijo podpisnika in zaščito celovitosti. Ustvarimo ga lahko brez dostopa do »on-line« storitev (časovnega žiga). Vendar ta oblika ne nudi možnosti za določitev časovnega okvirja (kdaj je bil elektronski podpis ustvarjen). Zaradi tega nam ta oblika ne nudi zaščite proti kasnejšemu zanikanju podpisnika, da je bil elektronski podpis ustvarjen v času veljavnosti pripadajočega potrdila.

2. **elektronski podpis s časovnim žigom, ES-T** (angl. *electronic signature with time*): doda ali časovni žig k ES (začetni koraki k zagotavljanju dolgoročne veljavnosti) ali časovno oznako k ES, tako da shrani ES in časovno oznako na varno revizijsko sled,

3. **elektronski podpis z vsemi podatki za overjanje, ES-C** (angl. *electronic signature with complete validation data*): k ES-T doda referenco (in ne vrednosti) na vse podatke, ki zagotavljajo veljavnost elektronskega podpisa (overitveno pot, informacijo o preklicu). ES-C vsebuje tako referenco na vse podatke za vrednotenje, kot tudi njihove zgostitvene vrednosti. Ni nujno, da se vsi podatki za vrednotenje hranijo skupaj z ES. V osnovni ES-C obliki jih ni, ES-X (ES extended) oblika pa se razlikuje v tem, da so podatki za vrednotenje priloženi samemu ES.

Shematski prikaz elektronskega podpisa (ES) z dodanim časovnim žigom (ES-T) prikazuje Slika 1. V skrajnem primeru je potrebno e-podpisu dodati tudi podatke, in sicer statuse uporabljenih potrdil oz. vse informacije, uporabljene pri verifikaciji (ES-C).



Slika 1 – Elektronski podpis s časovnim žigom in informacijo o statusu potrdil

Za veljavnost digitalno podpisanega dokumenta in s tem uspešne verifikacije digitalnega podpisa nekaj let po samem nastanku dokumenta sama vsebina dokumenta in digitalni podpis nista zadostna. Potrebno je imeti dostop do ustreznega digitalnega potrdila, in seveda dokazilo o njegovi veljavnosti v času nastanka podpisanega dokumenta. Možno je seveda, da je bilo digitalno potrdilo takrat veljavno, vendar je bilo kasneje preklicano ali pa je potekla njegova veljavnost. Posledično je potrebno hraniti tudi status digitalnega potrdila v času nastanka digitalnega podpisa. Pridobitev teh podatkov je potrebno z verifikacijo digitalnega podpisa zbrati takoj oz. čimprej po nastanku samega podpisa (kot je opisano v prejšnjem razdelku).

Evropska komisija je pooblastila institucijo EESSI (angl. *European Electronic Signature Standardization Initiative*) za analizo področja za določitev potrebnih standardov. Izsledki analize so zbrani v poročilu ekspertne skupine iz leta 2000 [3]. Eno izmed ključnih področij je tudi določitev priporočil za izdelavo formata samega elektronskega podpisa, tudi za namene dolgotrajnega ohranjanja dokumentov. Priporočilo je bilo objavljeno v preteklem letu (*Electronic Signature Formats*, ETSI TS 101 733 v 1.3.1, februar 2002), format elektronskega podpisa za ohranjanje arhivskih dokumentov pa je opisan tudi v nadaljevanju.

Za pravno veljavnost dokumenta je pomembna veljavnost digitalnega podpisa v času nastanka dokumenta, za katero pa je potrebno zagotoviti zaupanja vredno evidenco, s pomočjo časovnega žiga (Slika 1).

Ko govorimo o hrambi za dolgotrajno obdobje, potem moramo predvideti možnosti, da:
- je bil od nastanka podpisa podpisnikovo ali pa izdajateljevo potrdilo zlorabljeno, preklicano ipd.,
- je status digitalnih potrdil (npr. register preklicanih digitalnih potrdil) ni več na voljo (izdajatelj je lahko prenehal z delovanjem ali pa je njegove storitve prevzel drug overitelj),
- da so bili uporabljeni kriptografski algoritmi razbiti in s tem niso več vredni zaupanja, s tem pa tudi razbitje ključev, časovnih žigov itd.

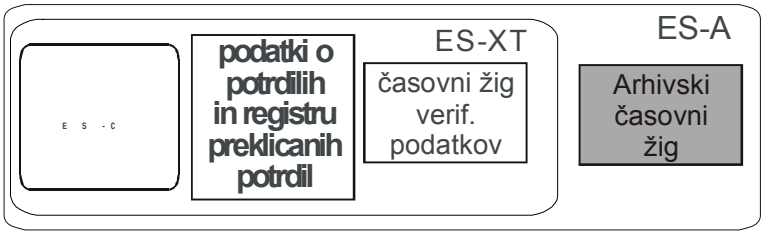
Za e-podpisane dokumentov arhivske vrednosti (dolgotrajna veljavnost e-podpisa) je potrebno pred možnostjo razbitja in s tem ogroženo legitimnostjo dokumenta poskrbeti za podaljševanje veljavnosti z dodajanjem časovnih žigov, narejenih z varnejšimi algoritmi oz. z daljšimi ključi kot so bili uporabljeni pri prejšnjem časovnem žigu (npr. ES-T).

Sekvenčno dodajanje časovnih žigov z daljšimi ključi in novejšo tehnologijo (če je le-ta na razpolago) zaščiti podpis, v primeru, ko tehnologija napreduje do te mere:
- da je mogoče iz javnega ključa ugotoviti zasebnega, ki je bilo uporabljeno za podpis,
- da zgoščevalna funkcija nima več zaupanje vrednih lastnosti.

