UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

RAVNANJE Z DIGITALNO PODPISANIMI DOKUMENTI OD NASTANKA DO ARHIVA V POGOJIH POSLOVANJA, KI JIH DOLOČA ZEPEP

SAŠA MEHAK ROJEC

LJUBLJANA, APRIL 2006

IZJAVA

Študentka Saša Mehak Rojec izjavljam, da sem avtorica tega magistrskega dela, ki sem ga napisala pod mentorstvom prof. dr. Borke Jerman Blažič in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne

Podpis:_____

KAZALO VSEBINE

KAZALO SLIK

KAZALO TABEL

1 UVOD

Z izrazom "dokument" (angl. record) poimenujemo pisno potrdilo ali dokazilo o nekem dejstvu, zato že dolgo predstavlja osrednjo enoto poslovanja z dokumentarnim gradivom. Dokument sestoji iz informacije, elementov verodostojnosti in relativno trajnega nosilca. Do nedavnega je bil najpogostejši nosilec dokumentov papir (klasično poslovanje), z razvojem informacijske tehnologije se vse bolj uveljavljajo elektronski nosilci.

Poslovanje z dokumenti se je zaradi mnogih prednosti (večja hitrost in nižja cena poslovanja, večja fleksibilnost, shranjevanje podatkov na manjšem prostoru ipd.) preselilo v elektronski svet. Nova internetna tehnologija je zagotovila nove poslovne modele, ki so povezali decentralizirane enote in vpeljali standarde, hiter nadzor poslovanja ter možnost neomejene komunikacije (Jerman Blažič, 2001, str. 22). Nov pristop v poslovanju je prinesel tudi slabosti, med katerimi še posebej izstopajo problemi z zagotavljanjem varnosti podatkov in elektronskih dokumentov. Dokumente je v elektronskem svetu mogoče enostavno spreminjati brez kakršnihkoli sledi. Nova verzija dokumenta ne kaže sprememb, ki so nastale v postopku obdelave in prenosa; poleg tega običajen elektronski dokument sam po sebi ne vsebuje podatkov, ki bi zagotavljali pristnost dokumenta in identifikacijo avtorja. Možnost zlorabe je realna, zato se pravila, ki so veljala vrsto let, v sodobnem svetu spreminjajo. Dokumente je potrebno varovati z varnostnimi mehanizmi na več ravneh.

Prvi postopek, ki nam lahko zagotavlja pristnost in neokrnjenost elektronskega dokumenta, je tehnologija digitalnega podpisa. Digitalni podpis je v skladu z določili Zakona o elektronskem poslovanju in elektronskem podpisu - ZEPEP (Uradni list RS, št. 98/2004) sodobna alternativa klasičnemu lastnoročnemu podpisu: v pogojih, ki jih prav tako določa ta zakon (15. člen), je enakovreden lastnoročnemu podpisu. Informacijski sistemi različnih organizacij že podpirajo uporabo digitalnega podpisa (bančno poslovanje, oddaja napovedi za odmero dohodnine, uporaba zemljiške knjige ipd.). Digitalno podpisovanje je s stališča uporabnika izredno enostavno: potreben je le pritisk na tipko za začetek postopka. Po drugi strani strojna in programska oprema v ozadju izvajata kompleksne postopke za zaščito dokumentov na kar se da visoki ravni. Potrebna je obsežna infrastruktura, ki omogoča nedvoumno identifikacijo uporabnika, časa nastanka sporočila ipd.

Nadgradnjo pravnega priznanja digitalno podpisanega elektronskega dokumenta predstavlja elektronska hramba in arhiviranje vsebine ter atributov, potrebnih za ohranjanje dokazne vrednosti. Elektronske dokumente hranimo za obdobje, ki ga predpisujeta zakon ali posebna regulativa na posameznem področju. Problematika hrambe digitalno podpisanih dokumentov je še vedno premalo raziskana. Uporaba digitalnih potrdil odpira problem časovno omejene veljavnosti digitalnih podpisov. Zaradi staranja strojne in programske opreme (kot posledice napredka tehnologije) se lahko pojavi problem prikaza elektronskega dokumenta, ranljivi so tudi nosilci dokumentov.

Problematika je tem bolj kompleksna, čim daljši je predpisani rok hrambe. Zanesljivost hrambe elektronskega gradiva zastavlja kopico tehnoloških, pravnih, in organizacijskih vprašanj. Primanjkuje ustreznih standardov, obstoječa tehnologija ni dovolj časovno testirana. Pomanjkljiva je tudi zakonodaja.

Tema pričujočega magistrskega dela je: Na kakšen način lahko dosežemo zadovoljivo raven varnosti elektronskih dokumentov? Namen dela je opredelitev potrebnih postopkov za varno upravljanje z elektronskimi dokumenti, ki vsebujejo elemente verodostojnosti, s tehničnega, pravnega in organizacijskega vidika, ter raziskati okvirje za njihovo varno hrambo. Ob temeljni hipotezi, da lahko magistrsko delo služi kot pomoč pri presojah v zvezi s stopnjo zaupanja v elektronsko poslovanje z dokumenti in morda celo pri odločitvah povezanih z uvedbo tovrstnega poslovanja v podjetjih, sem si za cilj zadala izdelavo tehnično-pravnega modela okolja varnega elektronskega poslovanja.

Celotno magistrsko delo je razdeljeno na pet tematskih sklopov. Najprej so predstavljeni osnovni varnostni mehanizmi (šifriranje, digitalni podpis, časovni žig), pomen infrastrukture javnih ključev ter opisi nekaterih protokolov za zagotavljanje varnosti na komunikacijskih poteh. Sledi opis problematike elektronskega arhiviranja, alternativne rešitve in pomen varnega javnega elektronskega arhiva. V četrtem poglavju je opisan tehnični vidik varnega elektronskega poslovanja, ki zajema splošno sprejete tehnične standarde in priporočila za učinkovito delovanje elektronskih arhivov. Pri tem je poudarek na ohranjanju vsebine in njenih atributov ter oblikah varnega elektronskega podpisa. Sledi predstavitev temeljne zakonske ureditve elektronskega poslovanja in elektronskega podpisa tako v Republiki Sloveniji, kot tudi v tujini. Na koncu magistrskega dela je strnjeno predstavljen predlog modela za varno ravnanje z digitalno podpisanimi dokumenti v okviru celotnega življenjskega cikla dokumenta (od nastanka do arhiva). Delu sta dodani dve prilogi: v prvi so zbrani uporabljeni strokovni izrazi in kratice s slovenskim prevodom; v drugi je podano uradno prečiščeno besedilo Zakona o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Uradni list RS, št. 98/2004).

Varovanje elektronskih dokumentov v celoti zajema še druge ukrepe, kot so zaščita informacijskega sistema s požarno pregrado, protivirusna zaščita, zagotavljanje visoke razpoložljivosti sistema ipd., vendar ti ukrepi presegajo okvir mojega magistrskega dela.

Saša Mehak Rojec

2 OKOLJE VARNEGA ELEKTRONSKEGA POSLOVANJA

Dokumenti v elektronskem okolju niso verodostojni sami po sebi, saj jih je mogoče enostavno in brez sledi kopirati ali celo spreminjati. Zaupanje vanje lahko dosežemo le z zanesljivim varovanjem pred nepooblaščenimi dejanji, ne le v okviru informacijskega sistema, kjer dokument nastaja, temveč tudi na komunikacijskih poteh, po katerih dokument potuje. Način zagotavljanja varnosti je odvisen od vrednosti virov, potencialnih groženj in učinka teh groženj (Jerman Blažič, 2001, 99). Pomembno je, da so storitve, ki se vršijo po elektronski poti, enako ali celo bolj varne kot storitve, ki se opravljajo na klasičen način.

Elektronske dokumente lahko varujemo na različne načine. Za najvišji nivo varnosti v elektronskem poslovanju je potrebno zagotoviti naslednje varovalne funkcije (http://www.gov.si/ca/dokumenti/priporo%E8ila-PKI-aplikacije-v1.0.pdf):

- **avtentikacijo** - nedvoumno identifikacijo (overjanje) uporabnika ali strežnika oz. aplikacije, do katere uporabnik dostopa;
- **avtorizacijo** – nadzor nad dostopom (zagotoviti uporabniku avtoriziran dostop do podatkov / storitev in določiti pogoje za dostop);
- **nezatajljivost** – nezmožnost zanikanja izvora podatkov; vključenost v opravljanje storitev; preprečitev možnost ponarejanja opravljenih storitev;
- **celovitost podatkov** – zagotoviti celovitost (nespremenjenost) izmenjanih podatkov, kar pomeni, da podatki od svojega nastanka niso bili kakorkoli spremenjeni, da o tem ciljni uporabnik ne bi bil obveščen;
- **zaupnost** – zagotoviti zaupnost povezave med uporabnikom in strežnikom; prav tako mora biti zagotovljena zaščita podatkov, ki se ob tem izmenjajo.

Tabela 1: Varovalne funkcije in mehanizmi

VAROVALNA FUNKCIJA	VAROVALNI MEHANIZEM
zaupnost sporočila	šifriranje
celovitost sporočila	nadzorni niz (digitalni podpis)
avtentikacija	digitalni podpis
nezatajljivost	digitalni podpis
nepodvajanje sporočila	časovni žig

Vir: http://ecom.fov.uni-mb.si/ecomSLO/Studenti/Predmeti/Prezentacije/Varnost%20interneta.ppt

V praksi je varovalne funkcije mogoče zagotavljati s kriptografskimi[1] varovalnimi mehanizmi (šifriranjem, digitalnim podpisom, časovnim žigom,…) in z njimi povezano

[1] Kriptografija – veda, ki se ukvarja z zakrivanjem podatkov.

uporabo digitalnih potrdil. Pregled, katere funkcije zagotavljajo posamezni varovalni mehanizmi, je podan v tabeli 1.

2.1 Osnovni kriptografski mehanizmi

Osnovni kriptografski mehanizmi so temelj pravnega priznanja dokumentov, sami po sebi ne morejo varovati dokumenta na celotni poti od nastanka do arhivranja. Zasnovani so na načelu enosmerne preslikave binarne vrednosti vsebine po določenem algoritmu.

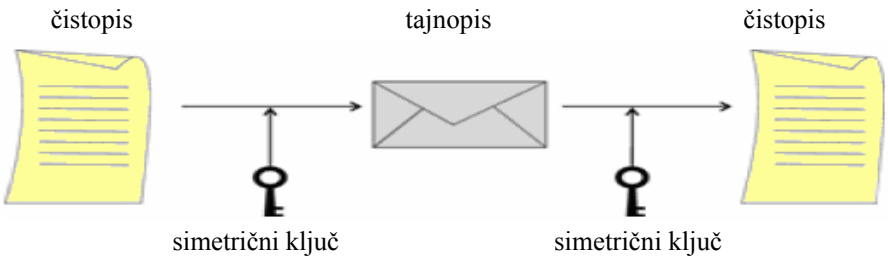
2.1.1 Šifriranje

Šifriranje je postopek preoblikovanja berljivega besedila (čistopis) v neberljivo obliko (tajnopis), z namenom zagotavljanja zaupnosti oz. zaščite podatkov pred nepooblaščenimi pogledi. Osnovni operaciji pri tem sta premeščanje (transpozicija) ali nadomestitev (substitucija) znakov sporočila po določenem ključu. Obraten postopek, ki na podlagi znanega algoritma in ustreznega ključa iz tajnopisa vrne berljivo obliko podatkov, imenujemo dešifriranje. Stara tehnika, ki izhaja iz antičnih časov in je imela v zgodovini pomembno vlogo, je s pojavom računalnikov dobila nove razsežnosti. Nova tehnologija omogoča hitro in učinkovito izvajanje zapletenih matematičnih algoritmov. V praksi uporabljamo različne algoritme, ki se med seboj razlikujejo glede na stopnjo kompleksnosti in pripadajočo mero varnosti.

2.1.1.1 Simetrični algoritmi

Simetrični algoritmi za šifriranje in dešifriranje podatkov uporabljajo isti - sejni ključ. Uporabljeni algoritem je znan. Ključ predstavlja skupno skrivnost udeležencev (subjektov), zato ga je potrebno izmenjati na varen način.

Slika 1 : Simetrično šifriranje



Vir: Jerman Blažič, 2001, str.103

V grobem ločimo tekoče in blokovno šifriranje. Tekoči šifrirni algoritmi sproti (zaporedno) preslikajo posamezne bite sporočila (npr. XOR[2] operacija med biti sporočila in biti

[2] XOR – ekskluzivna disjunkcija – rezultat je enak 1, če sta seštevanca različna (0, 1), v nasprotnem primeru je rezultat enak 0.

