UNIVERZA V LJUBLJANI
Fakulteta za Računalništvo in Informatiko
Tržaška 25,
Ljubljana

RAČUNALNIŠKA VARNOST IN KRIPTOGAFIJA

PROJEKT

»Standard XAdES in zakonodaja«

Boris Glavić
VŠ: 24012842

Ljubljana, 15.12.2004

Kazalo

Povzetek

V projektni nalogi bo opisano področje digitalnega podpisa, načini njegove implementacije s pomočjo dokumentov XML, osnove časovnega žiga, in pravna podlaga, ki ureja področje digitalnega podpisa. Glede na pomembnost XMLa v elektronskem poslovanju, in potrebo po standardu, ki bi omogočal elektronsko podpisovanje, pojavila se je ideja za razvoj standarda za elektronsko poslovanje v obliki dokumentov XML. Specifikacijo standarda *XML Advanced Electronic Signatures (XAdES)* so razvili v European Telecommunications Standard Institute (ETSI). Standard XAdES zadošča zahtevam Zakona elektronskem poslovanju o elektronskem podpisu (ZEPEP [6]) in direktivam Evropske unije ([7], [8]). Dodatno onemogoča zanikanje podpisa in omogoča dolgoročno veljavnost.

1. Uvod

Elektronsko poslovanje in digitalni podpis

Računalniška industrija se že vrsto let prizadeva doseči popolnoma elektronsko poslovanje. Končni cilj je zamenjati uporabo papirja in papirnih dokumentov z elektronskimi sredstvi. Čeprav je bil dosežen veliki napredek, določeni dokumenti se še vedno v večini primerov hranijo v papirni obliki. Razlog za to je da so zakoni izrecno zahtevali uporabo lastnoročnih podpisov, kar v računalništvu ni mogoče. Šele v zadnjih letih se je to začelo spreminjati. V zakonodajo so bile dodane odredbe, ki omogočajo uporabo digitalnih dokumentov, tudi v primeru da so prej izrecno zahtevali papirne.

V primerjavi s papirnimi, digitalni dokumenti imajo nekaj prednosti in pomanjkljivosti. Dokumente v digitalni obliki lažje hitro prenašamo, in učinkovito hranimo. Po drugi strani je veliko težje ugotoviti spreminjanje takšnih dokumentov, kot tistih v papirni obliki.

Za to da dosežemo enakopravnost digitalnega in papirnega poslovanja, moramo v digitalnem svetu imeti mehanizem, ki je enakovreden lastnoročnem podpisu. Na srečo tak mehanizem obstaja. Dokumente tudi v digitalnem svetu lahko podpisujemo, le da se lastnosti digitalnega podpisa razlikujejo od lastnosti lastnoročnega podpisa (v vsebini in ne v pravni veljavi).

Kdo uporablja digitalni podpis? Po sprejetju zakona o elektronskem poslovanju in elektronskem podpisu število storitev, ki v svojem delovanju uporabljajo digitalni podpis, raste. Začelo se je pri bankah, ki so želele svoje storitve ponuditi preko spleta. Kmalu za tem je svoje storitve preko interneta začela ponujati tudi država. Trenuten seznam storitev, ki uporabljajo digitalni podpis je:

- e-davki,
- e-upravne zadeve,
- e-zaposlitve,
- e-demokracija,
- vodniki e-uprave,
- ISPO - Informacijski servis podatkov,
- VLOP - Vpogled v lastne osebne podatke,
- portal upravnih enot,
- vodnik po upravnih storitvah,
- upravne storitve - zbirka obrazcev,

- javne objave (prodaja zemljišč),
- interaktivni atlas,
- vpogledovalnik v zbirke geodetskih podatkov.

Število tovrstnih storitev bo samo naraščalo, ker se je država zavezala da bo vse svoje storitve ponudila tudi po elektronski poti.

Jezik XML (eXtensible Markup Language)

XML je jezik za opis dokumentov, ki vsebujejo strukturirane informacije. Strukturirani dokumenti vsebujejo tako besedilo, slike, kot informacijo o tem kakšno vlogo ima ta informacija. Skoraj vsi dokumenti imajo določeno strukturo.

Jezik XML je definiran prav z namenom da omogoči standardni način dodajanja oznak strukture dokumentov. Čeprav obstajajo tudi drugi podobni jeziki kot so HTML in SGML, v poslovnih aplikacijah večinoma uporabljamo jezik XML. Razlog za to je da je HTML vnaprej definiran, in ga ne moremo spreminjati, SGML pa je preobsežen in njegova popolna implementacija je zapletena, težka in draga. Jezik XML po drugi strani omogoča spreminjanje vsebine oznak, in ni tako obsežen kot SGML.

Število aplikacij, ki trenutno uporabljajo jezik XML je ogromno, in še narašča. Za naše potrebe beseda »dokument« ne označuje samo tradicionalne dokumente, kot je ta, pač pa tudi množico drugih XML »podatkovnih formatov«. Ti lahko vsebujejo vektorsko grafiko, transakcije v e-poslovanju, digitalne podpise, matematične enačbe, podatke o objektih, ukaze strežnikom, in tisoče drugih stvari.

Glede na pomembnost jezika XML v elektronskem poslovanju, in potrebo po standardu, ki bi omogočal elektronsko podpisovanje, razvila se je ideja za razvoj standarda za elektronsko poslovanje v obliki XML. Specifikacijo standarda »*XML Advanced Electronic Signatures (XAdES)«* so razvili v European Telecommunications Standard Institute (ETSI). Standard XAdES zadošča zahtevam Zakona elektronskem poslovanju o elektronskem podpisu (ZEPEP [6]) in direktivam Evropske unije. Dodatno onemogoča zanikanje podpisa in omogoča dolgoročno veljavnost.

Kateri izraz uporabiti - elektronski ali digitalni podpis?

Elektronski podpis je pravni izraz, ki pomeni podpis nečesa v elektronski obliki. Podpisnik se identificira in potrjuje podpisane podatke, in pod določenimi pogoji je zamenjava za lastnoročni podpis. Pogoji, pod katerimi je elektronski podpis enakovreden lastnoročnem, so opisani v poglavju 5. **Digitalni** podpis je zelo primeren tehnični način izvedbe elektronskega podpisa. Zagotavlja

- celovitost podpisanih podatkov (nič ne manjka, niso spremenjeni),
- identiteto in avtentičnost podpisnika,
- nezmožnost zanikanja (v povezavi s časovnim žigom in kriptografijo javnih ključev – PKI [9]), in
- arhivsko vrednost - ohranjena potrditev avtentičnosti podpisnika (časovni žig+PKI) in celovitost podpisanih podatkov ali transakcije skozi čas.

Kateri izraz uporabiti?

- Če želimo poudariti pravno vlogo podpisa, usklajenost z zakonodajo, in/ali vlogo podpisa v poslovnem procesu, uporabimo izraz elektronski podpis.
- Če želimo poudariti tehnične lastnosti podpisovanja, uporabimo izraz digitalni podpis.