B 1. Format za dolgotrajno hranjenje e-podpisanih dokumentov

V skladu s priporočili (EESSI "Trusted Archival Services", http://www.ict.etsi.fr/eessi/Documents/Final-Report.pdf, julij

2000) je potrebno za dolgotrajno veljavnost osnovnemu formatu podpisa ES-T oz. ES-C (Slika 1) dodati tudi same vrednosti digitalnih potrdil, vključno s potrdili izdajateljev in njihovimi statusi. Te razširjene podatke zaščitimo s časovnim žigom, ki varuje proti morebitni zlorabi digitalnih potrdil (izdajateljev). Format e-podpisa s tako razširjenimi podatki za verifikacijo prikazuje Slika 2 (označeno ES-XT).



Slika 2 – Arhivski format elektronskega podpisa

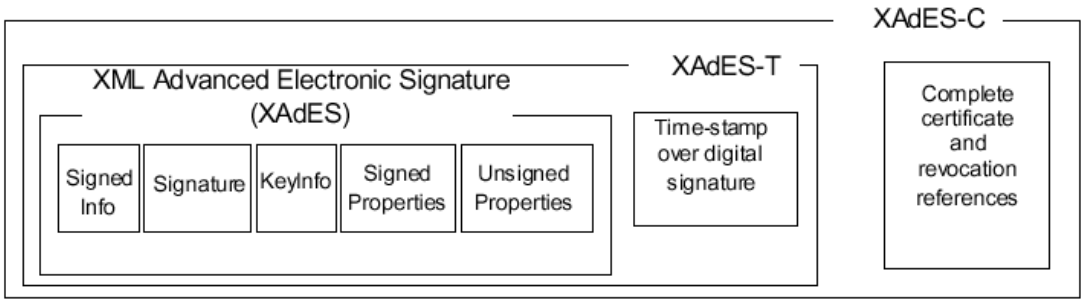
Razširjene podatke podpisa pa je potrebno na novo zaščititi potem, ko postane varnost časovnega žiga (ES-XT) ogrožena. Kot že navedeno uporabimo nov časovni žig, ko je to potrebno glede na razvoj tehnologije in algoritmov. Arhivski format e-podpisa (ES-A) z varovanimi podatki za verifikacijo digitalnega podpisa shematsko prikazuje Slika 2.

B 2. Format elektronskega podpisa v XML

XML (angl. *eXtensible Markup Language*) postaja *de-facto* (odprt) standardni format zapisa podatkov v elektronski obliki, uporablja pa se za različne aplikacije. V zadnjem času se XML uveljavlja tudi kot edini perspektivni format za dolgotrajno hranjenje dokumentov v elektronski obliki. Pred časom je združenje IETF W3C XML-Signature Working Group objavilo priporočila sintakse elektronskih podpisov v XML [5]. Priporočilo podaja osnovne funkcije digitalnega podpisa pa tudi osnovne elemente za varen elektronski podpis. Priporočilo ETSI za sheme XML (*XML Advanced Electronic Signatures (XAdES),* ETSI TS 101 903, februar 2002), osnovni obliki e-podpisa po [5] dodaja predlog sheme XML, ki bo poleg elementov za varen podpis vključevala tudi vse potrebno za dolgotrajno in legitimno hranjenje e-podpisa.

Priporočilo ETSI za XML temelji na že prej navedenem priporočilu ETSI za format e-podpisa (pogl. 6) s podano realizacijo e-podpisa z različnimi zahtevami po času ohranjanja v formatu XML. Slednji realizacijo e-podpisa uporablja notacijo ASN.1 (Abstract Syntax Notation 1) in sledi priporočilu RFC 2630.

Osnovni formati podpisa ES, ES-T in ES-C v izvedbi XML prikazuje spodnje slika, ekvivalenti v XML se imenujejo XadES, XadES-T, XadES-C. Osnovnim elementom podpisa (Signed Info, Signature, KeyInfo), ki so v skladu s standardom W3C, so dodani podatki za zagotovitev varnega e-podpisa oz. celotne informacije za varno preverjanje digitalnega podpisa.



Več o realizaciji formata podpisa je podano v navedenem standardu W3C in priporočilu ETSI.

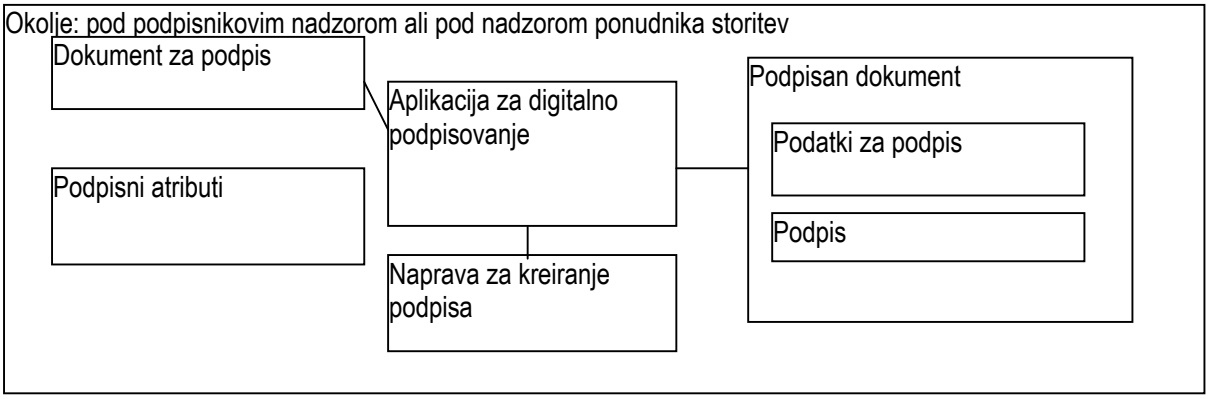
C. PRIPOROČILA PRI IZDELAVI APLIKACIJ ZA E-PODPIS

(CWA 14170:2001)

To poglavje povzema zahteve za aplikacije za digitalno podpisovanje, ki so podrobneje predstavljene v dokumentu Evropskega komiteja za standardizacijo CWA 14170:2001, dostopen na naslovu: http://www.cenorm.be/isss/cwa_download_area/cwa14170.pdf.