šifrirnega ključa). V praksi so pogostejši blokovni šifrirni algoritmi, ki vsebino sporočila razdelijo na bloke, nato drugega za drugim preoblikujejo z operacijami, kot sta substitucija in transpozicija.

Najbolj znan blokovni algoritem je **DES**[3] (angl. Data Encryption Standard), ameriški kriptografski standard, ki sta ga razvili organizacija NIST (angl. National Institut of Standards and Technology) in korporacija IBM. Algoritem najprej vhodno vrednost (binarna vrednost dokumenta) razdeli na bloke dolžine 64 bitov, nato jih šifrira z naključno izbranim 56 bitnim nizom, razširjenim na 64 bitov za potrebe parne kontrole (vsak osmi bit). Možnih je $2^{56}-1$ različnih kombinacij, kar znese približno $7{,}2\cdot 10^{16}$ različnih ključev. Za današnje potrebe po varnosti takšna dolžina ključa ne zadošča več, zato so nastale nove različice npr. 3DES[4] (angl. Triple-DES), kjer se postopek ponovi trikrat zapored (npr. šifriranje s ključem 1, dešifriranje s ključem 2, šifriranje s ključem 3) in tako dosega stopnjo varnosti 168 ($3\cdot 56$) bitnega ključa. NIST je 19. maja 2005 zaradi varnosti umaknil vse standarde v zvezi z algoritmom DES (http://cryptome.org/nist051905.txt).

Kot naslednika DES je NIST leta 2000 izbral **AES**[5] algoritem (angl. Advanced Encription Standard), ki vhodno vrednost razdeli na bloke dolžine128 bitov in jih šifrira z 128, 198 ali 256 bitov dolgimi ključi. Drugi simetrični algoritmi so še CAST, Rivestovi algoritmi, IDEA itd.

Simetrični algoritmi so nezahtevni matematični postopki, zato dosegajo visoko hitrost procesiranja tudi na počasnejših računalnikih. Primerni so za (de)šifriranje velikih količin podatkov ali (de)šifriranje podatkov v realnem času. Slabosti teh algoritmov sta problem izmenjave ključev in potreba po večjem številu ključev v primeru, ko bi zaradi zaupnosti želeli uporabiti različne ključe pri poslovanje z različnimi subjekti (za skupino N uporabnikov je potrebno $\frac{1}{2}\cdot\left[N^2-N\right]$ ključev).

2.1.1.2 Asimetrični algoritmi

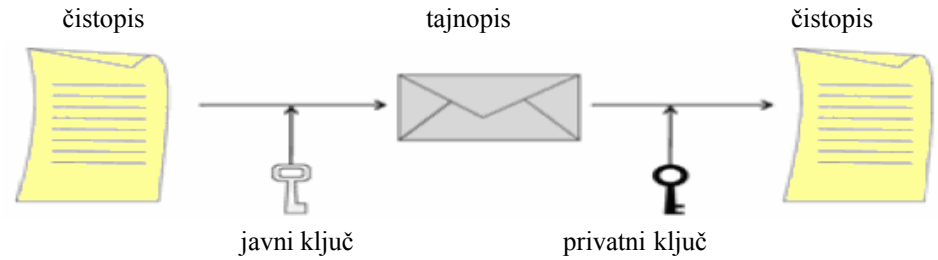
Asimetrični algoritmi za šifriranje in dešifriranje uporabljajo par različnih ključev, javni in zasebni ključ. Osnovni lastnosti obeh povesta že sami imeni. Javni ključ ni nobena skrivnost, celo javno ga je potrebno objaviti, da ga za šifriranje lahko uporabi več ljudi. Za dešifriranje se uporablja zasebni ključ, ki ga teoretično pozna in zato lahko uporabi samo ena oseba - lastnik ključa, ki mu je sporočilo namenjeno. Ključa sta sicer matematično povezana, kljub temu je na osnovi enega praktično nemogoče izračunati drugega.

[3] DES (Data Encryption Standard) – Federal Information Processing Standards - FIPS PUB 46 (1977), FIPS PUB 46-2 (1994); American National Standards Institute ANSI X3.92 (1981).

[4] 3DES – Federal Information Processing standards FIPS PUB 46-3.

[5] AES (Advanced Encription Standard) – Federal Information Processing tandards – FIPS PUB 197 (2001).

Slika 2: Asimetrično šifriranje



Vir: Jerman Blažič, 2001, str.104

Danes je najpogosteje v uporabi asimetrični algoritem blokovnihnih šifer **RSA**[6] (imenovan po začetnicah priimkov avtorjev: Ronald Rivest, Adi Shamir, Leonard Adleman). Uporablja ključe različnih dolžin. Priporočena dolžina ključa je okoli 2000 bitov. Uporaba daljšega ključa poveča varnost, uporaba krajšega ključa omogoča večjo hitrost procesiranja.

Osnova RSA algoritma sta dve veliki različni praštevili. Varnost kriptosistema temelji na dejstvu, da je faktorizacija velikih števil težka. Ob predpostavki, da sta praštevili dovolj veliki, je faktorizacija praktično nerešljiv problem.

Oznake:

p in q → veliki različni praštevili
N → zmnožek $N = p \cdot q$
e → javni eksponent - poljubno celo število e, za katero velja:
$1 < e < N$; največji skupni delitelj št. e ter produkta $(p-1)\cdot(q-1)$ ali zmnožka N je 1
d → privatni eksponent - poiščemo takšno število d, da velja
$e \cdot d \equiv 1[\mathrm{mod}(p-1)\cdot(q-1)]$

Privatni ključ sestoji iz komponent p, q in d; javni ključ sestoji iz komponent N in e.

Če je M vrednost vhodnega in C vrednost izhodnega niza, lahko preslikave opišemo z naslednjimi enačbami:

šifriranje $M^d = C(\mathrm{mod}\, N)$
dešifriranje $C^e = M(\mathrm{mod}\, N)$

Primer za manjši praštevili (Churchhouse, 2002, 176)

$p = 7, q = 13 \quad \Rightarrow \quad N = p \cdot q = 91$

[6] RSA – Public-Key Criptografic Standards PKCS#1 v2.1 (RFC 3447).

$$(p-1)\cdot(q-1)=72$$

$e=29 \quad \Rightarrow \quad 13\cdot d=1(\mathrm{mod}\,60)$

Evklidov algoritem $\Rightarrow$

$$72=2\cdot 29+14$$
$$29=2\cdot 14+1$$
$$1=29-2\cdot 14=29-2\cdot(72-2\cdot 29)=5\cdot 29-2\cdot 72$$
$$5\cdot 29=2\cdot 72+1=1(\mathrm{mod}\,72)$$
$$e=29,\ d=5$$

šifriranje

$M=10 \quad \Rightarrow \quad 10^5=C(\mathrm{mod}\,72) \quad \Rightarrow \quad C=64$

dešifriranje

$C=64 \quad \Rightarrow \quad 64^{29}=M(\mathrm{mod}\,72) \quad \Rightarrow \quad M=10$

Drugi asimetrični algoritmi so še DSA (angl. Digital Signature Algorithm) in Diffie-Hellman. V zadnjem času dobivajo vse večjo veljavo algoritmi na podlagi eliptičnih krivulj (npr. ECC – angl. Elliptic Curve Cryptosystems), ki so hitrejši od RSA kriptosistemov, ter za zagotavljanje enake stopnje varnosti uporabljajo krajše ključe.

Asimetrični algoritmi odpravljajo problem izmenjave ključev in potrebo po večjem številu ključev, vendar so zaradi svoje kompleksnosti počasni (okoli 10000x počasnejši od simetričnih algoritmov). V praksi so primerni le za šifriranje krajših vsebin. Pogosto se uporablja hibridne pristope, ki izkoriščajo prednosti obeh (simetričnih in asimetričnih) tehnologij, npr. podatke zaradi hitrosti šifriramo s simetričnimi algoritmi, nato zaradi varnosti šifriramo ključe z asimetričnimi algoritmi.

2.1.1.3 Pomen dolžine ključa

Z različnimi šifrirnimi postopki dosegamo različno stopnjo varnosti, ki je običajno enaka varnosti najšibkejše komponente. Absolutne varnosti ni, zato med varne šifrirne postopke štejemo tiste, za katere je verjetnost zlorabe oz. dešifriranja sporočila s strani napadalca, odkritje šibkosti šifrirnega postopka ali odkritje tajnega ključa dovolj majhna. Ob predpostavki, da uporabljeni algoritmi nimajo varnostnih lukenj, je najbolj kritičen element sistema ključ za šifriranje podatkov.

Pri simetričnem šifriranju je potemtakem edini način napada preizkušanje vseh možnih ključev, kar pomeni, da je pri ključu dolžine D potrebno izvesti 2^{D-1} šifriranj. Ker je za vsako posamezno šifriranje potreben določen čas, bi pri dovolj veliki dolžini ključa za takšno akcijo potrebovali nerealno velik čas. Varnost šifriranja je torej odvisna od dolžine ključa. Danes velja za varno simetrično šifriranje uporaba najmanj 128 bitnega ključa.

Asimetrične algoritme je, poleg preizkušanja vseh možnih ključev, mogoče razbiti tudi na druge načine, npr. z izračunom privatnega ključa s pomočjo faktorizacije javnega ključa. Varni asimetrični ključi so zato daljši od simetričnih. Približno enako stopnjo varnosti kot z uporabo 128 bitnega ključa pri simetričnih postopkih dosežemo z uporabo 2048 bitnega ključa pri asimetričnih postopkih. Ker razvoj tehnologije prinaša vedno hitrejše računalnike, so relativno varni ključi vedno daljši.

Tabela 2: Primerjava dolžine ključev

Stopnja varnosti	Simetrični algoritmi dolžina ključa	Asimetrični algoritmi	
		dolžina ključa RSA	dolžina ključa ECC
nizka	40 bitov	512 bitov	106 bitov
srednja	64 bitov	1024 bitov	160 bitov
visoka	128 bitov	2048 bitov	211 bitov

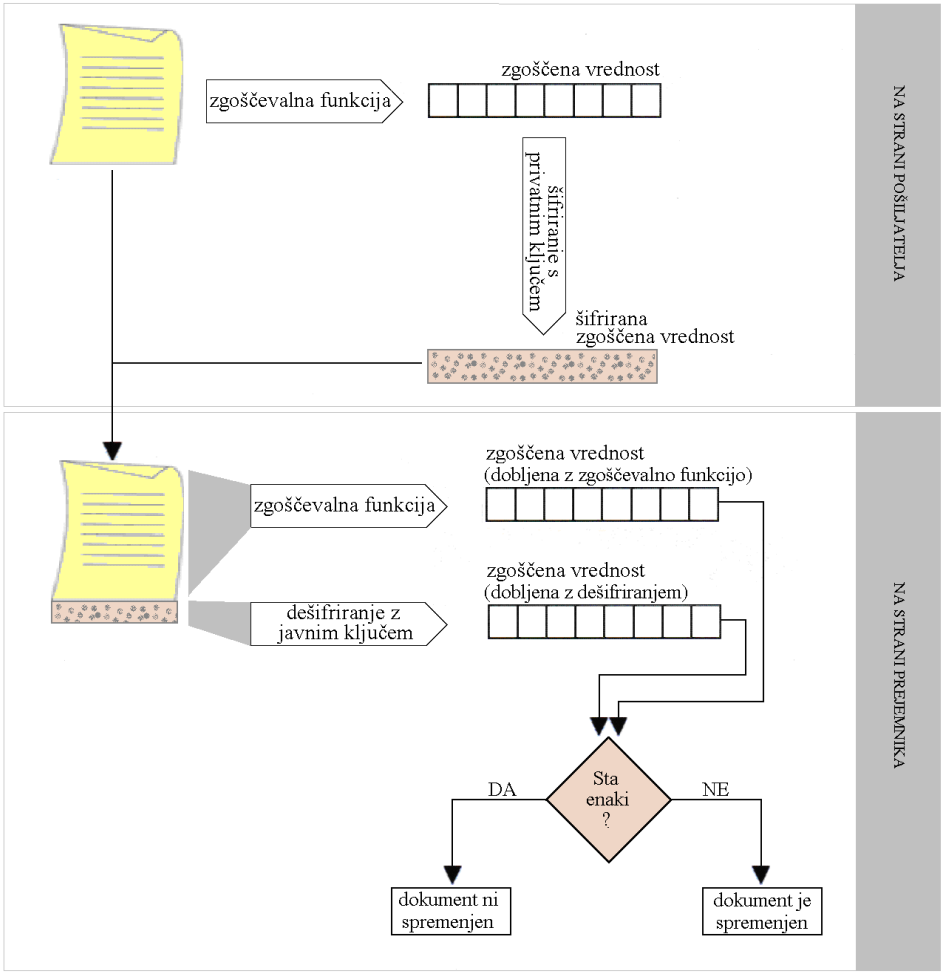
2.1.2 Digitalni podpis

Z razmahom elektronskega poslovanja se je pojavila tudi potreba po elektronskem podpisovanju dokumentov. Izraz "elektronski podpis" sicer označuje širok spekter metod, od vključevanja slike lastnoročnega podpisa ali podpisovanja z elektronskim peresom do uporabe matematičnih funkcij za preoblikovanje podatkov. Večina teh metod ne zagotavlja primerne stopnje varnosti dokumenta, zato evropska direktiva in slovenski ZEPEP ločita elektronski podpis v splošnem in varen elektronski podpis, ki izpolnjuje dodatne varnostne zahteve. Trenutno edina varna in pravno veljavna tehnična rešitev, ki lahko opravlja funkcijo klasičnega lastnoročnega podpisa (identifikacija podpisnika, dokazovanje avtorstva, strinjanje z vsebino ipd.), je digitalni podpis. To je šifriran niz znakov, ki nastane z uporabo asimetrične kriptografije in enosmerne zgoščevalne funkcije nad vhodnimi podatki. Njegova naloga ni varovanje podpisane vsebine pred vpogledi, temveč pred nepooblaščenim spreminjanjem, zato ga pripnemo k nešifrirani vsebini kot dodatek. Ločevanje podpisa od vsebine pomeni tudi dodatno prednost pri skupinskem podpisovanju iste vsebine.