Organizacija projektne naloge

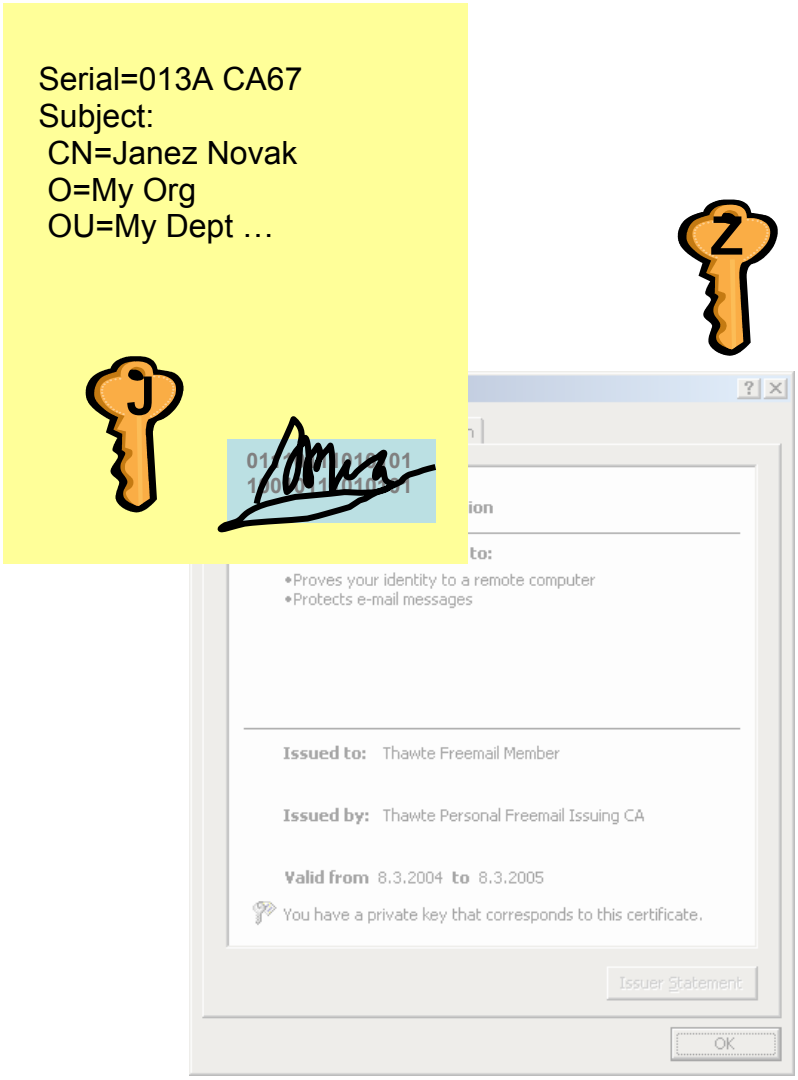
Poglavje 1 definira osnovne pojme katere uporabljamo v dokumentu, poda kratek zgodovinski okvir razvoja, in opis postopka digitalnega podpisa namenjen bralcu, ki ga tehnične podrobnosti ne zanimajo. V nadaljevanju opisujemo konkretni implementaciji sistemov, ki temeljita na dokumentih XML (standard XMLDSig - poglavje 2, in njegovi razširitvi standardu XAdES - poglavje 3). Ker standard XAdES veliko uporablja tehniko časovnega žiga, poglavje 4 poda osnovne definicije, možne načine izvedbe, in pregled dostopnih agencij za časovno žigosanje v Sloveniji. Poglavje 5 vsebuje povzetek Slovenske i Evropske zakonodaje, ki so povezani s področjem elektronskega poslovanja in z digitalnim podpisom (Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP, in priporočila Evropske skupnosti).

2. Izvedba digitalnega podpisa

Za izvedbo digitalnega podpisa uporabljamo asimetrično kriptografijo javnih ključev (PKI – Public Key Infrastructure). Infrastruktura javnih ključev, ki jo sestavljajo izdajatelji digitalnih potrdil (Certification authorities - CA), certifikati, imeniki, aplikacije, podpisne politike, in postopki. Certifikati ali digitalna potrdila so “Potrjeni” – digitalno podpisani - javni ključi in identifikacijski podatki, ki jih potrdi CA (= overitelj). Veljavnost digitalnega potrdila je omejena na določeno časovno obdobje. Tehnični razlog za to je zmanjševanje časovnega okna za izračun zasebnega ključa. Komercialni razlog pa je poslovni model trženja certifikatov kot letni, ali več-letni najem. Za preklic digitalnega potrdila lahko uporabimo eno izmed standardov:

- CRL – Certificate Revocation List [10],
- OCSP – Online Certificate Status Protocol, ali
- CRT – CR Tree.

Slika 1.1 prikazuje shematsko zgradbo certifikata.



Slika 1.1 shematska zgradba certifikata

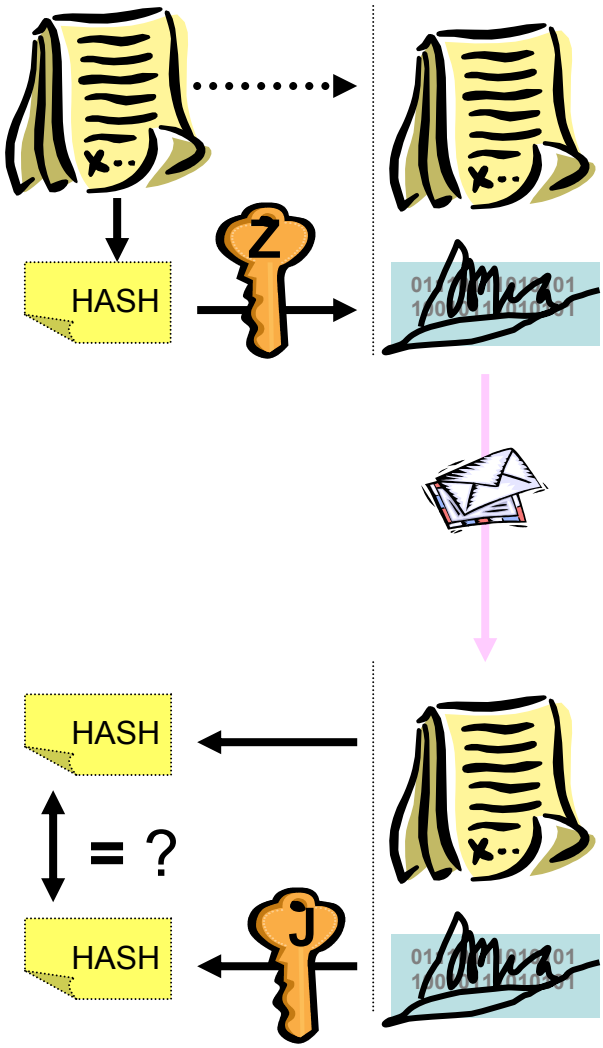
Za sam podpis je potrebno narediti naslednje korake:

- izračun zgostitvene (hash) funkcije nad podatki [9],
- šifriranje rezultata z zasebnim ključem podpisnika.

Pri preverjanju podpisov je potrebno:

- odšifriranje podpisa z javnim ključem podpisnika,
- izračun zgostitvene funkcije nad podatki,
- primerjava izračunane vrednosti zgoščvalne funkcije z vrednostjo zapisano v podpisu.

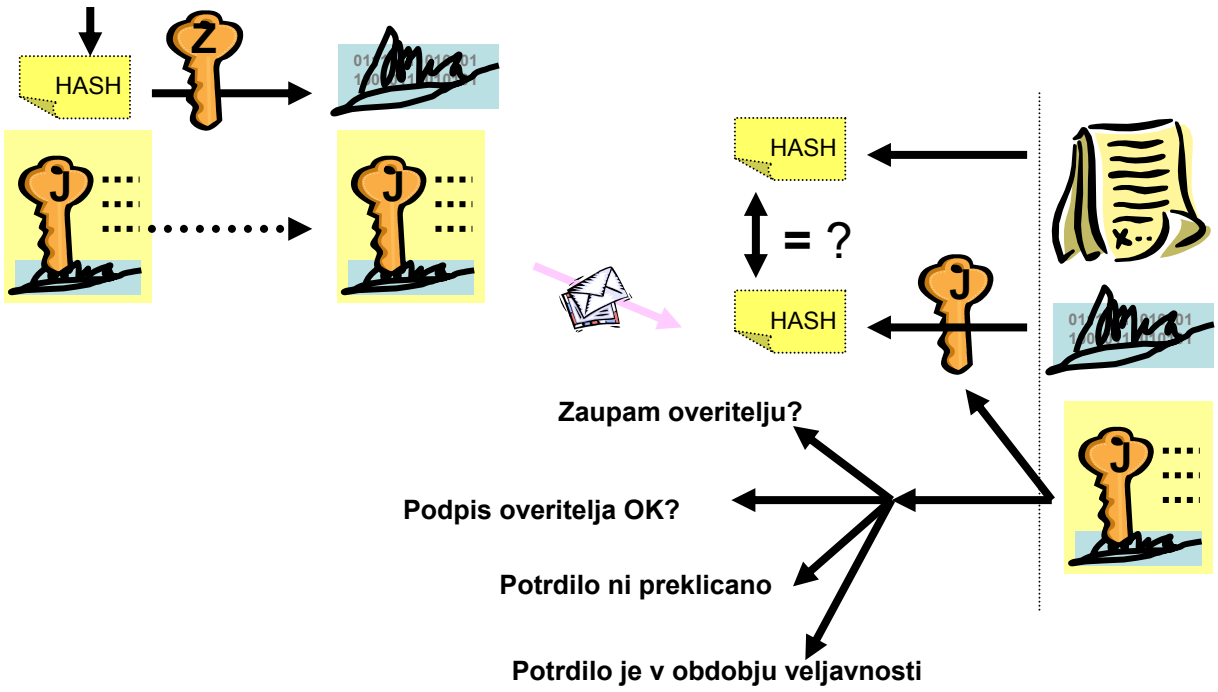
Celotni potek podpisovanja in preverjanja podpisa je prikazan na sliki 1.2.