Ni uradni standard, je pa priporočilo, pripravljeno s sodelovanjem različnih evropskih strokovnjakov iz gospodarstva, univerz in uradov za standardizacijo, in predstavlja dobro vodilo za pripravo ali preverjanje aplikacij za digitalno oz. elektronsko podpisovanje. Format e-podpisa temelji na priporočilih ETSI, povzetih v poglavju 6 in prilogi B.

Postopek podpisa lahko predstavimo kot naslednji sistem:



Dokument za podpis mora biti tako predstavljen podpisniku, da točno ve, kaj podpisuje. Ne bi smel vsebovati skritih dodatkov (teksta, makrojev, virusov, itd.), ki se jih podpisnik ne zaveda oziroma jih ne vidi. Format dokumenta je opisan v podpisnem atributu, ki natančno določa tip aplikacije, ki naj jo uporabi preverjalec (angl. *verifier*) in kako naj bo dokument predstavljen. Podpisnik uporabi program za kreiranje dokumenta (angl. *Signer's Document Composer*) in program za predstavitev dokumenta (angl. *Signer's Document Presenter*), da preveri, kaj bo podpisal.

Podpisni atributi so dodatna informacija za kreiranje elektronskega podpisa in so vključeni v podpis skupaj z dokumentom. Vsebujejo informacijo o formatu dokumenta, identifikacijski številki iz elektronskega potrdila podpisnika, politiki podpisovanja in pravni veljavnosti, kontekstu oziroma namenu podpisa, časovni žig itd.

V postopku podpisa imamo več korakov, v katerih se osnovni dokument z upoštevanjem podpisnih atributov preoblikuje v naslednje oblike:

- **Podatki za podpis (Data to be signed – DTBS):** vsebujejo dokument za podpis in podpisne atribute. Ta datoteka se najprej se preuredi tako, da je v skladu z izbranim podpisnim standardom – npr. ETSI Electronic Signature Format, ki je opisan v dokumentu ETSI TS 101 733 (angl. *Data to be signed formatted*–DTBSF) in povzet v pogl. 6. Če bi kdo kasneje hotel spremeniti podpisne atribute, verifikacija podpisa ne bi bila uspešna.

- **Povzetek podatkov za podpis (Data to be signed representation – DTBSR)**: je rezultat, ki ga dobimo iz DTBSF z zgoščevalno funkcijo z uporabo komponente za povzetke (angl. *Data Hashing Component*).

- **Varen elektronski podpis (Qualified Electronic Signature)**: pripravi naprava za kreiranje podpisa iz povzetka podatkov za podpis. Pri tem uporabi ustrezni podpisni algoritem in podpisnikove podatke za podpis (Signature Creation Data) v povezavi s podpisnikovim kvalificiranim elektronskim potrdilom.

- **Rezultat podpisa (npr. podpisana datoteka) (Signed Data Object)** vsebuje poleg varnega elektronskega podpisa običajno še dokument za podpis in/ali DTBSF, lahko pa so dodane še različne informacije, ki niso vključene v podpis.

C.1. Potek podpisovanja

1. Podpisnik aktivira aplikacijo.
2. Aplikacija in naprava za kreiranje podpisa se medsebojno overita.
3. Podpisnik izbere podpisne atribute, ki bodo upoštevani pri podpisu.
4. Aplikacija v skladu z varnostno politiko registrira podpisne atribute, ki jih je izbral podpisnik. Poveže podatke iz podpisnikovega digitalnega potrdila z imenom ali psevdonimom in vlogo, v kateri nastopa kot podpisnik.
5. Aplikacija omogoči podpisniku, da si ogleda dokument in izbrane podpisne atribute. V tem koraku preveri elektronske podpise, če so vsebovani v dokumentu za podpis.
6. Če aplikacija omogoča več različnih tipov podpisa, podpisnik izbere ustreznega (npr. varianto formata po standardu ETSI TS 101 733 ali katerega od možnih digitalnih potrdil naj uporabi, če jih ima podpisnik več).
7. Podpisnik sproži postopek podpisovanja - vključi se naprava za kreiranje podpisa.
8. Naprava za kreiranje podpisa overi podpisnika - ta vnese geslo oziroma PIN (ali biometrične podatke).
9. Aplikacija pripravi DTBSF - od zdaj naprej dokumenta ni mogoče več spremeniti.
10. Iz DTBSF se izračuna DTBSR (povzetek) - bodisi v napravi za kreiranje podpisa, bodisi v aplikaciji.
11. Naprava za kreiranje podpisa pripravi elektronski podpis, v katerega je vključen DTBSR.
12. Elektronski podpis se iz naprave za kreiranje elektronskega podpisa prenese v aplikacijo.
13. Aplikacija elektronskemu podpisu doda podatke, ki jih je zahteval podpisnik, da nastane rezultat podpisa - SDO.
14. Podpisnik lahko, če je tako določeno v postopku, verificira podpis in še enkrat preveri DTBS.
15. Rezultat podpisa se shrani ali pošlje naslovnikom.
16. Podatki o postopku podpisovanja se zapišejo.
17. Aplikacija zbriše podatke, ki jih je uporabila za podpisovanje. To je posebej pomembno, če je implementirana na javnem prostoru, ki ni pod podpisnikovo kontrolo.