Proces digitalnega podpisovanja poteka v dveh korakih: podatke najprej skrčimo z eno izmed enosmernih zgoščevalnih funkcij; nato dobljeno vrednost (prstni odtis) asimetrično šifriramo s privatnim ključem. Digitalni podpis je odvisen od vsebine na nivoju bita (opazna je že najmanjša sprememba, npr. dodan presledek ali vejica), zato ga ni mogoče kopirati ali povezovati z drugimi vsebinami.

Pri preverjanju celovitosti dokumenta podpis najprej dešifriramo z javnim ključem in tako dobimo prstni odtis dokumenta. Neodvisno od tega postopka izračunamo tudi prstni odtis iz osnovnega, nešifriranega dokumenta. Obe dobljeni vrednosti medsebojno primerjamo in če se ujemata, je podpis veljaven.

Slika 3: Digitalno podpisovanje in preverjanje podpisa



Vir: Perenič, 2001, str. 23

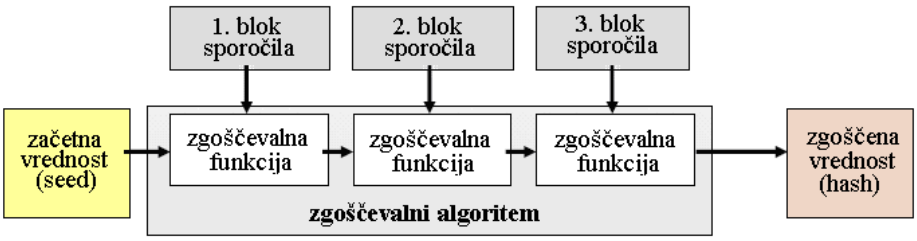
V praksi se uporablja splošno znane in standardizirane postopke digitalnega podpisovanja (npr. DSS[7]), najpogosteje sta v uporabi algoritma RSA ali DSA v kombinaciji z enosmernimi zgoščevalnimi funkcijami.

2.1.2.1 Enosmerna zgoščevalna funkcija

Zgoščevalna funkcija (angl. Hash Function) je matematična operacija, ki poljubno dolg niz znakov preslika v zgoščeno vrednost konstantne dolžine (t.i. prstni odtis vhodnega niza). Zgoščevanje poteka v sekvencah. Najprej se binarno vrednost dokumenta razbije na 512 (ali 1024) bitne bloke in na koncu doda bite do polnega bloka. Prvi blok sporočila se kombinira z začetno vrednostjo. Vsi ostali bloki se kombinirajo z rezultatom predhodne sekvence. Dolžina izhodna vrednosti je odvisna od algoritma; običajno od 128 do 512 bitov. V postopek ni vključenih skrivnih ključev. Na končno vrednost (prstni odtis) vplivajo le vhodni podatki (binarna vrednost dokumenta) in izbrani algoritem.

[7] DSS (Digital Signature Standard) – National Institute of Standards and Technology NIST 186-2 (2000).

Slika 4: Potek zgoščevanja vhodnega niza



Vir: http://www.kompas-xnet.si/Portals/0/2106delavnica.PDF

Zgoščevalna funkcija je sestavni del aplikacije za digitalno podpisovanje, zato mora izpolnjevati določene varnostne zahteve:

- isto sporočilo mora vedno preslikati v enak prstni odtis;
- vsaka najmanjša sprememba (enega samega bita) v sporočilu mora povsem spremeniti prstni odtis;
- v razumnem času ne sme obstojati možnost nastanka dveh različnih sporočil, ki bi ju lahko preslikali v popolnoma enak prstni odtis;
- mora biti enosmerna – ne sme obstojati možnost restavriranja vhodnih podatkov iz prstnega odtisa.

V praksi ni postopkov, ki bi sto-odstotno zagotavljali izpolnjevanje tretje alineje, čeprav je verjetnost, da bi iz različnih podatkov dobili enak prstni odtis, pri dovolj velikih blokih zelo majhna. Pojav, ko se popolnoma različni podatki preslikajo v enako zgoščeno vrednost, imenujemo hash kolozija. To se lahko zgodi pri zelo velikih vhodnih vrednostih, kjer imajo vrednost prvih blokov zelo majhno težo. Danes velja za dovolj varno vhodno vrednost dolžina med 2^{64} in 2^{128} bitov. Nekateri znanstveniki menijo, da zgoščevalne funkcije niso dovolj preučene in da znanje na tem področju za 20 let zaostaja za znanjem o blokovnih šifrirnih algoritmih (http://www.gov.si/tecaj/kripto/kr-zgo.htm).

Najbolj znani algoritmi za zgoščevanje vsebine so MD5[8] (angl. Message Digest), ki vhodno vrednost razbije na bloke dolžine 512 bitov in vrne 128 bitno zgoščeno vrednost, ter RIPEMD-160 in SHA-1[9] (angl. Secure Hash Standard), ki vhodno vrednost razbijeta na bloke dolžine 512 bitov in vrneta 160 bitno zgoščeno vrednost. SHA-1 že izpodrivajo novejše različice SHA-256, SHA-386 in SHA 512, ki vrnejo 256, 386 oz. 512 bitne povzetke. Zaradi želje po večji varnosti sporočil se ponekod v praksi uporablja koda za overitev sporočila (angl. Cryptographic Message Authentication Code). Algoritem za izračun kode je podoben zgoščevalni funkciji s ključem. Izhodna vrednost je odvisna od vhodne vrednosti in uporabljenega ključa. Najbolj znani tovrstni algoritem je HMAC[10].

[8] MD5 (Message Digest) – Request for Comments RFC 1321.

[9] SHA-1 (Secure Hash Standars) - Federal Information Processing tandards FIPS PUB 180-1.

[10] HMAC (Keyed-Hashing for Message Authentication) – Request for Comments RFC 2104).

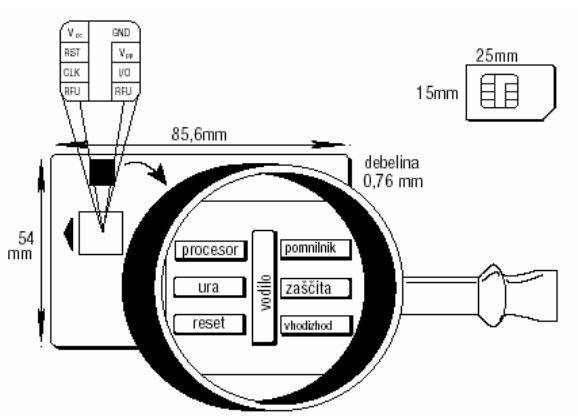
2.1.2.2 Zaščita privatnega ključa pred zlorabo

Varnost digitalnega podpisa je odvisna od varnosti uporabljenih šifrirnih algoritmov (poglavje 1.1.1.3). Še tako visoka tehnološka varnost (npr. dolžina ključa) ne doseže svojega namena, če za varnost ne skrbijo tudi uporabniki sami.

Digitalno podpisovanje je smiselno le, če zasebni ključ za podpisovanje pozna in uporablja zgolj njegov lastnik. Le tako je identifikacija podpisnika zanesljiva. Ta ključ je v večini primerov veliko praštevilo, ki si ga uporabnik ne more zapomniti, zato ga mora imeti shranjenega, kar povečuje možnost zlorabe digitalnega podpisa. Pomembna je hramba ključa ločeno od aplikacije za digitalno podpisovanje, po možnosti na prenosljivem mediju, ki ne omogoča izvoz ključa, npr. na pametnih karticah, magnetnih karticah, USB disku ipd. Priporočljivo je dodatno varovanje z geslom, osebno identifikacijsko številko PIN (angl. Personal Identification Number) ali biometrično kontrolo.

Mikroprocesorska **pametna kartica**[11] je zelo primeren medij za shranjevanje privatnega ključa predvsem na strani odjemalca (uporabnika). Ponavadi vsebuje mikroprocesor, vhodno-izhodno enoto in pomnilnik. Zasnova je prilagojena potrebam po varnosti in namenu uporabe, v našem primeru hrambi privatnega ključa. Operacijski sistem poskrbi, da privatni ključ nikoli ne zapusti pametne kartice. Šifriranje se izvaja na kartici, razen časovno in prostorsko potratnejših operacij, ki se lahko prenesejo na računalnik z večjo zmogljivostjo.

Slika 5: Pametna kartica



Vir: http://valjhun.fmf.uni-lj.si/~ajurisic/sc/m1.pdf

Za uporabo pametne kartice je potrebno na računalnik uporabnika namestiti ustrezen gonilnik in programsko opremo. Ključ aktiviramo z vnosom gesla. V primeru večkratnega neuspešnega vnosa gesla se kartica samodejno zaklene. Sodobnejše kartice so zaščitene celo s čitalci prstnih odtisov.

[11] ISO 7816 - najpomembnejši standard za kontaktne pametne kartice. Opisuje položaj čipa in kontaktov, protokole itd.

Za shranjevanje privatnih ključev strežnikov so primernejši **strojni šifrirni moduli** (angl. Hardware Security Module). Obstajajo tudi programski moduli, vendar ne dosegajo takšne varnosti kot strojni moduli.

2.1.3 Časovni žig

Časovni žig je digitalni zapis, ki povezuje datum in čas podpisa z elektronskimi podatki na varen način. Potrjuje obstoj določene vsebine ob navedenem času, dokazuje, da je bil elektronski dokument kreiran v času, ko je bilo digitalno potrdilo še veljavno, ter ohranja veljavnost digitalnega podpisa v primeru preklica digitalnega potrdila (poglavje 2.2.2).

Časovni žigi se izdajo na zahtevo za potrebe posameznih aplikacij. S tehničnega vidika je postopek podoben digitalnemu podpisu. Modul za digitalno podpisovanje na strani uporabnika pošlje zahtevek za časovno žigosanje prstnega odtisa elektronskega dokumenta strežniškemu sistemu, ki je sinhroniziran z natančnim in zanesljivim časovnim virom. Časovni strežnik prstnemu odtisu dokumenta, ki je sestavni del zahtevka, dopiše podatke (datum, točen čas /najmanj na sekundo natančno/ idr.) in vse skupaj digitalno podpiše s svojim privatnim ključem. S tem je ustvarjena časovna sled dokumenta.

Odgovor časovnega strežnika, ki ga prejme aplikacija, sestoji iz:

- statusa o uspešnosti časovnega žiga;
- časovnega žiga (podatke o žigosanih poljih, digitalni podpis in digitalno potrdilo časovnega overitelja, podatke o časovnem žigu).

Slika 6: Časovno žigosanje

Vir.: http://www.si-tsa.si/osnove.htm

Vsebina in oblika časovnih žigov, ki se uporabljajo v internetu, sta določena v dokumentu RFC3161[12]. Zahtevek za časovni žig dokumenta vsebuje naslednje podatke (http://www.si-tsa.si/navodila.htm):

[12] RFC3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol.

- informacije o dokumentu (transformaciji, zgoščevalni funkciji, prstni odtis);
- naključno število za povezovanje zahtevka z odgovorom časovnega strežnika;
- neobvezna polja.