Slika 1.2 potek podpisovanja in preverjanja podpisa

Pri elektronskem podpisu z digitalnim potrdilom, digitalno potrdilo navadno priložimo podpisu in podatkom. Dodatno pri preverjanju veljavnosti potrdila preverimo še (slika 1.3):

- zaupanje overitelju,
- veljavnost podpisa overitelja,
- preklic potrdila,
- obdobje veljavnosti, in opcijsko
- (namen potrdila).



Slika 1.3 dodatna preverjanja pri podpisu

3. Standard XMLDSig

Ključna lastnost podpisov v standardu XMLDSig je da je sam podpis zapisan v obliki dokumenta XML. Podatki, ki jih podpisujemo niso nujno v obliki XML. En podpis lahko podpiše več dokumentov. Standard XMLDSig omogoča podpis vseh podatkov, ki so dostopni preko naslovov v obliki URI (Uniorm Resource Interface), ali pa jih dobimo iz URI-a s pomočjo algoritmičnih transformacij. Razlikujemo tri tipe podpisov XMLDSig glede na pozicijo podpisa in podatkov:

- vsebujoč podpis (enveloping signature),
- vsebovan podpis (enveloped signature), in
- ločen podpis (detached signature).

Vsebujoč podpis vsebuje vse podatkovne objekte znotraj XMLDSig strukture. **Vsebovan** podpis je tak podpis pri katerem sam podpis pripnemo podatkovnim objektom, ki jih podpisujemo.

Pri **ločenem** podpisu pa podatkovne objekte, ki jih podpisujemo in sam podpis hranimo v ločenih dokumentih. V izjemnem primeru se lahko zgodi da je, ker XMLDSig podpis lahko podpisuje več podatkovnih objektov, podpis hkrati vsebujoč, vsebovan in ločen.

Ker za podpis uporabljamo strukturo XML, je način kako podpis organiziramo izredno pomemben. Najbolj razširjeni in najbolj naraven način predstavitve dokumenta XML v računalniškem spominu je drevesna struktura. Strukturo sestavljajo koren in podrejena vozlišča, ki imajo enega nadrejenega, in poljubno število podrejenih vozlišč. Ker predstavitev v drevesni strukturi ni enolična (vrstni red vozlišč ni vnaprej določen), je možnih variacij veliko. Lahko se zgodi da v praksi vsaka implementacija jezika XML zgradi drevo malo drugače. Ker pri digitalnem podpisu uporabljamo zgoščevalne funkcije za preverjanje sprememb podpisanih dokumentov, je ta vrstni red izredno pomemben. V primeru da dve implementaciji jezika XML vzamejo isti dokument in na osnovi drevesne strukture izračunajo

zgoščeno vrednost, dobijo dve različne vrednosti za enaka dokumenta. Da se temu izognemo, moramo zagotoviti da vse implementacije jezika XML iz dokumenta zgradijo identično drevo. Le na ta način bodo zgoščene vrednosti enakih dokumentov enake.

Taki obliki dokumentov XML rečemo kanonična oblika. Dobimo je s postopkom kanonizacije (angl. Canonicalization method). Več o kreiranju kanonične oblike lahko preberete na [3].

XML naslovni prostor (angl. namespace) trenutne verzije standarda XMLDSig je http://www.w3.org/2000/09/xmldsig. Vozlišče <*Signature*> vsebuje naslednje elemente:

- <*SignedInfo*> podpisane podatkovne objekte, metode, uporabljene algoritme za kanonizacijo in podpisovanje, in reference na podpisane objekte (URI)
- <*SignatureValue*> izračunana vrednost podpisa
- (Opcijski) <*KeyInfo*> podatki o ključu uporabljenem za podpis in ključu, ki ga moramo uporabiti za verifikacijo
- (Opcijski) <*Object*> dodatni podatki o podpisu, in vsebina podpisanih dokumentov (če podatke shranjujemo skupaj s podpisom)

Podpisovanje

Kreiranje podpisa sestavljata dva koraka. Prvo moramo kreirati vozlišče ali vozlišča <*Reference*>. Za tem je pa potrebno kreirati vozlišče <*SignedInfo*>, ki mora biti kanonizirano in podpisano.

Kreiranje referenc

Za kreiranje vsakega vozlišča <*Reference*> je potrebno:

1. dobiti podatke preko danega URI-a,
2. uporabiti vse transformacije, ki so definirane v vozlišču <*Transform*>,
3. izračunati vrednost zgostitvene funkcije nad podatki dobljeni v koraku 2,
4. kreirati vozlišče <*Reference*> iz dobljenih podatkov.

Kreiranje podpisa

Kreiranje podpisa poteka na naslednji način:

1. kreiranje elementa <*SignedInfo*>,
2. uporaba kanonizacijske metode nad vozliščem <*SignedInfo*>,
3. izračun vrednosti podpisa iz rezultata koraka 2 iz ključa, ki ga uporabljamo za podpis,
4. kreiranje vozlišč <*SignatureValue*> in <*Signature*>.

Preverjanje podpisov

Tako kot proces podpisovanja, tudi proces preverjanja XMLDSig podpisov sestavljata dva koraka – preverjanje podpisa in preverjanje referenc.

- Preverjanje podpisa
  1. Priprava ključa za preverjanje podpisa.
  2. uporaba algoritma za kanonizacijo definiranega v vozlišču <*CanonicalizationMethod*> nad vozliščem <*SignedInfo*>,
  3. uporaba ključa za preverjanje podpisa in rezultata koraka 2 za verifikacijo podpisa.

- Preverjanje referenc nam potrjuje da so podatki bili zares podpisani na osnovi zgoščenih vrednosti zapisanih v vozlišču <*Reference*>. Za preverjanje referenc v vozlišču <*SignedInfo*> potrebujemo naslednje korake:
  1. Branje podatkov, ki smo jih uporabili za kreiranje referenc,
  2. izračun njihove zgoščene vrednosti s pomočjo metode navedene v vozlišču <*DigestMethod*>, in
  3. primerjavo dobljene zgoščene vrednosti s tisto, ki je shranjena v ustreznem vozlišču <*DigestValue*>.

XMLDSig podpis je veljaven le v primeru da so vse vrednosti podpisa in zgoščene vrednosti vseh vsebovanih referenc, ki jih izračunamo sami, enake vrednostim zapisanim v podpisu.

4. Standard XAdES

Kratica XAdES je okrajšava za »XML Advanced Electronic Signatures«. Sam standard XAdES je nadgradnja standarda XMLDSig, ki specificira kako omogočimo dolgoročno veljavnost in onemogočimo zanikanje elektronskega podpisa. Zadošča zahtevam za napredni digitalni podpis (Advanced digital signature) in vsebuje 7 nivojev XAdES podpisov:

- XAdES (osnovni nivo)
- XAdES-T (Time stamped)
- XAdES-C (Complete)
- XAdES-X (eXtended)
- XAdES-X-T (eXtended long-Term)
- XAdES-A (Archival)

Vsak nivo je nadgradnja predhodnega, in zato vsebuje se elemente iz prejšnjih nivojev. Shematski prikaz XAdES hierarhije je prikazan na sliki 3.1.