C 2. Komponente, ki sestavljajo aplikacijo za e-podpis

Nekatere komponente naj bi vsebovala vsaka aplikacija – te so označene z zvezdico. V tabeli navajamo, v katerem koraku podpisovanja je komponenta običajno uporabljena, v zadnjem stolpcu pa so napisana poglavja v priporočilu CWA 14170, v katerih so v originalnem dokumentu navedene varnostne zahteve za komponento.

komponenta	*ime v originalnem dokumentu*	*kratica*	*korak*	*pogl.*
Komponenta za predstavitev dokumenta	Signer's document presentation component	SDP*	5	10
Pregledovalnik podpisnih atributov	Signature attribute viewer	SAV*	5	11
Komponenta za komunikacijo med	Signer's interaction component	SIC*	3,4,6,7	12

podpisnikom in aplikacijo				
Komponenta za overitev podpisnika	Signer's authentication component	SAC*	8	13
Komponenta za končno oblikovanje dokumenta za podpis	DTBS formatter	DTBSF*	9	14
Komponenta za povzetke	Data hashing component	DHC*	10	15
Vmesnik med napravo za kreiranje podpisa in aplikacijo	SSCD/SCA communicator	SSC*	12	16
Komponenta za medsebojno overitev aplikacije in napravo za kreiranje podpisa	SSCD/SCA authenticator	SSA*	2	17
Komponenta za pripravo dokumenta za podpis	Signer's document composer	SDC	5	18
Komponenta za pripravo podpisanega dokumenta v končni obliki	Signed data object composer	SDOC	13	19
Komponenta za zapis podatkov o poteku podpisovanja	Signature logging component	SLC	16	20
Komponenta za dostop do overitelja digitalnih potrdil	CSP interaction component	CSPC	4	21
Komponenta za prikaz podpisnikovih podatkov iz SSCD	SSCD holder indicator	SHI	3,4,6,7	22

Poleg varnostnih zahtev za posamezne komponente so v dokumentu v poglavju 9 obdelane varnostne zahteve za aplikacijo na splošno, v poglavju 23 pa zahteve za priključitev v omrežje.

C 3. Splošne varnostne zahteve aplikacij za e-podpis (CWA 14170, pogl. 9)

- Vloga in pooblastila podpisnika morajo biti jasno določeni z uporabo ustreznih podpisnih atributov;
- Predpostavljamo uporabo kvalificiranih elektronskih potrdil;
- Naprava za kreiranje podpisa in aplikacija morata biti v tako zaščitenem okolju, da ni mogoče prisluškovati podatkom, ki si jih izmenjujeta, ali jih spremeniti;
- Aplikacija mora po opravljenem podpisu zbrisati vse podatke, ki se nanašajo nanj;
- Dostop do aplikacije mora biti tako fizično zaščiten, da ni mogoče videti ali posneti, kaj vnaša podpisnik;
- Podatkov za podpis (DTBS), ki jih je izbral podpisnik, ni mogoče spremeniti ali zamenjati;
- Noben sistemski ali aplikacijski program ali proces, ki ni nujno potreben za delovanje aplikacije za podpisovanje, ne sme imeti dostopa do postopka za podpis;
- Dobro je, če ima podpisnik možnost po končanem podpisovanju preveriti, če rezultat podpisa vsebuje pravi dokument in podpisne atribute (npr. po CWA 14171).

C 4. Zahteve za varno priključitev v omrežje (CWA 14170, pogl. 23)

To so običajne zahteve za varno poslovanje prek interneta. Nameščen mora biti primeren požarni zid in omogočeno odkrivanje virusov, internetnih črvov, trojanskih konjev in drugih škodljivih programov. Aplikacija za elektronsko podpisovanje mora biti nameščena v takem okolju, da ni mogoče nepooblaščeno spreminjati njenih komponent. Imeti mora možnost preveriti veljavnost elektronskih potrdil na varen način.

D. PRIPOROČILA PRI IZDELAVI APLIKACIJ ZA VERIFIKACIJO E-PODPISA

(CWA 14171:2001)

Pričujoči dokument povzema zahteve za aplikacije za overjanje elektronskih podpisov, ki so podrobneje predstavljene v dokumentu Evropskega komiteja za standardizacijo CWA 14171:2001, dostopen na naslovu: http://www.cenorm.be/isss/cwa_download_area/cwa14171.pdf.

Podpisnik lahko podpiše dokument brez dostopa do storitev "on line", s čimer pripravi osnovno obliko podpisa, ki pa ne zagotavlja nezatajljivosti. Za običajno overjanje podpisa pa je potrebno pridobiti še dodatne informacije. Te se pridobi z začetnim overjanjem.

V dokumentu CWA 14171 so opisane varnostne zahteve za različne elemente sistema za overjanje podpisov. Poleg samega postopka overjanja, dokument predstavi različne vmesnike (npr. APIs, MMIs), ki so potrebni za:

- izbiro podpisanega dokumenta in podpisa za overjanje,
- predstavitev podpisanih podatkov v pravem formatu,
- pridobitev informacij o podpisniku in prikaz statusa po overjanju dokumenta,
- pridobitev dodatnih podatkov za običajno overjanje in
- pridobitev podatkov od različnih CSPjev.

Ta dokument določa podatke, ki jih moramo pridobiti in arhivirati, da omogočimo kasnejšo morebitno arbitražo med podpisnikom in osebo, ki overja podpis. Dokument uporablja koncept Politike podpisa (angl. Signature policy - SP) kot osnove za overjanje elektronskega podpisa.

Primarni cilj dokumenta je postavljanje okvirov za verifikacijo kvalificiranega elektronskega podpisa in razlaga pomembnosti uporabe časovnega žiga in časovne oznake tehnologij za kasnejše overjanje podpisa.

Poznamo dve obliki overjanja:

1. začetno overjanje in
2. običajno/dolgoročno overjanje.