Veljavnost časovnega žiga se preverja na enak način kot digitalni podpis. Aplikacija preveri enakost prstnega odtisa v časovnem žigu s prstnim odtisom, ki ga je poslala časovnemu strežniku v zahtevku za časovno žigosanje dokumenta. Nato preveri še digitalno potrdilo časovnega strežnika in po potrebi še digitalna potrdila nadrejenih overiteljev (poglavje 2.2.1).

Časovno žigosanje opravljajo posebne agencije TSA (angl. Time-Stamp Authority). V Sloveniji sta v register overiteljev[13] vpisani dve agenciji:

- SI-TSA (angl. Slovenian Time Stamp Authority); ter
- POŠTA-CA - časovni žig.

2.2 Infrastruktura javnih ključev

Ena izmed glavnih komponent zaupanja je prepričanje, da podpis res pripada določenemu podpisniku sporočila. Ker digitalni podpis v primerjavi s klasičnim lastnoročnim podpisom ni biološko povezan s podpisnikom, je za nedvoumno povezovanje podpisnika z ustreznim parom podpisnih ključev potrebno overjanje javnih ključev. Preverjanje povezave med podpisnikom in ključem omogoča infrastruktura javnih ključev PKI (angl. Public Key Infrastrukture). To je celovit sistem na pravni, tehnični in organizacijski ravni, ki ustvarja varno okolje poslovanja celo v varnostno nezanesljivih javnih okoljih kot je internet. Temelj infrastrukture predstavlja veriga posebnih ustanov, imenovanih agencije. Sestavni deli so še digitalna potrdila, seznami preklicanih potrdil, aplikacije, ki podpirajo PKI, itd. Infrastruktura javnih ključev predstavlja osnovo za:

- šifriranje dokumentov in poštnih sporočil;
- digitalno podpisovanje dokumentov in poštnih sporočil;
- razpoznavanje udeležencev komunikacije oz. uporabnikov pri dostopu do aplikacij.

2.2.1 Agencije

Overitelji oz. **agencije za overjanje** javnih ključev – CA (angl. Certificate Authority) so posebne ustanove, ki svojim komitentom izdajo digitalno potrdilo o lastništvu javnega ključa. S tem zagotavljajo drugim udeležencem v elektronskem poslovanju, da javni ključ res pripada določeni osebi. Naloga overiteljev je tudi nadaljnje upravljanje s potrdili (hramba, objava v splošno dostopnih imenikih, preklic veljavnosti ipd), preverjanje identitete in druge storitve, ki jih določa politika overjanja.

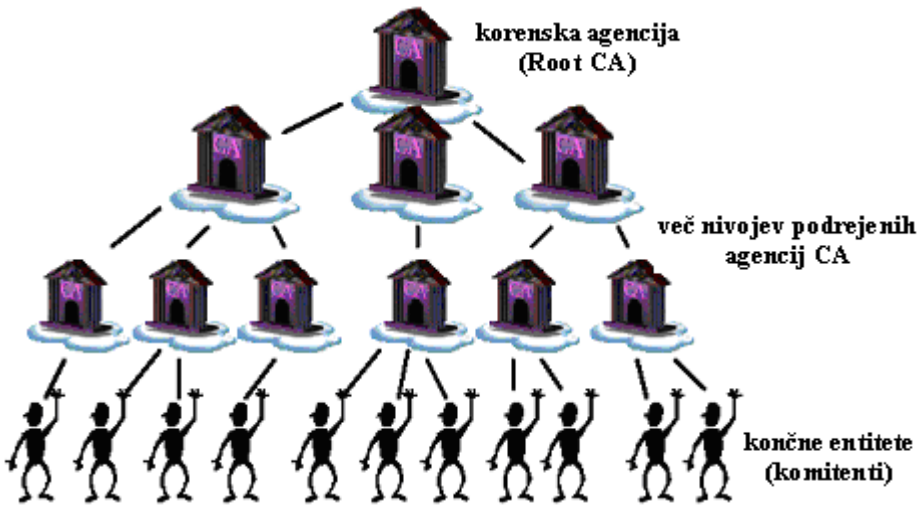
[13] Register overiteljev v Republiki Sloveniji - URL: http://mid.gov.si/mid/mid.nsf/V/K581418FEF1C225D7C1256E060030BDF5/$file/Register_Overiteljev.html

Registracijo klientov in druga, s tem povezana administrativna dela (preverjanja podatkov novih komitentov ipd.), lahko prevzamejo **uradi** oz. **agencije za registracijo** – RA (angl. Registration Authority), ki delujejo kot posredniki med klienti in agencijo CA. Takšni uradi so lahko bančne poslovalnice, poštni uradi ali upravne enote (Monitor 5-2001, str.5). Za posameznega overitelja lahko deluje več registrarjev RA.

Potrdila se lahko izdajo za različne namene. V Republiki Sloveniji trenutno delujejo štirje overitelji digitalnih potrdil:

- Ministrstvo za javno upravo, v okviru katerega delujeta dva izdajatelja digitalnih potrdil:
  - SIGOV-CA (angl. Slovenian GOVernmental Certification Authority) za javno upravo; ter
  - SIGEN-CA (angl. Slovenian GENeral Certification Authority) za pravne in fizične osebe;
- Halcom informatika d.o.o. - HALCOM-CA;
- Nova Ljubljanska banka d.d. - AC-NLB;
- Pošta Slovenije d.o.o. - POŠTA CA.

Slika 7: Koncept hierarhije zaupanja



Vir: http://www.isaca.be/Presentations/RT020525_PKITheory.pdf

Za overjanje ključev si izberemo tistega overitelja, ki mu zaupamo. Posledično zaupamo tudi vsem digitalnim potrdilom, katerih izdajatelj je naš overitelj. Zaradi predpostavke, da zaupamo tudi drugemu overitelju, če mu zaupa naš overitelj, se overitelji medsebojno priznavajo in tako gradijo verigo zaupanja znotraj infrastrukture PKI. Območje varnega poslovanja se tako širi. V praksi je najpogostejša hierarhična struktura povezovanja (slika 7), kjer višje agencije overjajo oz. izdajajo digitalna potrdila neposredno podrejenim agencijam. Slovenske overitelje tako združuje SI-CA, na območju Evrope EuroPKI itd. Najvišja v piramidi je korenska agencija (Root CA), ki si digitalno potrdilo izda sama.

2.2.2 Digitalno potrdilo

Digitalno potrdilo oz. certifikat, ki ga izda overitelj, je digitalno podpisan elektronski dokument, torej digitalna datoteka, ki povezuje javni ključ z identiteto imetnika potrdila. Potrdilo se lahko izda osebi, strežniku ali drugemu overitelju. Zaradi varnosti (dolžina ključa – poglavje 1.1.1.3) imajo takšna potrdila omejen čas veljave. V skladu z ZEPEP je rok veljavnosti digitalnega potrdila največ pet let. Potrdila, ki izpolnjujejo zakonske določbe v zvezi z vsebino in jih je izdal overitelj, ki prav tako izpolnjuje dodatne zakonske določbe, imenujemo kvalificirana digitalna potrdila. V praksi kvalificirana digitalna potrdila sledijo internetnemu standardu ISO X.509v3[14] in vsebujejo naslednja polja (Pavliha, 2002, str.41):

- različico formata po priporočilu X.509;
- serijsko oznako potrdila v okviru izdanih potrdil posameznega overitelja;
- identifikator algoritma, s katerim je bil narejen digitalni podpis overitelja;
- ime overitelja, ki je izdal potrdilo;
- obdobje veljavnosti potrdila;
- ime imetnika javnega ključa;
- javni ključ in identifikator algoritma, v katerem se ključ uporablja;
- neobvezni polji, ki omogočata ponovno uporabo že dodeljenih razločevalnih imen overitelja ali lastnika javnega ključa;
- neobvezne razširitve, ki vsebujejo dodatne informacije o javnem ključu in politikah, v skladu s katerimi je bilo potrdilo izdano, o imetniku in izdajatelju potrdila ter različnih omejitvah.

V praksi ločimo dve vrsti kvalificiranih potrdil, :

(1) spletna potrdila;
(2) osebna potrdila.

Pogosteje se uporabljajo **spletna potrdila**, ki so izdana največ za dobo petih let z možnostjo podaljšanja. Spletno potrdilo je povezano z enim parom ključev, ki se uporablja za šifriranje oz. dešifriranje sporočil, digitalno podpisovanje, varovanje povezav, avtentikacijo udeležencev varne povezave itd.

Za še višji nivo varnosti se uporabljajo **osebna potrdila**. Ta so izdana za dobo treh let. Z njimi je povezana uporaba dveh parov ključev: prvi par se uporablja za digitalno podpisovanje oz. overjanje podpisa, medtem ko se za (de)šifriranje uporablja drugi par ključev. Osebna potrdila se lahko uporabljajo za šifriranje oz. dešifriranje datotek in direktorijev, digitalno podpisovanje, varovanje povezav, avtentikacijo udeležencev varne

[14] X.509 – format in oblika potrdila sta opredeljena v dokumentu ITU T Recommendation X.509; ISO/IEC 9594-8: Information Technology – Open Sistem Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks (2001).

povezave itd. Osebno potrdilo se ponavadi hrani pri imetniku in ni objavljeno v javnem imeniku.

2.2.2.1 Preverjanje digitalnega potrdila

Za ugotavljanje verodostojnosti digitalno podpisanega dokumenta je poleg celovitosti digitalno dokumenta (primerjanje prstnega odtisa – poglavje 1.1.2), potrebno preveriti tudi veljavnost digitalnega potrdila podpisnika. Pri tem je potrebno biti pozoren predvsem na čas veljavnosti (angl. "Valid from", "Valid to") in morebiten preklic potrdila. Preverimo lahko tudi veljavnost digitalnega potrdila izdajatelja podpisnikovega potrdila ali vseh potrdil po verigi zaupanja navzgor vse do overitelja, ki mu zaupamo.

Digitalno potrdilo se lahko prekliče še pred potekom veljavnosti (npr. zaradi izgubljenega privatnega ključa). Prekliče ga lahko uporabnik ali overitelj. ZEPEP (Uradni list RS, št. 98/2004, 30. člen) določa, da mora overitelj kvalificiranih potrdil voditi register preklicanih potrdil. Vsebino registra in postopke preklica natančneje določajo standardi. Seznami preklicanih potrdil se objavijo v skladu s politiko certifikatne agencije. V praksi se za obveščanje o preklicanih potrdilih uporabljajo različni koncepti.

Sezname preklicanih potrdil - **CRL**[15] (angl: Certificate Revocation List) objavljajo pooblaščeni organi – overitelji na svojih spletnih strežnikih. Seznami so digitalno podpisani in časovno žigosani. Njihova slabost je njihova dolžina, s katero je povezan čas preverjanja potrdil in procesorsko obremenjevanje opreme.

Seznami CRL so lahko objavljeni tudi v posebnih imenikih tipa X.500[16], ki so prilagojeni hitremu in učinkovitemu iskanju informacije. Podatki so vneseni v hierarhično strukturo. Komunikacija med strežnikom X.500 in odjemalcem poteka po lahkem protokolu za dostop do imenikov **LDAP**[17] (angl. Lightweight Directory Access Protocol). Odjemalec pošilja zahtevke in prejema odgovore preko TCP protokola, s katerim vzpostavi sejo s strežnikom. Da bi bile zahteve na ustrezen način posredovane strežniku, je potreben vmesnik (angl. gateway), znan po imenu LDAP strežnik. Dandanašnji LDAP strežniki (angl. stand-alone) združujejo funkcijo vmesnika in imenika. Določeni so le s pravili LDAP protokola in niso več odvisni od standarda X.500. Za primere izpada povezljivosti s centralnim strežnikom se seznami CRL prenašajo na LDAP strežnike v lokalna omrežja (t.i. sinhronizacija seznamov). S tem se doseže večja neodvisnost od certifikatne agencije. V praksi se uporabljata dva modela:

- "Push model" – overitelj ažurira CRL in ga pošlje LDAP strežnikom;
- "Pull Model" – LDAP strežniki povprašujejo po CRL.

[15] CRL (Certificate Revocation List) – Request for Comments RFC2587.

[16] X.500 – standard ISO/IEC 9594.

[17] LDAPv3 – Request for Comments RFC 2251.