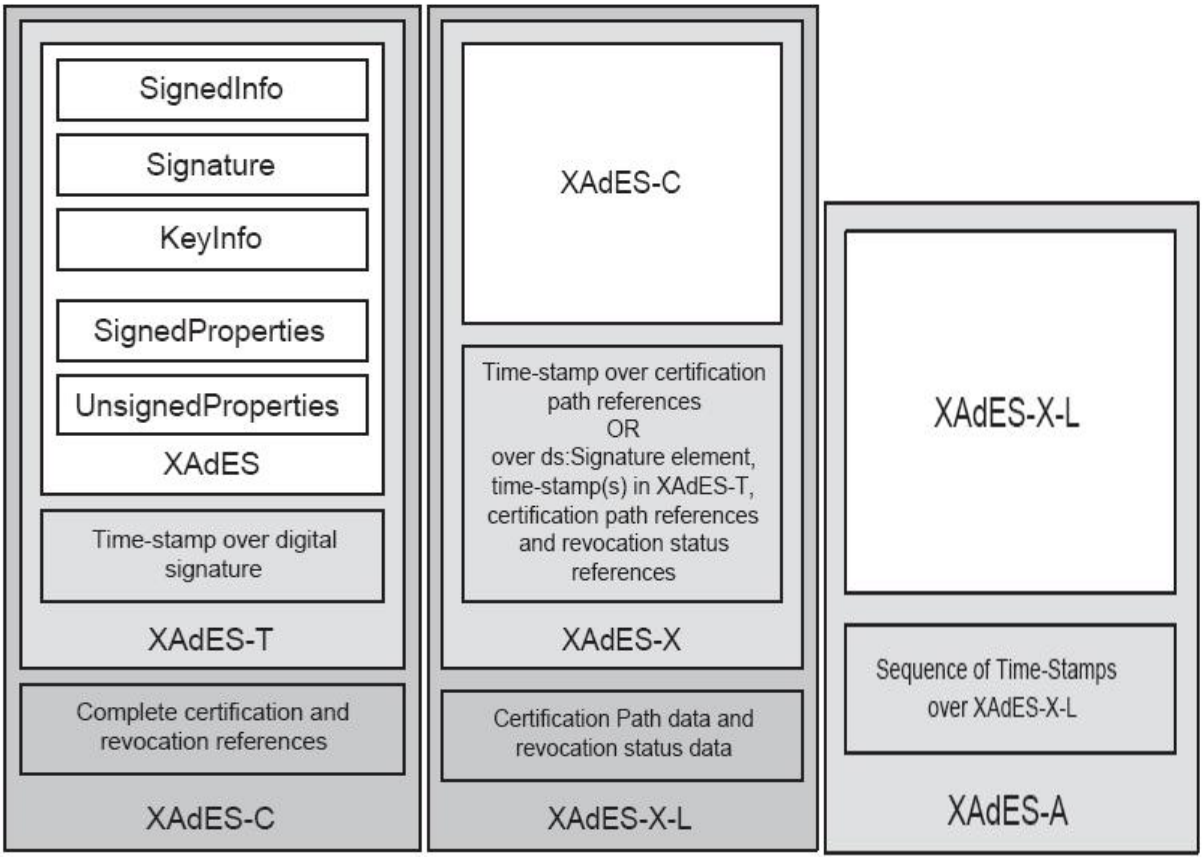
XAdES (Osnovni nivo)

XMLDSig dokumentom doda informacije, ki bolje opisujejo podpisani objekt**.** Vsebuje obvezne in opcijske elemente**.** Obvezni elementi so:

- Čas podpisa
- Referenca na certifikat, ki vsebuje privatni ključ s katerim je objekt podpisan
- Referenca na “Politiko elektronskega podpisovanja”

Opcijski elementi:

- Lokacija na kateri je podpis nastal
- Vloga v kateri je nastal podpis
- Dodatne informacije o formatu in tipu podpisanega objekta
- Časovne žige za nekatere, ali vse objekte
- Dodatne informacije o obveznostih, ki jih s podpisom prevzamemo



Slika 3.1 Nivoji standarda XAdES

XAdES-T (Time-stamped)

- XAdES-T = XAdES + Časovni žig čez podpis

Da bo podpis veljaven, mora biti narejen znotraj časovnega intervala veljavnosti vseh certifikatov, ki sestavljajo certifikatsko verigo certifikata s katerim podpisujemo. Po drugi strani ni sprejemljivo da postane podpis neveljaven ko eden od certifikatov v verigi poteče, ali je preklican. Zaradi tega je čas podpisa zelo pomemben.

Način da dokažemo da je neki podatek (npr. podpis) obstajal pred določenim časom, je da ga opremimo z časovnim žigom. Bolj detajlen opis časovnega žigosanja je opisan v poglavju 4. Pri uporabi časovnega žiga je pomembno opozoriti da podatkov ne moremo podpisati off-line, oziroma takrat ko ni dostopen overitelj časovnega žiga (Time-stamp authority - TSA). Priporočljivo je časovno žigosati podpis v čim krajšem času po kreiranju podpisa. Dodatno lahko v politiki podpisovanja določimo časovni interval, znotraj katerega mora biti izdan časovni žig za podpis, da bo ta veljaven.

XAdES-C (Complete)

- XAdES-C = XAdES-T + reference na vse podatke potrebne za preverjanje veljavnosti podpisa

Za dolgoročno veljavnost podpisa moramo arhivirati vse podatke, ki smo jih uporabili pri preverjanje podpisa za potrebe morebitnih arbitraž. Podatke, ki moramo shraniti vsebujejo celotno certifikatsko verigo, od certifikata s privatnim ključem katerega smo uporabili za podpisovanje, certifikata certifikatske agencije (CA) znotraj katere je bil izdan do zaupanega overitelja, ter podatke o preklicu za te certifikate. Te podatke lahko shranimo znotraj podpisa, ali pa na ločeno lokacijo pod kontrolo

tistega, ki preverja podpis. Če podatke o certifikatih in preklicne liste hranimo zunaj podpisa, v podpis moramo dodati reference na te objekte da nedvoumno določimo podatke, ki smo jih uporabili pri preverjanju podpisa. Za to sta namenjena vozlišča <*CompleteCertificateRefs*> in <*CompleteRevocationRefs*>, ki omogočata da shranimo reference na potrebne objekte.

XAdES-X (eXtended)

- XAdES-X = XAdES-C + časovni žig čez celotno XAdES-C strukturo, ali
- XAdES-X = XAdES-C + časovni žig čez reference na certifikacijsko pot in podatke o preklicu

V primeru da se zgodi da postane privaten ključ enega od overiteljskih agencij v certifikatski verigi kompromitiran, podatkom tega overitelja ne moremo več zaupati. Da zaščitimo veljavnost podpisa v tem primeru, moramo časovno žigosati vse podatke o certifikatih in njihovem preklicu (certificate revocation list - CRL) zato da lahko dokažemo da so podatki, ki jih uporabljamo obstajali pred časom ko je privatni ključ postal kompromitiran.

XAdES-X omogoča dva načina da to naredimo:

- časovni žig nad podpisom in vsemi podatki o certifikatih in njihovih preklicih, kar shranimo v vozlišču <*SigAndRefsTimeStamp*>, ali
- časovni žig le nad vsemi podatki o certifikatih in njihovih preklicih, kar shranimo v vozlišču <*RefsOnlyTimeStamp*>

Če želimo obdelati več podpisov, ki uporabljajo skupni nabor certifikatov, potem je bolje uporabljati drugo metodo ker v tem primeru zahtevane podatke lahko pridobimo samo enkrat, in jih lahko uporabimo za več podpisov.