D 1. Postopek overjanja - začetno overjanje

Opravi se takoj po elektronskem podpisu dokumenta z namenom pridobitve dodatnih informacij, ki bodo uporabljene oziroma so potrebne za kasnejše običajno overjanje. Podpisnik mora za potrebe začetnega overjanja pripraviti vsaj osnovno obliko elektronskega podpisa.

Pri začetnem overjanju mora oseba/sistem, ki overja podpis najprej nedvoumno identificirati Politiko podpisa. V nadaljevanju si mora na varen način priskrbeti kopijo Politike podpisa in preveriti ali elektronski podpis ustreza zahtevam iz Politike podpisa.

Začetno overjanje tako po eni strani zahteva sistem za obdelavo Politike podpisa (implicitne ali eksplicitne) ter po drugi strani:

1. podpisnikov dokument,
2. e-podpis podpisnikovega dokumenta,
3. dodatne podatke, povezane s podpisom, (imenovani tudi podatki za vrednotenje).

Pri začetnem overjanju, ko ni dodatnih informacij, predpostavimo, da je trenutni čas zelo blizu časa kreiranja podpisa. Tako se pogoji preklica aplicirajo na čas začetnega overjanja. Ker bodo bolj strogi od tistih, ki bi bili sicer v veljavi, ni rizika da sprejmemo neveljaven e-podpis. Obstaja pa nevarnost, da ne sprejmemo veljavnega.

D 1.1. Izhodi začetnega overjanja

1. Izhodni statusi

Začetno overjanje nam vrne naslednje rezultate:
- USPEŠNO kar pomeni, da je elektronski podpis veljaven in v skladu s Politiko za overjanje podpisa,
- NEUSPEŠNO, kar pomeni, da elektronski podpis ni v skladu s Politiko za overjanje podpisa,
- NEPOPOLNO, kar pomeni, da overjanje elektronskega podpisa ni neuspelo, vendar pa ni dovolj informacij za določitev veljavnosti podpisa.

2. Podatki za vrednotenje – angl. *validation data* (VD)

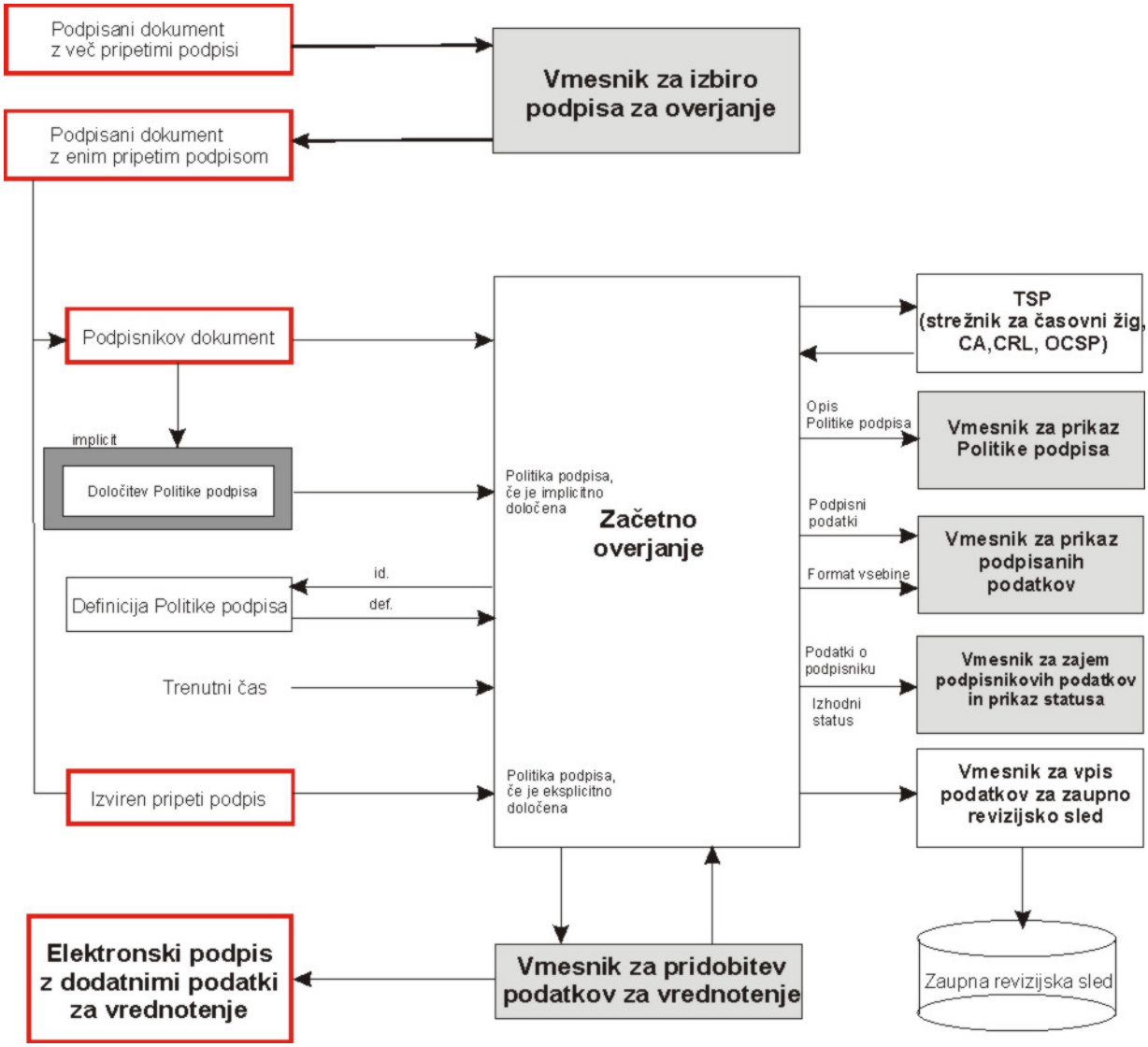
Podatki za vrednotenje elektronskega podpisa so dodatni podatki, ki so potrebni za overjanje elektronskega podpisa in vključujejo:
- dodatna potrdila,
- podatke o preklicu,
- podatke o veljavnosti overitvene poti v času podpisa,
- časovne žige ali časovne oznake.