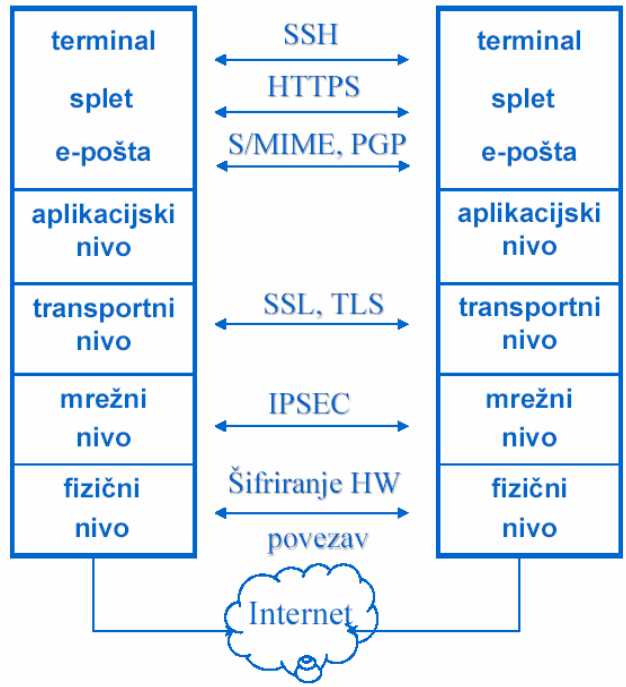
Ker so spletne povezave vedno hitrejše, se čedalje bolj uveljavlja storitev za takojšnje preverjanje veljavnosti potrdil po **OCSP**[18] protokolu (angl. On-line Certificate Status Protocol). Strežnik v lokalnem omrežju sproži poizvedbo pri pooblaščenem organu (overitelju potrdila) in dobi odgovor za natančno določeno potrdilo. Slabost je lahko počasna povezava kadar zahteva oz. išče odgovore več uporabnikov hkrati. OCSP strežnik je mogoče postaviti tudi v lokalnem omrežju in s tem doseči neodvisnost od centralnega strežnika. V tem primeru je potrebno zagotoviti sinhronizacijo imenikov.

Napredno validacijo varnostnih atributov omogoča tudi metoda **DVCS**[19] (angl. Data Validation and Certification Server Protocols), ki za izvajanje uporablja CRL in OCSP. Na zahtevo za preverjanje veljavnosti digitalnega podpisa in pripadajočih podatkov se posreduje podpisan odziv - DVC potrdilo (angl. Data Validation Certificate), ki vsebuje potrditev oz. zavrnitev. Komunikacija lahko poteka po poljubnem protokolu (npr. http, https ipd.)

2.3 Protokoli za zagotavljanje varnosti

Elektronskim dokumentom na njihovih poteh skozi omrežja pretijo nevarnosti kot so prestrezanje informacij, ponarejanje dokumentov, pretvarjanje, nepooblaščeno razkritje ipd.

Slika 8: Protokoli za zagotavljanje varnosti



Vir: http://lt.fe.uni-lj.si/gradiva/kso2/p_varnost_v_omrezjih_ip_v1.1.pdf

[18]OCSP (On-line Certificate Status Protocol) – Request for Comments RFC 2560.

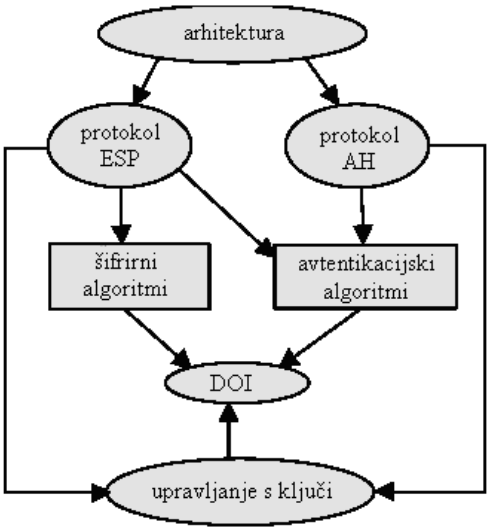
[19] DVCS (Data Validation and Certification Server Protocols) - Request for Comments RFC 3029.

Zgolj implementacija varnostnih mehanizmov v aplikacije ne zadošča, za varnost je potrebno poskrbeti na vseh ravneh ISO/OSI modela (slika 8). Za zaščito na komunikacijskih poteh uporabljamo protokole, ki zagotavljajo avtentikacijo obeh strani komunikacije in podatke pošiljajo po varnih kanalih. To je pomembno zlasti takrat, kadar dokumente pošiljamo prejemniku preko javnega omrežja.

2.3.1 Protokoli IPsec

IPsec (angl. IP Security) je skupina protokolov za varovanje podatkov na mrežnem nivoju ISO/OSI modela. Uporablja se za vzpostavljanje navideznih zasebnih omrežij VPN (angl. Virtual Private Network). Mednarodna organizacija za standardizacijo v internetu IETF (angl. Internet Engineering Task Force) jih razvija kot del prihajajočega standarda IPv6[20] (RFC1883). Uporabljajo jih že različni produkti, ki podpirajo standard IPV4.

Slika 9: Gradniki tehnologije IPSec



Vir: http://www.ltfe.org/pdf/Varnost_IPsec.pdf

Tehnbologijo IPsec opisuje več RFC (angl. Request for Comments) dokumentov, ki so logično razvrščeni v naslednje skupine (http://www.ltfe.org/pdf/Varnost_IPsec.pdf):

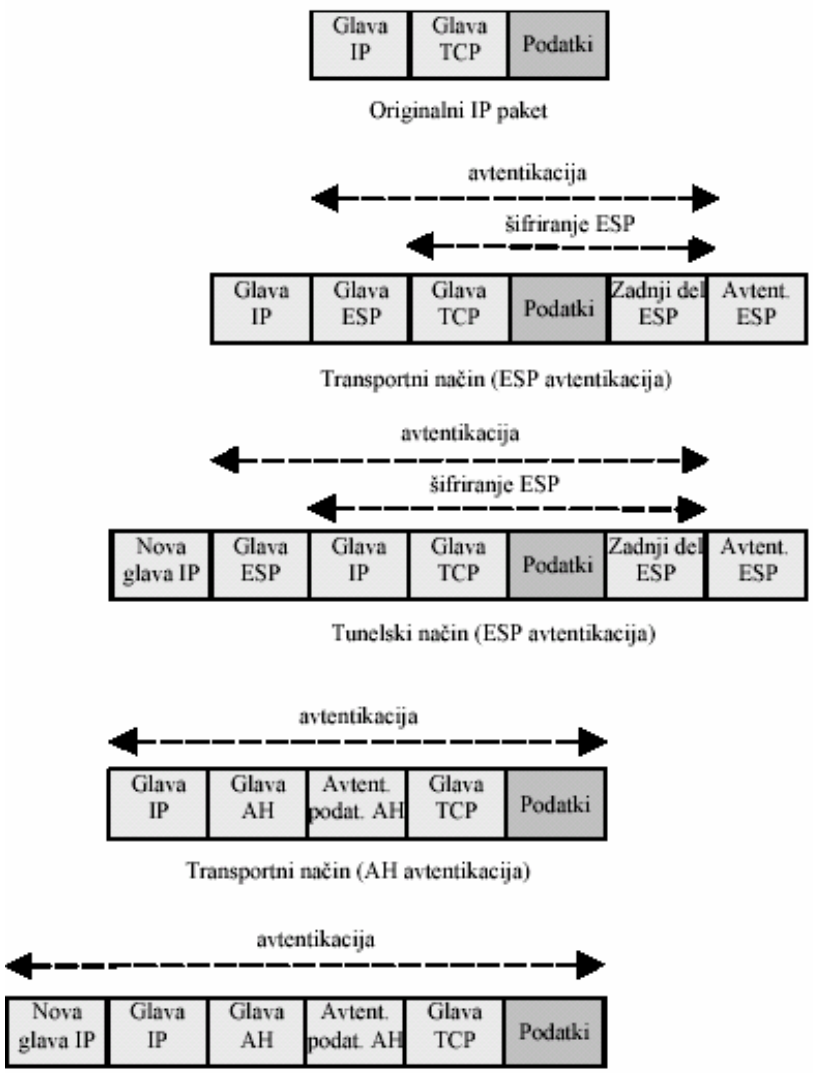
- arhitektura – pokriva vse vidike tehnologije in varnosti;
- protokol avtentikacijskega čela AH (angl. Authentication Header);
- protokol za šifriranje koristne vsebine ESP (angl. Encapsulating Security Payload);
- šifrirni algoritmi;
- avtentikacijski algoritmi;
- domena interpretacije DOI (angl. Domain of Interpretation) – dokument za sodelovanje posameznih gradnikov;

[20] IPv6 – Request for Comments RFC1183

- upravljanje s ključi (angl. Key Management) – dogovor o načinu šifriranja in izmenjava ključev.

IPsec vključuje uporabo že uveljavljenih algoritmov za avtentikacijo in šifriranje podatkov. Ob vzpostavi varnostne zveze se najprej opravi avtentikacijski proces, nato se prične prenos podatkov. Vsaka vzpostavljena zveza predstavlja enosmerno komunikacijo. V primeru dvosmerne komunikacije je potrebno vzpostaviti dve varnostni zvezi.

Slika 10: Ovijanje pri transportnem in tunelskem načinu povezovanja



Vir: http://www.ltfe.org/pdf/Varnost_IPsec.pdf

Za avtentikacijo in integriteto (nespremenjenost) podatkov skrbi protokol AH, medtem ko protokol ESP skrbi zgolj za šifriranje podatkov. Poleg dejanske vsebine se lahko šifrira tudi glava IP paketa. Celotni IP paket se v tem primeru ovije v nov IP paket. Protokola se lahko uporabljata ločeno ali v kombinaciji. IPsec definira dva načina vzpostavitve varnostne zveze:

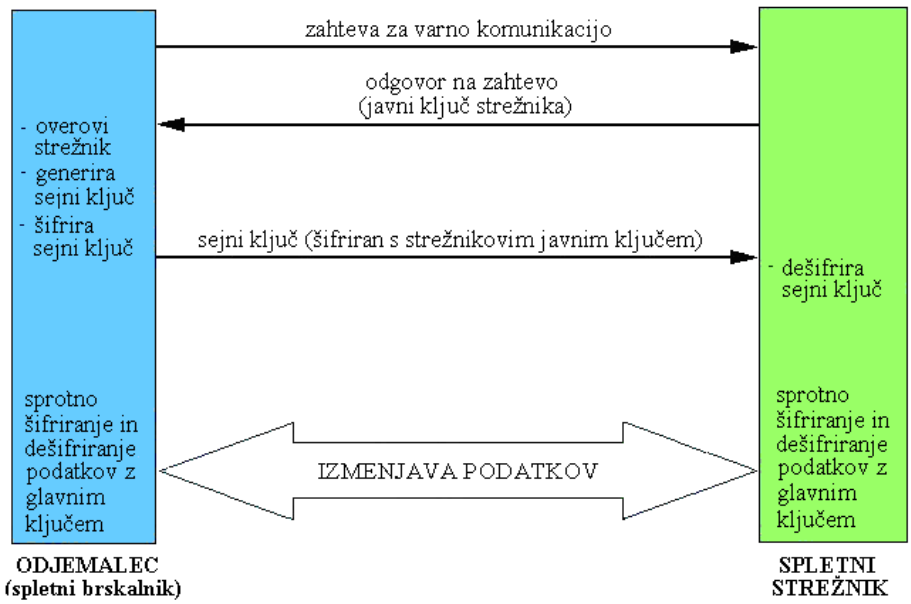
- transportni način - za zaščito povezave med končnimi sistemi (npr. strežnikom in odjemalcem) brez posrednikov;
- tunelski način - za zaščito povezave med računalniki iz različnih omrežij (prenos podatkov skozi varnostne prehode).

Uporablja se tudi povezava več lokacij z mrežo tunelov ali zvezdasta povezava oddaljenih lokacij okoli centralne lokacije.

2.3.2 Protokol SSL/TLS

Protokol SSL (angl. Secure Socket Layer) se uporablja za vzpostavitev varne povezave na internetu ali intranetih med spletnim strežnikom in spletnim odjemalcem. Ko odjemalec pošlje strežniku zahtevo za komunikacijo, se ta odzove tako, da pošlje svoj javni ključ. Odjemalec generira simetrični ključ za šifriranje podatkov in ga asimetrično šifriranega s prejetim javnim ključem pošlje strežniku. Izmenjani podatki so šifrirani simetrično. Celotna komunikacija je prikazana na sliki 11.