V enem podpisu lahko shranimo več časovnih žigov, različnih overiteljev za podatke o cretifikatih in njihovem preklicu. Moramo se pa zavedati da standard XAdES ne dovoljuje mešanja vozlišč <*SignAndRefsTimeStamps*> in <*RefsOnlyTimeStamps*>. Moramo se odločiti na uporabo ene izmed njih.

XAdES-X-L(eXtended Long-term)

- XAdES-X-L = XAdES-X + vsi podatki potrebni za preverjanje podpisa

V primeru arbitraže, uporabnik ki podpis preverja mora priložiti vse certifikate uporabljene v procesu preverjanja podpisa in ustrezne podatke o njihovem preklicu. Ker po določenem času vsi podatki niso več dostopni, mora obstajati način da se le-ti shranijo v priročen arhiv - nivo XAdES-X-L omogoča prav to.

Vsak certifikat v certifikatski verigi—oziroma vsak certifikat vsebovan v vozlišču <*CompleteCertificateRefs*> mora biti shranjen v vozlišču <*KeyInfo*> XMLDSig podpisa, ali pa v vozlišču <*CertificateValues*>.

Podobno podatki o preklicu vseh certifikatov v certifikatski verigi—oz. vseh certifikatov vsebovanih v vozlišču <*CompleteRevocationRefs*> morajo biti vsebovani v vozlišču <*RevocationValues*>.

XAdES-A (Archival)

Omogoča preverjanje veljavnosti podpisa tudi v primeru potencialnih “padcev” kriptografskih algoritmov.

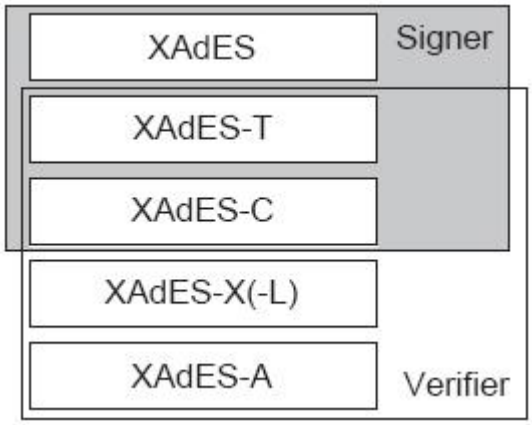
- XAdES-A = XAdES-X-L + časovni žig čez arhivske validacijske podatke

V prihodnosti se lahko pokažejo tudi slabosti pri kriptografskih, in/ali zgostitvenih algoritmih, ki smo jih uporabili za izdelavo podpisa. Zaradi napredka v računalništvu, čas potreben za kriptoanalizo in izboljšave tehnik za kriptoanalizo povečujejo verjetnost zloma kriptografskih algoritmov uporabljenih ključev. Preden se takšna situacija zgodi, kontrolor podpisa mora zagotoviti mere da lahko ohrani veljavnost podpisov. Obstaja več načinov kako je to mogoče narediti, glede na lastnosti ogroženih algoritmov. Nivo XAdES-A uporablja enostaven vendar učinkovit pristop “arhiviranja podatkov za preverjanje”. Arhiviramo vse podatke potrebne za preverjanje podpisa, in jih časovno žigošemo skupaj s podpisom. Na ta način lahko dokažemo da je podpis bil preverjen v času ko so uporabljeni algoritmi veljali za varne.

Če ne moremo zagotoviti da kriptografski algoritmi in zgostitvene funkcije uporabljene s strani overitelja časovnih žigov ostanejo varni, moramo uporabiti gnezdene časovne žige čez celotno strukturo. Dodatni časovni žigi morajo biti dodani pred prenehanjem veljavnosti uporabljenega certifikata overitelja časovnih žigov. Vozlišče *<ArchiveTimeStamp>* je bilo dodano prav s tem namenom.

Kdo kreira določene nivoje XAdES?

Uporabniki pri XAdES podpisih nastopajo v dveh vlogah: kot *podpisniki* in kot *kontrolorji*. Ker obstaja več nivojev XAdES podpisov, se postavlja vprašanje: »Kdo je zadolžen za izgradnjo posameznega nivoja XAdES podpisa?«



Slika 3.2 kdo kreira posamezni nivo XAdES

Pravilo je prikazano na sliki 3.2. Prvi nivo XAdES podpisa zgradi podpisnik. Drugi nivo (XAdES-T) lahko kreira bodisi podpisnik, ali kontrolor. Tretji nivo (XAdES-C) najpogosteje naredi kontrolor, čeprav v redkih primerih to lahko naredi tudi podpisnik. Ostale nivoje (XAdES-X, XAdES-X-L in XAdES-A) pa kreira izključno kontrolor.

5. Časovno žigosanje (Time Stamping)

V primerjavi s papirnimi, digitalni dokumenti imajo nekaj prednosti in pomanjkljivosti. Dokumente v digitalni obliki lažje hitro prenašamo, in učinkovito hranimo. Po drugi strani je veliko težje ugotoviti spreminjanje takšnih dokumentov, kot tistih v papirni obliki. Za to da lahko uporabljamo digitalne dokumente kot medij za varno hranjenje informacij in uradnih dokumentov tako kot na papirnih, moramo uporabiti metode za zagotavljanje integritete dokumentov.

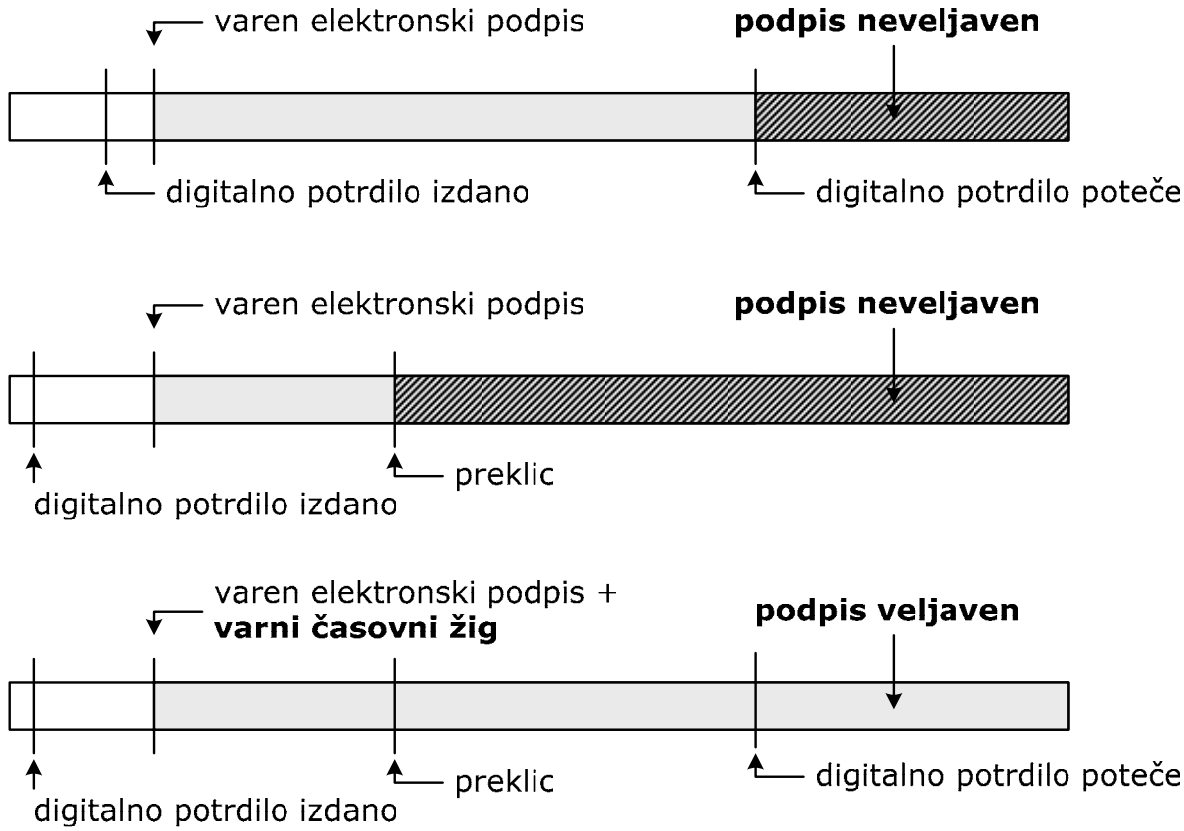
Kot je v tem dokumentu že bilo zapisano, je digitalni podpis možen način enkripcije podatkov in določanja podpisnika. Preverjanje podpisa poteka s pomočjo

javnega ključa, ki ustreza privatnemu ključu digitalnega potrdila s katerim smo dokument podpisali. Če pa digitalno potrdilo poteče ali je preklicano, ni več mogoče preveriti če je podpis bil narejen v času veljavnosti potrdila. Nihče namreč ne garantira da bo izvajal potrebnih kontrol privatnega ključa po poteku digitalnega potrdila. Veljavnost digitalnih potrdil je ponavadi prekratka za dolgoročno zagotavljanje veljavnosti podpisa.