Pridobi jih bodisi oseba ali sistem, ki overja podpis, bodisi podpisnik sam (če pripravi ES-C). V primeru, da podpisnik ne pripravi ES-T temveč samo ES, mora oseba ali sistem, ki overja podpis dodati časovni žig/oznako ob prvem overjanju podpisa. Podatki za vrednotenje morajo izpolnjevati vse zahteve iz Politike podpisa.

Če podpisnik ne pripravi ES-C, mora oseba/sistem, ki overja podpis pridobiti te podatke za vrednotenje, ko so le-ti na voljo.

D 1.2. Komponente sistema za začetno overjanje

Sistem za začetno overjanje je sestavljen iz naslednjih komponent:
- komponente za varno overjanja podpisa,
- vmesnika za vnos podpisnikovega dokumenta in izbiro podpisa za overjanje (za primer več podpisov),
- vmesnika za prikaz podpisnikovega dokumenta v pravem formatu,
- vmesnika za prikaz podatkov o podpisniku in podatkov o izhodnem statusu začetnega overjanja,
- vmesnika za pridobitev elektronskega podpisa z dodatnimi podatki za vrednotenje,
- vmesnika za vpis varne revizijske sledi (opcijsko),
- mrežnega vmesnika za pridobitev podatkov od TSP-jev (CRL, OCSP, CA, TSA),
- vmesnika za pridobitev definicije Politike podpisa (opcijsko za primer, da sistem ne podpira dinamčno programibilne politike podpisa).



D 2. Postopek overjanja - običajno overjanje

Opravlja se lahko leta po elektronskem podpisu dokumenta. Za tovrstno overjanje naj ne bi bil potreben zajem dodatnih podatkov, kot so bili zajeti pri začetnem overjanju.

Običajno overjanje zahteva po eni strani sistem za obdelavo politike e-podpisa (implicitne ali eksplicitne) ter po drugi strani:

- podpisnikov dokument,
- e-podpis podpisnikovega dokumenta,
- dodatne podatke, povezane s podpisom (podatki za vrednotenje).

Podatki za vrednotenje (angl. *validation data*) pa morajo biti v primeru običajnega overjanja že na voljo, saj so priskrbljeni z začetnim overjanjem. S podatki za vrednotenje lahko med drugim dokažemo, da je bil podpis kreiran dokler je bilo potrdilo še veljavno. To lahko naredimo na dva načina:

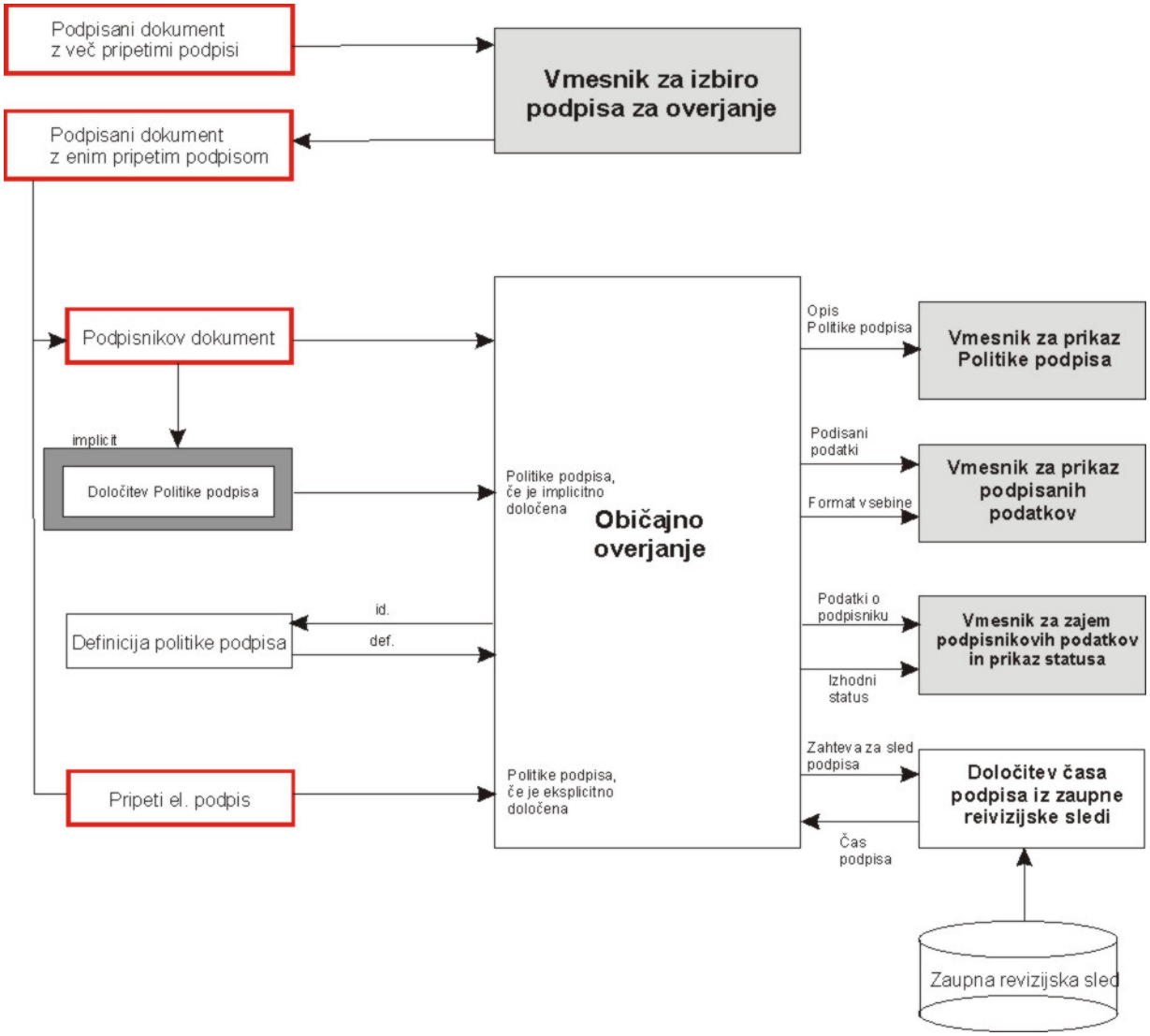
- s časovnim žigom,
- preko varne "revizijske sledi" (angl. *audit trail*), v kateri sta zapisani vsaj časovna oznaka in e-podpis.