Slika 11: Komunikacija po protokolu SSL



Vir: http://ecom.fov.uni-mb.si/ecomSLO/Studenti/Predmeti/Prezentacije/Varnost%20interneta.ppt

Protokol SSL zagotavlja naslednje varnostne storitve (http://www.microsoft.com/technet/security/topics/cryptographyetc/certs.mspx):

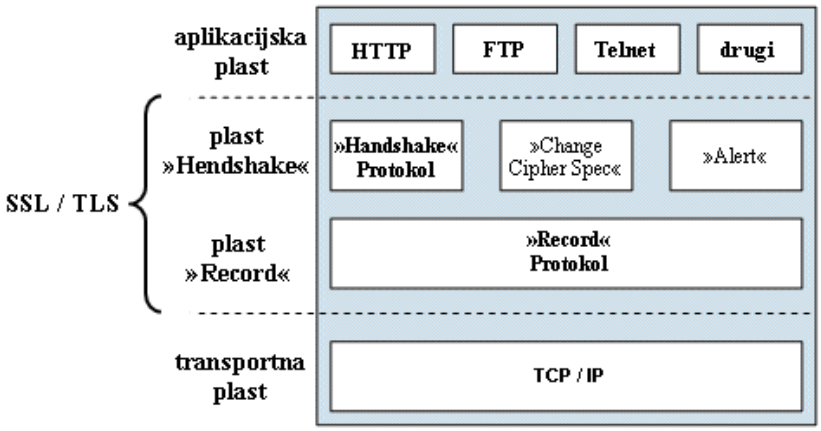
- medsebojno avtentikacijo - preverjanje identitete obeh strani komunikacije z izmenjavo in preverjanjem digitalnih potrdil,
- zaupnost komunikacije - izmenjava šifriranih podatkov med strežnikom in klientom po varnem kanalu,

- celovitost komunikacije - preverjanje celovitosti vsebine izmenjanega sporočila z jamstvom, da sporočilo ni bilo spremenjeno.

SSL sestoji iz dveh plasti protokolov med aplikacijskim in trasportnim nivojem:

- plast **"Handshake"**:
  (1) "Handshake" protokol;
  (2) "Change Cipher Spec" protokol;
  (3) "Alert" protokol;
- plast "**Record"**:
  (1) "Record" protokol.

Slika 12: Plasti protokolov SSL in TLS



Vir: http://202.41.85.117/~hussam/sslws03.mspx.html#EGAA

T.i. "Handshake" protokol preverja identiteto udeleženih subjektov (strežnika in odjemalca), uskladi uporabo algoritmov, ter poskrbi za prenos digitalnih potrdil in varno izmenjavo simetričnega ključa seje. Protokola "Change Cipher Spec Protocol" in "Alert Protocol" skrbita za sporočanje. Prvi potrjuje nadaljevanje postopka s pravkar dogovorjenimi parametri. Drugi zaključuje povezavo v primeru napak (uporaba različnih algoritmov ipd.). "Record Protocol" definira osnovni format izmenjanih podatkov ter skrbi za šifriranje in neokrnjen prenos podatkov.

Protokol SSL prepoznamo po določilniku protokola v naslovu "https", namesto "http". Trenutno se uporablja SSL verzijo 3.0, ki jo podpira večina sodobnih spletnih brskalnikov (MS Internet Explorer 6.x, Netscape, Mozzila itd.). Naslednika protokola SSL sta TLS (angl. Transport Layer Security), ki se uveljavlja predvsem na področju tehnologij strežnikov imenikov, in WTLS (angl. Wireless Transport Layer Security), ki je namenjen brezžičnim komunikacijam.

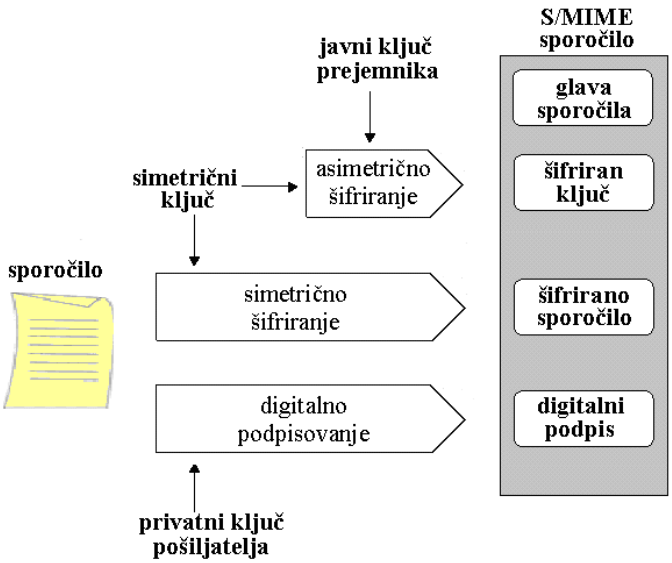
2.3.3 S/MIME (Secure Multipurpose Internet Mail Extensions)

S/MIME[21] (angl. Secure Multi-Purpose Internet Mail Extensions) je internetni protokol, ki določa obliko sporočil za varno izmenjavo med različnimi poštnimi sistemi. Danes ga praktično podpirajo že vsi odjemalci elektronske pošte.
Protokol S/MIME deluje na aplikacijskem nivoju ISO/OSI modela. Za varovanje uporablja mehanizme za šifriranje in digitalno podpisovanje. Poleg digitalnega podpisa se v S/MIME sporočilo pripne tudi digitalno potrdilo pošiljatelja, ki vsebuje javni ključ. Protokol je prilagojen uporabi digitalnih potrdil X.509.

Sporočilo nastane tako, da se vsebina digitalno podpiše in šifrira s simetričnim ključem. Nato se porabljeni simetrični ključ asimetrično šifrira z javnim ključem prejemnika in pošlje skupaj z vsebino sporočila. Kreirano sporočilo tako vsebuje:

- glavo sporočila (podatki o pošiljatelju, prejemniku in vsebini sporočila);
- asimetrično šifriran simetrični ključ za dešifriranje sporočila;
- simetrično šifrirano vsebino sporočila;
- digitalni podpis.

Slika 13:Oblika sporočila S/MIME



2.3.4 SOAP

SOAP (angl. Simple Object Acces Protocol) je enostaven protokol za izmenjavo XML sporočil med aplikacijami, ki delujejo na različnih operacijskih sistemih in so napisane v različnih programskih jezikih. Definirano je le ogrodje, zato je forma izredno fleksibilna. Na aplikacijskem nivoju pogosto izkorišča protokol HTTP, ki ga podpirajo vsi spletni brskalniki.

[21] S/MIME (Secure Multi-Purpose Internet Mail Extensions) – Request for Comments RFC1847, RFC1848.

Komunikacija poteka tako, da prvi udeleženec komunikacije pošlje zahtevo, na katero se odzove drugi udeleženec komunikacije.

Primer zahtevka za komunikacijo:
(http://www.w3schools.com/soap/soap_httpbinding.asp)

POST /item HTTP/1.1
Host: 189.123.345.239
Content-Type: text/plain
Content-Length: 200

Primer odgovora:
(http://www.w3schools.com/soap/soap_httpbinding.asp)

a) za uspešeno vzpostavljeno komunikacijo:

200 OK
Content-Type: text/plain
Content-Length: 200

b) za neuspešno vzpostavljeno komunikacijo:

400 Bad request
Content-Length: 0

Sporočilo se izmenja v SOAP ovojnici. Ovojnica ima XML sintakso (več v poglavju 4.1.1) in sestoji iz 4 osnovnih elementov:

- osnovni element SOAP – za identifikacijo SOAP sporočila,
- glava ovojnice – vsebuje informacije o sporočilu (npr. podatke za avtentikacijo),
- jedro,
- napake.

2.4 Zaključek poglavja 2

Zaključen je kratek pregled mehanizmov in protokolov za izgradnjo varnega okolja za elektronsko poslovanje in pomen infrastrukture javnih ključev. Opisani postopki se uporabljajo predvsem v aktivnih fazah življenjskega cikla elektronskega dokumenta, torej v času nastanka in uporabe dokumenta. Dokumente je potrebno varovati tudi v pasivnih fazah njihovega življenjskega cikla, kamor uvrščamo hrambo.

V nadaljevanju je predstavljena problematika dolgotrajne hrambe elektronskih dokumentov ter nekatere rešitve, ki prav tako temeljijo na uporabi infrastrukture javnih ključev.

3 ARHIVIRANJE DIGITALNO PODPISANIH DOKUMENTOV

Dokumente, ki imajo trajnejšo vrednost, je potrebno v skladu z zakonodajo arhivirati. Arhiviranje opredelimo kot postopek prevzemanja, hranjenja, vzdrževanja, obdelave in uporabe dokumentarnega in arhivskega gradiva (Jerman Blažič, 2005, str. 2-II). Postopki so v klasičnem poslovanju s papirnimi dokumenti postali že dolgoletna in preizkušena praksa, vendar elektronskega gradiva (zaradi drugačne narave) ne moremo hraniti na enak način. Razlike med okolji so prevelike, zato potrebujemo nova pravila, ki bodo zagotavljala kvalitetno arhiviranje elektronskega gradiva in hkrati ohranjala pravno veljavnost elektronsko podpisanih dokumentov v času zakonsko predpisane hrambe. Glede na določbe v 10. členu UNCITRAL-1 (poglavje 5.1.1), enega prvih dokumentov, ki formalno postavlja pravila elektronskega poslovanje, in v 12. členu ZEPEP (poglavje 5.2.1) mora hramba elektronskega gradiva izpolnjevati naslednje pogoje:

- podatki oz. dokumenti morajo biti dostopni na uporaben način in primerni za kasnejšo rabo;
- podatki morajo biti shranjeni v izvorni obliki ali v drugi obliki, ki lahko verodostojno predstavi izvorno obliko;
- možno je ugotoviti izvor in cilj poslanega sporočila, ter čas prenosa ali prejema;
- uporabljena tehnologija in postopki morajo zanesljivo zagotavljati nespremenljivost sporočila.

Današnja tehnologija omogoča, da elektronsko arhiviranje gradiva zmanjšuje glavne funkcionalne pomanjkljivosti klasičnih arhivov (npr. kompleksno upravljanje z gradivom, čas iskanje informacij, prostor ipd.); žal je z vidika varnosti še vedno premalo raziskano. Zanesljivost trajnejše hrambe (več kot 10 let) zastavlja kopico pravnih, organizacijskih in tehnoloških vprašanj. Življenjska doba digitalnega potrdila, ki je ključen za dokazovanje avtentičnosti digitalno podpisanih dokumentov, prej ali slej poteče, privatni podpisni ključ je lahko ukraden, njegova stopnja varnosti se, zaradi nenehnega napredka tehnologije, s časom zmanjšuje. Če dodamo še zastarevanje medijev ter strojne in programske opreme, ugotovimo, da je digitalni podpis brez nadaljnje podpore neprimerna forma za arhiviranje.

3.1 Problemi arhiviranja elektronskega gradiva

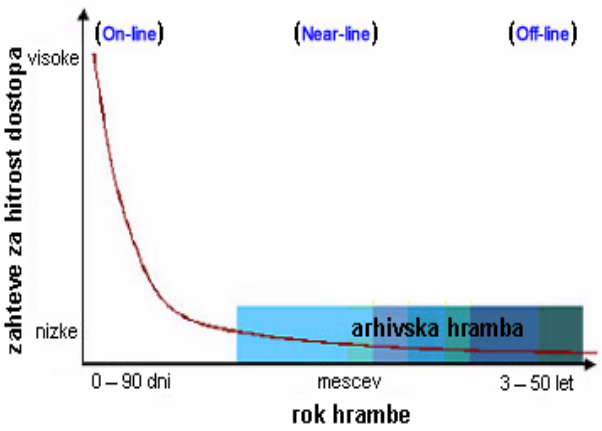
Pomanjkanje zagotovil za trajno ohranjanje elektronskih dokumentov v nekaterih primerih upravičeno vnaša dvome in zadržke. Natančno je potrebno raziskati predvsem pomanjkljivosti elektronske hrambe v primerjavi s klasično hrambo ter razlike med kratkotrajno in dolgotrajno hrambo elektronskega gradiva.

Pristopi, ki so primerni za krajši rok hrambe (npr. 5 let), v daljšem časovnem obdobju prinašajo tveganja, ki so opisana v nadaljevanju.

a) Fizična obstojnost nosilcev podatkov

Za razliko od papirja, ki se je pokazal kot odličen nosilec, na katerem je mogoče ohraniti zapise več stoletij, se pri elektronski hrambi srečujemo s problemom relativno hitrega propadanja zapisov zaradi omejene življenjske dobe in velike odvisnosti kvalitete elektronskih nosilcev od parametrov okolja (temperatura, vlaga itd.), v katerem jih hranijo.

Slika 14: Prioritete v različni hrambi



Prioritete za hrambo aktivnih podatkov:
- neprekinjena dostopnost;
- visoka učinkovitost branja / pisanja in dostopa.

Prioritete za varnostne kopije:
- visoka kapaciteta medija;
- visoka učinkovitost branja / pisanja;
- nizka cena na GB podatkov.