Časovno žigosanje (Time Stamping) je metoda, ki zagotavlja obstoj digitalnih podatkov pred nekim časom. Za časovno žigosanje digitalno podpisanih dokumentom potrebujemo takšno metodo, ki ima naslednje lastnosti:

- mora biti mogoče izdati časovni žig za podatke, ne glede na karakteristike shranjevanja podatkov,
- ne sme biti mogoče da po spreminjanju dokumentov, časovni žig ostane veljaven,
- ne sme biti omogočeno izdajanje časovnega žiga za neki čas, ki se razlikuje od dejanskega.

Slika 4.1 prikazuje možnosti kako časovni žig pomaga pri ohranjanju veljavnosti digitalnih dokumentov. V prvih dveh primerih postane podpis neveljaven ob poteku, ali preklicu certifikata. V tretjem pa zaradi uporabe časovnega žiga, podpis ohrani veljavnost klub poteku, ali preklicu certifikata s katerim je bil ustvarjen.



Slika 4.1. Kako časovni žig ohranja veljavnost podpisa (primer 3), ko bi brez njegove uporabe podpisu preneha veljavnost (primera 1 in 2)

Uporabljeni simboli

Ko v tekstu uporabljamo zapis Sig$A\{X_1, \ldots, X_m\}$, to pomeni digitalni podpis uporabnika A urejene množice dokumentov $X_1, \ldots, X_m$.

Zgoščevalna funkcija brez trčenj h, je funkcija s polinomsko časovno kompleksnostjo takšna da je računsko praktično nemogoče uganiti dva argumenta $x_1 <> x_2$, ki dajo enako vrednost zgoščevalne funkcije $h(x_1) = h(x_2)$.

Absolutni (hash-and-sign) časovni žig

Absolutni (hash-and-sign) časovni žigi, so sestavljeni iz dokumenta (ali njegove zgostitve) in datuma/časa zapisanega kot številke. Varnost takšne sheme se zanaša na predpostavki da ima ponudnik storitve časovnega žiga (Time Stamping Authority - TSA) dovolj natančno uro, in da je popolnoma zaupanja vreden.

Več o zgostitvenih funkcijah in algoritmih za njihovo računanje lahko preberete v [9].

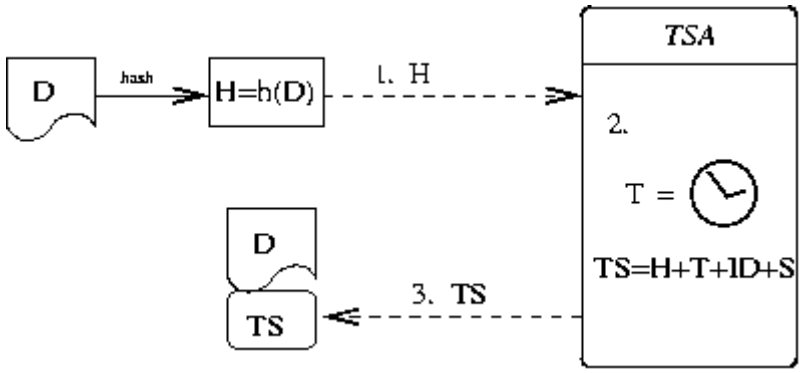
Če od TSA želimo dobiti trenutni časovni žig H, uporabnik A mora poslati ustrezno zahtevo. TSA podpiše trenutni čas t_1 in pošlje $H = SigTSA\{t_1\}$ uporabniku A. Na primer, za podpisan dokument = SigA{X, H}, uporabnik B lahko ugotovi da je dokument X podpisal uporabnik A po času t_1. Pri tem se moramo zavedati da tudi če zaupamo TSA, s tem še ne moremo dokazati da je podpis bil narejen točno ob času t_1. Pri preverjanju podpisa, uporabnik B pošlje podpis x agenciji TSA. TSA mu doda trenutni datum in čas t_2 in vrne podpis $T = SigTSA\{x, t_2\}$ uporabniku B. Trojček (H, x, T) je dokaz da je uporabnik A podpisal dokument X znotraj časovnega intervala [t_1, t_2]. V sistemih s samo eno agencijo TSA ni učinkovite rešitve problema kompromitiranja ključev agencije TSA.

Sheme za časovno žigosanje lahko razdelimo v tri skupine:

- enostavne,
- povezane, in
- distribuirane.

Enostavna shema

V enostavni shemi časovni žig ustvarimo tako da ne vsebuje podatkov, ki so vključeni v drugih časovnih žigih. Izdaja časovnega žiga poteka na naslednji način (slika 4.2):



Slika 4.2 enostavna shema

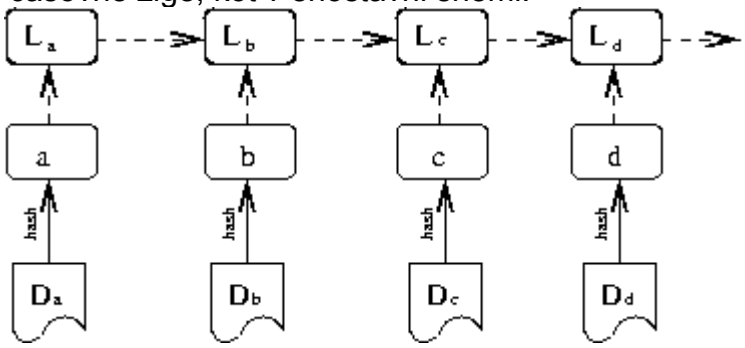
1. Uporabnik, ki želi časovni žig za določene podatke D pošlje zahtevek skupaj z zgoščeno vrednostjo H podatkov D izdajatelju časovnega žiga.
2. Izdajatelj kreira digitalni podpis S za H, časovni parameter T in identifikacijo ID izdajatelja (TSA). T označuje čas sprejema zahtevka. Časovni žig TS za D vsebuje vsaj H, T, ID in S.
3. Izdajatelj pošlje časovni žig TS uporabniku, ki ga je zahteval.

Pri preverjanju časovnega žiga uporabnik mora prvo izračunati zgoščeno vrednost podatkov D, in jo primerjati z vrednostjo zapisano v časovnem žigu. Za tem mora preveriti tudi veljavnost podpisa S časovnega žiga.

Ključna lastnost enostavne sheme je da je kljub relativni preprostosti, njena varnost pogojena z zanesljivostjo izdajatelja.

Povezana shema

V povezani shemi izdajatelj kreira časovni žig, ki vsebuje podatke vsebovane tudi v drugih časovnih žigih. Kot rezultat dobimo verigo časovnih žigov, kot je prikazano na sliki 4.3. Če bi izdajatelj želel naknadno ponarediti časovni žig, mora ponarediti tudi ostale časovne žige, ki jih vsebuje. Zaradi tega je v povezani shemi težje spreminjati časovne žige, kot v enostavni shemi.