D 2.1. Izhodni statusi običajnega overjanja

Običajno overjanje nam vrne naslednje rezultate:

- USPEŠNO kar pomeni, da je e-podpis veljaven in v skladu s politiko za overjanje podpisa,
- NEUSPEŠNO, kar pomeni, da e-podpis ni v skladu s politiko za overjanje podpisa.

D 2.2. Prikaz komponent sistema za običajno overjanje



D 3. Pravila za overjanje

Z določitvijo zahtev za podpisnika in overitelja lahko jasno definiramo odgovornosti obeh strank z namenom, da izvedemo zanesljivo overjanje.

E-podpis je veljaven, ko:

- vsebuje minimalno število elementov, da lahko izvedemo začetno overjanje,
- so na voljo ustrezni podatki za overjanje (dodatni cert., CRLji, OCSP odgovori, TS, TM),

- overjanje izvede "zaupanja vreden" (angl. *trusted*) sistem za overjanje.

Naslednja pravila predstavljajo minimalni nabor preverjanj.

D 3.1. Pravila za preverjanje podpisnikovega potrdila

V primeru uporabe kvalificiranega potrdila je potrebno preveriti ali to ustreza zahtevam iz Direktive 1999/93/EC oz. iz ZEPEP-a. Preveriti je potrebno ali je Politika za kvalificirana potrdila pravilno označena v potrdilu in ali jasno navaja, da gre za namensko izdajo kvalificiranega potrdila.

D 3.2. Pravila za preverjanje overitvene poti

CWA 14171:2001 str. 20-21.

D 3.3. Pravila za uporabo RSI (Revocation Status Information)

V postopku overjanja mora oseba ali sistem, ki izvaja overjanje, preveriti ali je lastnik potrdila tudi oseba, ki je imela zasebni ključ v času podpisa. Ker obstaja neizbežna časovna razlika med izgubo oz. kompromitiranjem ključa/potrdila in objavo njegovega preklica, je v Politiko za overjanje podpisa vpeljano prehodno obdobje. S tem določimo čas po katerem lahko z gotovostjo trdimo, da je bil podpis res veljaven. Oseba, ki overja podpis lahko počaka do preteka tega obdobja preden si priskrbi podatke o preklicu. Politika za overjanje podpisa lahko določi tako obdobje:.

Primer. Overitelj mora biti posebno pozoren v naslednji situaciji:
- v času 1 podpisnik podpiše dokument,
- e-podpisu je dodan časovni žig v času 2, ki je za časom 1,
- Času 2 dodamo prehodno obdobje, ki se konča ob času 3,
- potrdilo je preklicano ob času 4, ki je lahko pred ali po času 3,
- e-podpis je prvič overjen ob času 5, ki ne sme biti pred časom 3.

Če je potrdilo preklicano pred časom 3, potem e-podpisa ne moremo overiti. Če je potrdilo preklicano po času 3, potem e-podpis lahko overimo. V primeru, da oseba, ki overja podpis nima dokaza o tem ali je bil e-podpisu dodan časovni žig, potem e-podpis ne moremo overiti.

D 3.4. Pravila za uporabo časovnega žiga ali časovne oznake

Med časom podpisa in časovnim žigom je vedno časovna razlika. Čim daljša je časovna razlika, večja je nevarnost, da je podpis neveljaven zaradi kompromitiranja ali namernega preklica privatnih ključev s strani podpisnika. Politika podpisa naj bi predpisala **maksimalno sprejemljivo časovno razliko** med časom podpisa in časovnim žigom. Če taka časovna razlika ni predpisana, potem mora biti elektronski podpis časovno žigosan najkasneje tik pred potekom potrdila. V primeru uporabe časovne oznake, mora biti elektronski podpis zapisan v varni »revizijski sledi« (angl. *audit trail*).

D 3.5. Pravila za algoritme in dolžine ključev

Politika za overjanje podpisa lahko predpiše nabor algoritmov in minimalno dolžino ključev, ki se lahko uporabijo.

D 4. Komponente overjanja glede na subjekt, ki overja podpis

D 4.1. Overjanje podpisa s strani osebe

Za overjanje podpisa s strani **osebe**, morajo biti pripravljeni naslednji vmesniki:

- Vmesnik za izbiro e-podpisa za overjanje (če je dokumentu dodanih več podpisov),
- Vmesnik za prikaz opisa Politike podpisa, ki je uporabljena ob podpisu,
- Vmesnik za prikaz podpisnikovega dokumenta (koncept WIPIWIS *angl.* **W**hat **I**s **P**resented **I**s **W**hat **I**s **S**igned),
- Vmesnik za prikaz informacij o podpisniku in izhodnem statusu (ime ali psevdonim, ki se ga pridobi iz razločevalnega imena, ime CSP (politike delovanja overitelja), čas in datum podpisa, Statusi: overjanje uspešno, overjanje neuspešno, overjanje nepopolno)
- Vmesnik za pridobitev podatkov za overjanje (če je rezultat overjanja nepopoln, potem se tu vpiše dodatne podatke),
- Vmesnik z običajnimi uporabniškimi zahtevami (prikaz neuspešnih stvari rdeč, uspešnih: zelen, ipd.)