Prioritete za arhiviranje podatkov:
- avtentičnost podatkov;
- daljša življenjska doba medijev;
- visoka učinkovitost branja na zahtevo;
- nizka cena.

Vir: http://www.udo.com/compete/index_right.html

S časom postaja možnost napak pri branju s posameznih medijev večja, zato je za daljšo hrambo elektronskega gradiva potrebno izbrati visoko zanesljivo tehnologijo. Pri tem je potrebno upoštevati prioritete (avtentikacija, trajnost podatkov, fleksibilnost ipd.), ki so popolnoma drugačne od zahtev za hrambo aktivnih podatkov ali njihovih varnostnih kopij.

b) Zastarevanje strojne opreme

Kot posledica nenehnega razvoja tehnologije, se pri dolgotrajnejši hrambi elektronskega gradiva pojavlja zastarevanje strojne opreme (npr. pogonske enote za medije). Produkti na tržišču imajo omejeno dobo trajanja, nato jih zamenjajo nove – izboljšane verzije ali tehnološko popolnoma drugačni produkti. Vzdrževanje zastarelih produktov postane s časom varnostno (prenizka stopnja varnosti) ali ekonomsko (učinkovitost, cena popravil) neupravičeno. Zahtevani rok hrambe elektronskega gradiva lahko preseže dobo obstoja potrebne tehnične opreme. Daljši je čas arhiviranja, večji je problem zastarevanja opreme.

c) Zastarevanje formata

Zastarevanje formata predstavlja največji problem hrambe elektronskega gradiva. Je posledica razvoja komponent programske opreme, ki omogoča prikaz informacij, shranjenih na mediju. Komponente obsegajo (Arhiv Republike Slovenije, 2005, str. 63):

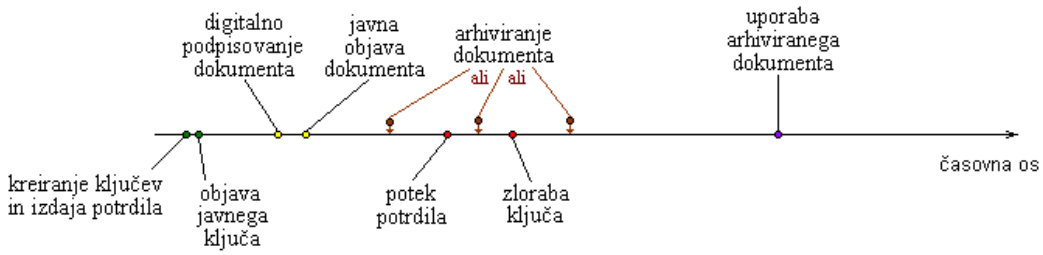
- standarde programiranja;
- formate datotek;
- aplikacije;
- baze podatkov in preostalo storitveno programsko opremo;
- operacijske sisteme.

Nekatere na novo razvite komponente so kompatibilne s prejšnjimi verzijami in omogočajo prikaz določenih starejših informacij. Pogosto se tudi zgodi, da s sodobno opremo ne moremo prebrati vsebine, ki je bila ustvarjena pred nekaj leti.

d) Problem stabilnosti zapisov

Večji problem trajnejše hrambe elektronskega gradiva predstavlja tudi stabilnost zapisov oz. integriteta podatkov. S časom hrambe se veča nevarnost poškodbe (spremembe) zapisa, zanikanja obstoja podatkov ali zlorabe varnostnih elementov. Stopnja varnosti posameznega elektronskega zapisa je v določenem trenutku odvisna od varnosti uporabljene tehnologije (algoritma, dolžine uporabljenega ključa itd.); ne glede na to dejstvo, je potrebno zagotoviti nespremenljivost vseh shranjenih podatkov v času predpisane hrambe. Medtem, ko nepodpisani zapisi sploh nimajo elementov za preverjanje integritete podatkov, predstavlja problem pri preverjanju digitalno podpisanih dokumentov časovna omejenost ali preklic digitalnega potrdila (poglavje 2.2.2). Digitalno potrdilo lahko postane neveljavno pred iztekom roka predpisane hrambe dokumenta: s tem preneha tudi veljavnost digitalnega podpisa.

Slika 15: Problem časovno omejene veljavnosti digitalnega potrdila



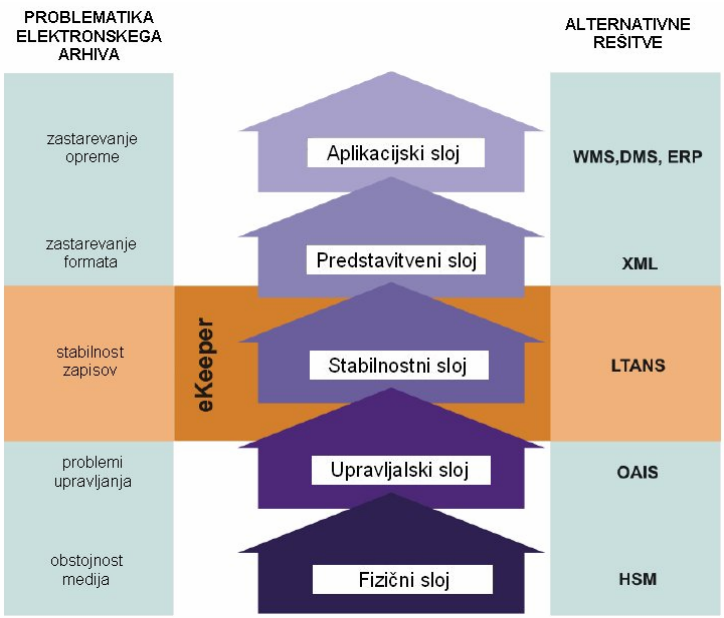
3.2 Varna hramba elektronskega gradiva

Našteti problemi elektronskega arhiviranja dokumentov vzbujajo dvome o primernosti tovrstne hrambe. Varna hramba elektronskega gradiva je kompleksno področje, ki zahteva zanesljivejšo infrastrukturo, ki bo sposobna zagotoviti trajno hrambo različnih elektronskih zapisov in vseh pripadajočih atributov. Osnovni elementi takšne infrastrukture so arhivski objekti (primarni podatki, metapodatki, digitalni podpis in drugi atributi, potrebni za varno arhiviranje) in komunikacijski protokoli. Drugi elementi, ki služijo za podporo infrastrukturi, so komunikacijsko omrežje, varnostni mehanizmi, časovni žig ter arhivski sistem (http://www3.ietf.org/proceedings/05aug/slides/ltans-4/sld4.htm).

V okviru infrastrukture lahko celotno problematiko elektronskega arhiviranja obravnavamo v okviru najmanj petih tehnoloških slojev (Jerman Blažič, 2005, str. 4-II):

- **fizični sloj** rešuje probleme zapisovanja podatkov na ustrezne medije glede na razpoložljivo infrastrukturo, hitrost dostopa ipd;
- **upravljavski sloj** dopolnjuje spodaj ležečo fizično infrastrukturo z logičnim upravljanjem hrambe elektronskega gradiva;
- **stabilnostni sloj** zagotavlja avtentičnost gradiva na dolgi rok,
- **predstavitveni sloj** in
- **aplikativni sloj** dopolnjujeta temeljno infrastrukturo na nivoju uporabnika, saj zagotavljata dolgoročno berljivost gradiva in integracijo arhivskih funkcij v aplikativno okolje.

Slika 16: Večplastna problematika elektronskega arhiviranja in alternativne rešitve



3.2.1 Fizični sloj

Izbira tehnologije za varovanje zapisov na fizičnem sloju je odvisna od potreb in želja. Medtem ko se za vsakdanjo rabo pogosto uporablja RAID (angl. Redundant Array of Independent Disc) sisteme ali magnetne medije, se za daljše arhiviranje zahteva nosilce, ki so kompatibilni s pričakovano dobo hrambe in ne omogočajo spreminjanja vsebine Za dolgoročnejšo hrambo se priporoča uporaba vrhunske t.i. WORM tehnologije (angl. Write Once Read Many), med katero uvrščamo magneto-optične MO (angl. Magneto-Optical) diske, UDO (angl. Ultra Density Optical) nosilce ipd.

Vsi elektronski mediji imajo omejeno življenjsko dobo. Ta je odvisna od lastnosti medija in pogojev hrambe. Življenjsko dobo medijev podaljšamo s hrambo v predpisanih pogojih

(temperatura, vlažnost, čistoča prostora itd.). Trajnejša hramba zapisov zahteva rutinsko menjavanje medijev oz. prepisovanje arhivskega gradiva na nove medije pred pričakovanim iztekom življenjske dobe. Priporočljiva je hramba več kopij na različnih nosilcih in fizično shranjevanje na ločenih lokacijah. To zahteva uporabo avtomatiziranih sistemov, ki samodejno nadzorujejo in odpravljajo napake, kjer je to mogoče.

Tabela 3: Primerjava arhivskih lastnosti različnih tehnologij

Arhivske lastnosti	RAID	Magnetni trak	DVD	MO	UDO
enkratni zapis	ne	ne	da	ne	da
dolga življenjska doba	ne	ne	da	da	da
zamenljivost medija	ne	da	da	da	da
profesionalna kvaliteta	da	da	ne	da	da
kapaciteta medija	srednja/visoka	visoka	nizka	nizka	srednja
hitrost branja / pisanja	visoka	visoka	nizka	srednja	srednja
hitrost dostopa / branja	visoka	nizka	nizka	srednja	srednja
cena sistema	visoka	nizka	nizka	nizka/srednja	nizka

Vir: http://www.plasmon.com/downloads/pdf/archivaltrends.pdf

3.2.2 Upravljavski sloj

Za upravljanje hrambe elektronskega gradiva je odbor CCSDS (angl. Consulative Comitee for Space Data Sistems) ameriške vesoljske agencije NASA (angl. National Aeronautics and Space Administration) predstavil odprt referenčni model OAIS[22] (angl. Open Archival Information System).

Model OAIS je konceptualni okvir za razumevanje trajnega arhiviranja digitalnega gradiva, namenjen je za oporo pri implementaciji elektronskih arhivov, medtem ko tehnologije ne določa. Gre za splošen model, ki definira potreben nabor elementov elektronskega arhiva in funkcij za varne arhivske storitve TAS (angl. Trusted Archival Services), vključno z minimalnim naborom odgovornosti tovrstnih arhivov.

3.2.2.1 Predstavitev referenčnega modela OAIS

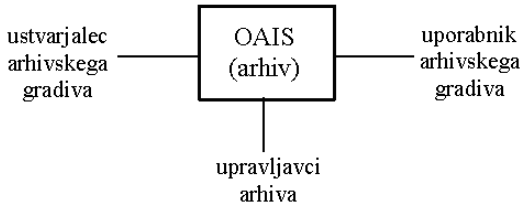
Sistem OAIS je utemeljen s tremi osnovnimi modeli, ki opisujejo:

- okolje arhivskega sistema;
- koncept informacije;
- temeljne funkcije arhiva.

[22] OAIS – priporočilo: CCSDS 650.0–B–1,Blue Book, Issue 1, 2002; sprejet ISO standard: ISO 14721:2003.

Prvi model v okviru referenčnega modela OAIS je **okolje sistema za arhiviranje**. V procesu arhiviranja sodelujejo ustvarjalci arhivskega gradiva, uporabniki arhivskega gradiva in upravljavci arhiva. Enostaven model, ki povezuje navedene entitete je prikazan na sliki 17.

Slika 17: Okolje sistema OAIS



Vir: http://www.ccsds.org/documents/650x0b1.pdf

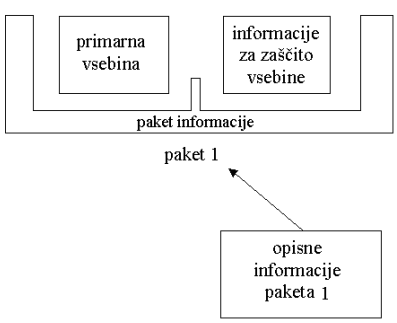
Po potrebi lahko posamezni OAIS arhivi med sabo sodelujejo v skladu z medsebojnimi dogovori. Tako lahko na primer posamezen OAIS arhiv prevzame vlogo ustvarjalca ali vlogo uporabnika arhivskega gradiva v okolju nekega drugega OAIS arhiva.