Slika 4.3 povezana shema

Primera povezanih shem sta PKITS in TIMESEC. Pri TIMESEC-u, podatke o časovnih žigih redno objavljajo z namenom da še dodatno zapletejo delo morebitnim napadalcem. Ta način povečuje varnost časovnih žigov v povezani shemi tudi če izdajatelj ni vedno zanesljiv. Problem povezane sheme je da je bolj zapletena kot enostavna shema.

Distribuirana shema

V distribuirani shemi več izdajateljev skupaj izdajo časovni žig. Namen je povečati varnost proti manipulaciji časovnih žigov. To je doseženo tako, da podatke potrebne za kreiranje časovnega žiga razdelimo med več izdajatelji. Za uspešno ponarejanje časovnega žiga je potrebno sodelovanje vseh izdajateljev, kar to akcijo dodatno otežuje.

Storitve časovnega žiga v Sloveniji

V Sloveniji delujeta dva izdajatelja časovnih žigov. Uporaba obeh je komercialna, ker pomeni da se njihove storitve plačujejo. Ponudnika sta:

- Pošta Slovenije (https://tsa.posta.si/), in
- Center Vlade za informatiko (http://www.si-tsa.si/).

Zanimivo je da sta se oba ponudnika odločila za uporabo enake programske opreme podjetja Entrust. To pomeni da sta obliki zahtevka za časovni žig in odgovora enaka. Storitvi sta dostopni preko protokola SOAP, kar omogoča uporabo na različnih platformah.

6. Digitalni podpis in zakonodaja

V Sloveniji je področje elektronskega podpisa urejeno z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP) in njegovimi podzakonskimi akti. Ta zakon bolj natančno opisujejo dodatne uredbe:

- Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP-A),
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, in
- Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji.

Zakon govori o elektronskem in ne o digitalnem podpisovanju (v tem delu je tehnološko neodvisen), a vsebuje tudi določila o overiteljih in digitalnih potrdilih. Definira zahteve za kvalificirana digitalna potrdila, in poslovanjem overiteljev v Republiki Sloveniji. Register overiteljev se trenutno vodi pri Ministrstvu za Informacijsko Družbo. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje podrobneje opredeljuje pogoje v zvezi z opremo, postopki, organizacijo, overitelji, digitalnimi potrdili, ... Zakon je povezan s naslednjimi uredbami evropske skupnosti:

- Direktiva 1999/93/Es Evropskega Parlamenta in Sveta,
- Direktiva 2000/31/Es Evropskega Parlamenta in Sveta.

O elektronskem poslovanju govori tudi »Modelni zakon združenih narodov o elektronskem poslovanju« (*UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm).

ZEPEP in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje

Ko govorimo o elektronskem podpisovanju, moramo najprej pojasniti, katere so temeljne naloge elektronskega podpisa. Te se bistveno ne razlikujejo od nalog, ki jih opravlja lastnoročni podpis.

S podpisom identificiramo osebo oziroma podpisnika ter zanesljivo ugotovimo osebno sodelovanje podpisnika pri podpisovanju. Podpis povezuje podpisnika z vsebino podpisanega dokumenta, ter dokazuje in zavezuje podpisnika, k vsebini podpisanega dokumenta. Podpis služi kot dokazovanje avtorstva pri določenem avtorskem delu. Podpisnik se lahko podpiše pod dokument, ki ga je sestavil nekdo drug in tako izrazi svoje strinjanje z vsebino dokumenta. Podpis dokazuje tudi dejstvo, da je bil podpisnik ob določenem času na določenem kraju.

Tehnološke možnosti, ki jih uporabljamo pri elektronskem poslovanju omogočajo, da se dokument izdela v praktično neomejenem številu izvodov. Izviren dokument je zato nemogoče ločiti od njegovih kopij. Elektronski dokument nima lastnoročnega podpisa in ni na papirju. Zato obstaja možnost, da bo kdo dokument prestregel in spremenil, oziroma celo ponaredil podatke. Da bi to preprečili, so se razvile različne tehnologije, ki omogočajo, da z njihovo uporabo dosežemo enake učinke kot jih ima v klasičnem poslovanju lastnoročni podpis. To so tehnologije elektronskega podpisovanja.

Po Zakonu o elektronskem poslovanju in elektronskem podpisu je overitelj, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi, lahko vsaka fizična ali pravna oseba. Za varno elektronsko poslovanje potrebujemo varen elektronski podpis, ki je overjen s kvalificiranim potrdilom. Tega lahko izda samo overitelj, ki je za to dejavnost registriran oz deluje skladno z določbami ZEPEP in uredbe.

Zakonodajalec je določil, da **elektronsko poslovanje** zajema poslovanje v elektronski obliki na daljavo z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu.

V nadaljevanju so obrazloženi nekateri pojmi in izrazi o elektronskem podpisovanju in overiteljstvu , ki so uporabljeni v zakonu.:

1. **Elektronski podpis** je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;
2. **Varen elektronski podpis**, je elektronski podpis, ki izpolnjuje štiri predpisane zahteve (povezan je izključno s podpisnikom; iz njega je mogoče zanesljivo ugotoviti podpisnika; ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom; povezan je s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi);
3. Podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
4. Sredstvo za elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;
5. Podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;
6. Sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;
7. Potrdilo je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
8. Overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Nihče se ne more sklicevati, da elektronski podpis ni veljaven oziroma nima dokazne vrednosti, samo zaradi tega, ker je v elektronski obliki ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.

Kljub temu, pa nima vsak elektronski podpis enake vrednosti kot lastnoročni podpis, temveč le elektronski podpis overjen s kvalificiranim potrdilom. Iz takega potrdila mora biti razvidno vse kar določa ZEPEP v 28. členu (npr. navedba da gre za kvalificirano potrdilo, ime oziroma psevdonim imetnika potrdila, podatki za preverjanje elektronskega podpisa, začetek in konec veljavnosti potrdila, varen elektronski podpis overitelja, ki je potrdilo izdal,…). Podatke ali sredstva za elektronsko podpisovanje je prepovedano uporabljati brez vednosti podpisnika ali imetnika potrdila. Kvalificirana potrdila lahko veljajo največ 5 let.

Overitelj mora pri opravljanju storitev elektronskega podpisovanja ravnati s skrbnostjo dobrega strokovnjaka in odgovarja po načelu obrnjenega dokaznega bremena. Dokazati mora, da je škoda nastala brez njegove krivde.

Overitelj odgovarja vsaki osebi, ki se upravičeno zanaša na kvalificirano potrdilo, ki ga je izdal in daje zagotovilo: potrdila, ter da potrdilo vsebuje vse predpisane podatke za kvalificirano potrdilo;

- za točnost podatkov v potrdilu od trenutka izdaje

- da je imel imetnik potrdila, naveden v potrdilu, v času izdaje potrdila podatke za elektronsko podpisovanje ustrezne podatkom za preverjanje elektronskega podpisa, navedenim ali označenim v potrdilu;
- da delujejo podatki za elektronsko podpisovanje in podatki za preverjanje elektronskega podpisa komplementarno v primeru, če overitelj oblikuje oboje podatke;
- za takojšen preklic potrdila in objavo preklica, če za preklic obstajajo razlogi;
- za izpolnjevanje zahtev tega zakona in na njegovi podlagi izdanih podzakonskih predpisov glede varnih elektronskih podpisov in kvalificiranih potrdil.

V kvalificiranem potrdilu se lahko označi meje uporabnosti ali najvišje transakcijske vrednosti določenega potrdila. Tako overitelj izključi svojo odgovornost za posledice uporabe potrdila izven določenih meja, če so omejitve prepoznavne tretjim osebam. Osebo, ki zahteva potrdilo, mora overitelj obvestiti o vseh pomembnejših okoliščinah uporabe potrdila in jo identificirati s pomočjo uradnega osebnega dokumenta s fotografijo za fizične osebe oziroma uradno potrjenega dokumenta za pravne osebe še pred sklenitvijo pogodbe.