D 4.2. Overjanje podpisa s strani strežnika (informacijskega sistema)

Za overjanje s strani sistema sta v grobem potrebni dve vrsti API-jev:

- za pridobitev informacij, ki so vsebovane v elektronskem podpisu,
- za overjanje elektronskega podpisa in pridobitev podatkov za overjanje

D 5. Prikaz komponent sistema za arhiviranje podpisa

E. PRIPOROČILA UPORABE KRIPTOGRAFSKIH ALGORITMOV

V aplikacijah uporabljamo tri osnovne vrste algoritmov:
1. zgoščevalne funkcije,
2. asimetrične algoritme za podpisovanje in izmenjavo ključev ter
3. simetrične za šifriranje.

E 1. Zgoščevalne funkcije

- SHA-1 v skladu z NIST FIPS PUB 180-1: Secure Hash Standard, april 1995
- MD5 v skladu z RFC 1321 (Rivest, R., "The MD5 Message-Digest Algorithm", april 1992)
- ripemd-160 (http://www.esat.kuleuven.ac.be/~cosicart/pdf/AB-9601/)

Priporočamo uporabo SHA-1 ali ripemd-160. To je v skladu z priporočilom ETSI SR 002 176 V1.1.1, poglavje 4.3.

E 2. Algoritmi za šifriranje (simetrični algoritmi)

- DES (Data Encryption Standard v skladu z U.S. FIPS PUB 46-2 in ANSI X3.92.
- Trojni-DES v skladu z FIPS PUB 46-3
- CAST v skladu z RFC 2144: »The CAST-128 Encryption Algorithm«, C. Adams, maj 1997
- RC2 v skladu z RFC 2268: » Description of the RC2(r) Encryption Algorithm«", R. Rivest, marec 1998
- AES oziroma Rijndael v skladu z NIST FIPS Pub197: Advanced Encryption Standard (AES), 26 november 2001
- RC4 za uporabo v protokolu TLS (RC4 je tekoči simetrični algoritem, ki ga je razvil R.Rivest 1987, zakonsko zaščitila organizacija RSA Data Security, anonimno objavljen na internetu 1994)

Dokler se ne bo uveljavil algoritem AES, priporočamo uporabo algoritma trojni-DES (angl. Triple DES).

Pri šifriranju z bločnimi simetričnimi algoritmi (to so vsi zgoraj navedeni razen RC4) je treba uporabiti tisti način povezovanja blokov (confidentiality modes of operation), ki je najbolj primeren za aplikacijo:

- Triple Data Encryption Algorithm modes of operation - ANSI X9.52
- DES, CAST, RC2 and Triple-DES encryption using CBC mode of operation in accordance with FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116
- Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," NIST Special Publication 800-38A, december 2001.

Priporočil ETSI za simetrične algoritme še ni, verjetno pa bodo vključena v bodoče verzije ETSI SR 002 176.

E 3. Asimetrični algoritmi

- Diffie-Hellman v skladu z X9.42 (RFC 2631)
- RSA v skladu z PKCS #1 v2.1 (RFC 3447)
- ElGamal – definicija v "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *Advances in Cryptology - CRYPTO '84*, str. 10-18, Springer-Verlag, 1985
- Eliptični algoritmi ECC (angl. *Elliptic curve cryptosystems*)- RFC 3278 za šifriranje sporočil

Pri implementaciji algoritmov nam je v pomoč priporočilo ETSI SR 002 176 V1.1.1, ki natančno določa zahteve za generiranje ključev in parametrov za vsak posamezni algoritem (generiranje naključnega števila in praštevil).

E 4. Algoritmi za digitalno podpisovanje

Algoritmi za digitalno podpisovanje morajo biti v skladu z DSS (Digital Signature Standard) - NIST FIPS Pub 186-2 (januar 2000), ki vključuje algoritme

- DSA – opis je vključen v NIST FIPS Pub 186-2
- RSA v skladu z ANSI X9.31 in ISO/IEC 14888-3 (1999)
- ECDSA v skladu z ANSI X9.62-1998 (Elliptic Curve Digital Signature Algorithm)

Priporočilo ETSI SR 002 176 V1.1.1 vsebuje poleg zahtev za generiranje ključev in parametrov za vsak posamezni algoritem tudi navodila za dodajanje bitov do zahtevane dolžine bloka (padding method) pri zgoščevalnih funkcijah, kar je v navedenem dokumentu povzeto v tabeli 1 na strani 9 (The list of approved signature suites).

E 5. Priporočila, ki urejajo načine implementacije algoritmov:

- CMS (Cryptographic Message Syntax)
  - RFC 3369 Cryptographic Message Syntax
  - RFC 3370 CMS Algorithms
  - RFC 3278 – Use of ECC Algorithms in CMS
- TLS 1.0 – RFC 2246 (v pripravi TLS 1.1), http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-02.txt
- IPsec – RFC 2401 in RFC na strani http://www.ietf.org/html.charters/ipsec-charter.html
- S/MIME - RFC 2631 do 2634 in povezani RFC na strani http://www.ietf.org/html.charters/smime-charter.html
- XML: XML Encryption Syntax and Processing (W3C, 10.december 2002) http://www.w3.org/TR/xmlenc-core/2002/REC-xmlenc-core-20021210/