Zagotovljen mora biti takojšen in varen preklic potrdila. Overitelj vodi register preklicanih potrdil, v primeru prenehanja svojega delovanja pa mora zagotoviti, da seznam vodi drug overitelj.

ZEPEP in uredba določata tudi druge obveznosti overitelja, kot je zaposlovanje oseb s strokovnim znanjem, uporaba zanesljivega sistema in opreme, izvajanje varnostnih ukrepov zoper ponarejanje potrdil, zanesljivo shranjevanje potrdil.

ZEPEP določa tehnične zahteve, ki jih mora izpolnjevati overitelj za varno elektronsko podpisovanje, podrobnejša merila za izpolnjevanje zahtev pa predpisuje uredba.

Inšpekcijsko nadzorstvo nad izvajanjem določb ZEPEP izvaja pristojno ministrstvo.

Direktiva 1999/93/ES Evropskega Parlamenta in Sveta

Izdana dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis - definira Evropsko pravno podlago za elektronski podpis. Cilj te direktive je olajšati uporabo elektronskega podpisa in prispevati k njegovemu pravnemu priznanju. Oblikuje pravni okvir za elektronski podpis in nekatere storitve overjanja, da bi bilo zagotovljeno primerno delovanje notranjega trga. Direktiva razlikuje med *»navadnim elektronskim podpisom«* in *»varnim elektronskim podpisom«*. Čeprav se navadnem elektronskem podpisu ne sme zanikati pravna vrednost, samo varen elektronski podpis, z določenimi omejitvami lahko enakovredno nadomesti lastnoročni podpis v pravnem smislu. S tem je omogočeno elektronsko poslovanje tudi povsod tam, kjer zakoni izrecno zahtevajo lastnoročne podpise. Tudi sicer pripiše določeno pravno veljavo elektronskim sporočilom, in sicer:

1. Države članice zagotovijo, da napredni elektronski podpisi, ki temeljijo na kvalificiranem potrdilu in so ustvarjeni z napravo za varno tvorjenje podpisa:

(a) izpolnjujejo pravne zahteve za podpis v zvezi s podatki v elektronski obliki na enak način kot izpolnjuje lastnoročni podpis zahteve v zvezi s podatki na papirju,

(b) so sprejemljivi v sodnih postopkih kot dokaz.

2. *Države članice zagotovijo, da se pravni učinki elektronskega podpisa in njegova sprejemljivost kot dokazno sredstvo v sodnih postopkih ne spodbijajo samo zato, ker:*
   (a) je podpis v elektronski obliki ali
   (b) ne temelji na kvalificiranem potrdilu ali
   (c) ne temelji na kvalificiranem potrdilu, ki ga izda akreditirani overitelj ali
   (d) ni oblikovan z napravo za varno tvorjenje podpisa.

Direktiva predpisuje da je med postopkom preverjanja podpisa treba dovolj zanesljivo zagotoviti, da:

(a) podatki, ki se uporabljajo za preverjanje podpisa, ustrezajo podatkom, ki so prikazani overitelju;
(b) je podpis zanesljivo preverjen in rezultat preverjanja pravilno prikazan;
(c) lahko overitelj po potrebi zanesljivo določi vsebino podpisanih podatkov;
(d) sta pristnost in veljavnost potrdila, zahtevanega med preverjanjem podpisa, zanesljivo preverjeni;
(e) sta rezultat preverjanja in istovetnost podpisnika pravilno prikazana;
(f) je raba psevdonima jasno označena, in
(g) se lahko odkrijejo vse spremembe, ki kakorkoli vplivajo na varnost elektronskega podpisa.

Direktiva 2000/31/Es Evropskega Parlamenta in Sveta

Izdana dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju). Direktiva obravnava širše področje elektronskega poslovanja, vendar v poglavju »Obravnava pogodb« določa da:

1. *Države članice zagotovijo, da njihov pravni sistem dovoljuje sklepanje pogodb z uporabo elektronskih sredstev. Države članice posebej zagotovijo, da pravni predpisi, ki se uporabljajo za sklepanje pogodb, ne ovirajo uporabe elektronskih pogodb ter da so te pogodbe kljub sklenitvi po elektronskih sredstvih pravno učinkovite in veljavne.*
2. *Države članice lahko določijo, da se odstavek 1 ne uporablja za vse ali za nekatere pogodbe, ki spadajo v eno izmed naslednjih kategorij:*
   (a) pogodbe, s katerimi se pridobijo ali prenašajo nepremičninske pravice z izjemo najemniških pravic;
   (b) pogodbe, za katere zakon določa sodelovanje sodišč, javnih organov ali poklicev, ki izvajajo javna pooblastila;
   (c) poroštvene pogodbe in pogodbe o varščini, ki jih sklepajo osebe zunaj svoje trgovske, poslovne ali poklicne dejavnosti;
   (d) pogodbe, ki jih ureja družinsko ali dedno pravo.

Če želimo doseči da to velja, ni dovolj da uporabimo navaden digitalni podpis (opisan v standardu XMLDSig). Uporabiti moramo varen digitalni podpis (takega opisuje standard XAdES).

7. Zaključek

Postavlja se vprašanje »Kdaj uporabiti elektronski podpis«? Elektronski podpis ni primeren v vseh scenarijih. Če primerjamo vrste podatkov, potem ga ne uporabljamo za dinamične poizvedbe (npr. promet na transakcijskem računu), primeren pa je za statične poizvedbe, tj. dokumente (npr. izpisek na transakcijskem računu). Uporabimo ga kot dodaten varnostni element, ali za pravno veljavne elektronske dokumente v odprtih sistemih (ZEPEP). Potreben je, kadar se dokument

prenaša preko zaupanja ne-vredne povezave ali hrani na zaupanja ne-vrednem mestu.

Tri do pet let nazaj je na tem področju prevladovalo nepoznavanje problematike. Veljalo je prepričanje: »Elektronski podpis je zapleten in vprašanje je, če je varen«. Danes se pogosto pojavlja pretirano poenostavljanje »Elektronski podpis zna ga narediti vsak – torej varnost ni več problem«. Nerazumevanje se pojavlja tudi pri zaupnosti certifikata. Ta v osnovi ni zaupen podatek (zaradi napačne uporabe lahko je), kar otežuje preverjanje veljavnosti podpisov. Načelno elektronski podpis ne zagotavlja zaupnosti – digitalno podpisani podatki niso nujno šifrirani!

Standard XAdES določa kaj je potrebno narediti da dosežemo varen elektronski podpis. Kot je razvidno, je to področje zapleteno, in pri sami implementaciji moramo biti zelo pozorni. Napačno razumevanje in pomanjkljiva implementacija, lahko pripeljejo do varnostnih lukenj, in neželenih težav pri pravnih postopkih. Poleg tega da opis standarda ustreza zahtevam Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP), omogoča dodatno tudi izvedbo dolgoročnega arhiva, in onemogoča zanikanje podpisa (non-reputidation).

Literatura

[1] Martin Centner: »XML Advanced Electronic Signatures (XAdES) - Implementation and Interoperability« Graz University of Technology, September 2003,

[2] XMLDSig standard: http://www.w3.org/Signature/,

[3] Spošno o XML: http://www.w3.org/XML/,

[4] Timestamp agencija Pošte Slovenija: http://democa.posta.si:9080/verificationserver/; https://tsa.posta.si/verificationserver/ (zahteva veljavno digitalno potrdilo),

[5] Timestamp agencija Centra vlade za informatiko http://www.si-tsa.si/navodila.htm,

[6] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP): http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO1973.html,

[7] Direktiva 1999/93/ES Evropskega Parlamenta In Sveta http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=sl&numdoc=31999L0093&model=guichett,

[8] Direktiva 2000/31/Es Evropskega Parlamenta In Sveta http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=sl&numdoc=32000L0031&model=guichett,

[9] Douglas R. Stinson: »Cryptography Theory and Practise«, Second edition, CRC Press 2002,

[10] What are Certificate Revocation Lists (CRLs)? http://www.rsasecurity.com/rsalabs/node.asp?id=2283.