OAIS **model informacije** sloni na konceptu, da je informacija v splošnem sestavljena iz primarnega podatkovnega objekta (vsebine) in predstavitvenih informacij (t.i. meta podatkov), ki programski opremi povedo, kako lahko vsebino prikaže. Za arhiviranje elektronskega gradiva sta ta dva objekta premalo. Dodati je potrebno informacije o tem, kako naj se gradivo hrani, kako se lahko gradivo najde itd. OAIS model informacijskega objekta tako sestoji iz:

- paketa informacij, ki zajema primarno vsebino in njene predstavitvene podatke;
- informacij za zaščito vsebine PDI (angl. Preservation Description Information), ki vsebujejo informacije o uporabljenih mehanizmih, izvoru idr;
- paketa informacije (angl. Packaging Information), ki povezujejo logične in fizične komponente informacij;
- opisnih informacij paketa DI (angl. Descriptive Information), ki služijo za iskanje, lociranje ipd.

Strukturo informacije, ki je opremljena tudi s podatki za dolgotrajno hrambo in kasnejši dostop do objekta, lahko imenujemo paket informacije in tudi ta potrebuje opisne informacije. Struktura celotne informacije je prikazana na sliki 18.

Slika 18: Konceptualni prikaz informacije



Vir: http://www.ccsds.org/documents/650x0b1.pdf

Ker posamezne funkcije arhiva (sprejem, arhiviranje, izdaja) potrebujejo le nekatere metapodatke, nastopajo paketi informacij v različnih oblikah:

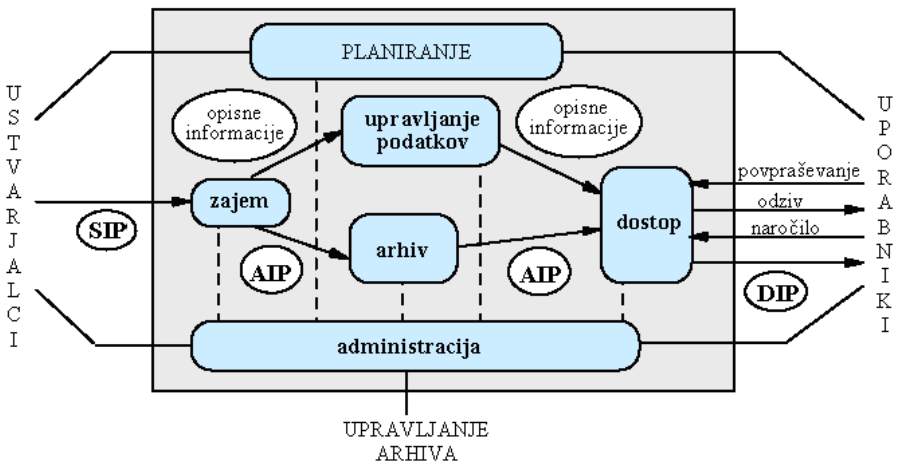
- sprejemni informacijski paket **SIP** (angl. Submission Information package) običajno potuje od ustvarjalca gradiva do arhiva in med drugim vsebuje metapodatke za sprejem informacije v arhiv;
- arhivski paket informacije **AIP** (angl. Archival Information Package) zadovoljuje notranje standarde OAIS arhiva in med drugim vsebuje metapodatke za trajno hrambo informacije;
- oddajni paket informacije **DIP** (angl. Dissemination Information Package) je prilagojen dogovorjenim zahtevam uporabnika in vsebuje podatke za zunanjo uporabo informacije.

Paketi informacij lahko glede na fazo arhiviranja spreminjajo svojo obliko. Tako je mogoče iz enega ali več SIP paketov oblikovati enega ali več AIP paketov in prav tako se lahko iz različnega števila AIP oblikuje različno št. DIP paketov.

Funkcijski model OAIS natančneje prikazuje delovanje arhiva (osrednjega elementa iz modela okolja). Njegov namen je približati nabor funkcijskih entitet s praktičnega vidika in glavne komunikacijske poti, po katerih potujejo informacije.
Za zagotavljanje temeljnih funkcij arhiva (prevzem, hramba, vzdrževanje, strokovna obdelava in uporaba arhivskega gradiva) OAIS model definira šest funkcijskih entitet:

- modul za zajem gradiva;
- podatkovno skladišče – arhiv;
- modul za upravljanje s podatki;
- modul za dostop do podatkov;
- administracija;
- planiranje zaščite arhiva.

Slika 19: Funkcijske entitete in paketi informacij



Vir: http://www.ccsds.org/documents/650x0b1.pdf

Modul za zajem gradiva je vmesnik med ustvarjalcem arhivskega gradiva in sistemom OAIS. Njegova naloga je sprejem elektronskih dokumentov v predpisani (dogovorjeni) obliki ter priprava in preoblikovanje dokumentov v ustrezno obliko za shranjevanje. Modul najprej opravi postopek indeksacije, nato posamezne informacijske pakete opremi z atributi za upravljanje in zaščito podatkov.

Osrednja entiteta arhiva je podatkovno skladišče. Njegova osnovna naloga je hramba podatkov (dokumentov). Pomemben del arhiva je funkcija upravljanja s podatki, ki deluje na podlagi metapodatkov. Za lažje obvladovanje arhiva in zagotavljanje verodostojnosti hranjenih zapisov so potrebne naslednje vrste metapodatkov (http://www.infotehna.si/Datoteke/SLO/pdf/clanek/varno%20arhiviranje.pdf):

- atributi, ki opisujejo arhivirano gradivo in so namenjeni iskanju, pregledovanju in naročanju arhivskega gradiva (avtor, datum arhiviranja,…);
- atributi, ki ščitijo arhivirano gradivo in so namenjeni zagotavljanju celovitosti arhiviranega gradiva;
- informacije o politiki (dostopne omejitve itd.);
- podatki o zahtevah in prenosu podatkov, ki vključujejo sledljivost sleherne transakcije med arhivom in uporabnikom;
- statistične informacije v zvezi z arhivom (časi prenosa, zasedenost prostora na diskih,…);
- informacije o uporabnikih, ki zagotavljajo identifikacijo uporabnikov in njihovih pravic (uporabniška imena, gesla ipd.).

Modul za dostop do arhivskega gradiva je vmesnik, preko katerega uporabniki iščejo in naročajo arhivirane dokumente. Običajno vključuje iskalne mehanizme in zaščito dostopa. Za izvajanje vseh potrebnih operacij v arhivskem sistemu skrbi upravljavska enota administracija. Za pripravo strategije tehnološkega posodabljanja arhiva skrbi entiteta za planiranje zaščite arhiva.

Med entitetami, ki jih opisuje model okolja OAIS, in opisanimi moduli znotraj funkcijskega modela OAIS potujejo paketi informacij (slika 19). Klient posreduje gradivo v paketih, oblikovanih za sprejem (SIP). Vmesnik jih sprejme, iz njih kreira arhivske pakete (AIP), ki jih pošlje podatkovni shrambi: z njimi povezane opisne informacije pošlje upravi podatkov. Ko uporabnik izda zahtevo za iskanje določenih informacij, podatkovna shramba obnovi določen (AIP) in ga pošlje enoti za dostop, ki paket preslika v obliko za oddajo informacij. Vse aktivnosti vodi upravljavska enota (administracija).

3.2.2.2 Naloge elektronskega arhiva OAIS

OAIS priporočila podajajo tudi minimalen nabor odgovornosti za organizacije, ki upravljajo arhive v skladu z OAIS priporočili

- arhiv lahko od ustvarjalca gradiva sprejme le ustrezne (dogovorjene) informacije;

- zagotoviti mora zadostno kontrolo informacij na nivoju, ki je potreben za trajno hrambo elektronskega gradiva;
- določiti mora nabor in pravice uporabnikov;
- zagotavljati mora razumljivost shranjenih informacij, brez dodatne podpore strokovnjakov ali ustvarjalcev gradiva;
- upoštevati mora dogovorjene politike in postopke arhiviranja, ter zagotavljati avtentičnost shranjenih objektov;
- določenemu naboru uporabnikov mora omogočati dostop do shranjenih informacij.

3.2.3 Stabilnostni sloj

V zadnjih letih lahko na mednarodnem nivoju zasledimo kar nekaj iniciativ in projektov za reševanje problemov elektronske hrambe gradiva. Analizo funkcionalnih zahtev, potrebnih za postavitev standardov na tem področju, je že leta 2000 pripravila organizacija EESSI (angl. European Electronic Signature Standardization Initiative) v poročilu z naslovom "Trusted Archival Services (TAS), Phase #3, Final report". Poročilo priporoča ohranjanje digitalnega podpisa v originalni obliki in določa dodatne naloge sistemov, ki bodo skrbeli za legitimnost in uporabnost tudi po daljšem obdobju od nastanka (DOK-SIS 03, str IV-33).

3.2.3.1 Storitve za zagotavljanje varnosti

Za varno arhiviranje digitalno podpisanega gradiva je običajnim arhivskih storitvam potrebno dodati še storitve za zagotavljanje varnosti. Funkcionalne zahteve se nanašajo na:

- sprejem elektronskih objektov v arhiv;
- obnovo arhiviranih objektov;
- brisanje arhiviranih objektov;
- določitev periodičnih aktivnosti za sprejete objekte;
- določitev opisnih podatkov za objekte;
- določitev politike upravljanja itd.

Arhiv lahko zagotovi varno hrambo gradiva le v primeru, če le-to vsebuje veljavne varnostne elemente že ob sprejemu. Zaradi tega so še pred sprejemom gradiva v arhiv potrebna nekatera preverjanja.

a) Preverjanje formata dokumenta

TAS lahko v arhiv sprejme le dokumente v predpisanih formatih, za katere lahko zagotovi varen sistem varovanja in izposoje. Vsi formati niso primerni za varno arhiviranje vsebine. Formati digitalno podpisanih dokumentov morajo izpolnjevati predvsem minimalne zahteve oz. najmanj zahtevo WYSIWYS (angl. What You Sign Is What You See) – "kar

podpišeš je to kar vidiš". Za arhiviranje so torej primerni le tisti formati, ki ne dopuščajo spreminjanja vsebine. To so npr. slikovni formati (angl. Imege Bitmap Format) in oblike za tiskanje (angl. Printable Dokument Formats); neprimerni so formati urejevalnikov (angl. Editable Document Formats).

Obetajoči so formati prilagojeni za meta podatke (angl. Meta Document Formats). Pri kriptiranih dokumentih sme biti kriptirana le primarna vsebina, medtem ko digitalni podpis in druge informacije, ki so potrebne za razna preverjanja, ne smejo biti kriptirane. Ker vsi formati dokumentov ne izpolnjujejo osnovne zahteve (WYSIWYS), bi moral vsak podpisani dokument vsebovati identifikator formata, podobno kot je to npr. končnica dokumenta v svetu aplikacij. Organizacija EESSI predlaga uporabo S/MIME tipa atributov, ki omogočajo avtomatsko prepoznavanje formata datoteke in njenih poddokumentov. Skupina EESSI priporoča, da se identifikator formata vključi tudi v oblike za digitalni podpis.

b) Preverjanje formata elektronskega podpisa

Podobno, kot velja za format dokumenta, je prisotna tudi potreba po preverjanju formata elektronskega podpisa. TAS lahko v arhiv sprejme le dokumente z digitalnimi podpisi, katerih formate podpira oz. zanje lahko zagotovi kasnejšo validacijo. Dolgoročna pravnomočnost digitalnih podpisov je izvedljiva le, če sistem lahko zbere vse podatke, potrebne za dokazovanje pravnomočnosti.

V okviru vzdrževanja arhiva mora TAS skrbeti za nenehno izvajanje nekaterih opravil, ki so potrebna za zagotavljanje verodostojnosti in varnega dostopanja do gradiva.

a) Sledenje napredku kriptografske tehnologije

TAS mora skrbeti za pravočasno časovno žigosanje gradiva s sodobnimi kriptografskimi algoritmi in uporabo primerne dolžine ključa. Trenutno najbolj alternativen pristop je sekvenčno skupinsko časovno žigosanje gradiva z močnejšimi algoritmi, še pred zlorabo zadnjega uporabljenega algoritma. Osnovna varnostna zahteva pri tem je, da novo uporabljeni algoritem zagotavlja najmanj doseženi nivo varnosti predhodnega algoritma. Skupinsko časovno žigosanje arhiviranega gradiva omogoča zagotavljanje dolgoročne varnosti digitalno podpisanih dokumentov, ne le pred zlorabo uporabljenega podpisnega algoritma, temveč tudi pred raznimi napadi virusov.

b) Zagotavljanje kompatibilnosti gradiva in tehnologije

TAS mora zagotavljati dostopnost vsebine in preverljivost digitalnega podpisa tudi v kasnejšem časovnem obdobju, ko originalna tehnologija ne bo več na voljo. Po potrebi mora skrbeti za ohranjanje niza aplikacij za prikazovanje dokumentov, skupaj z ustrezno

platformo (strojna oprema, operacijski sistem,…), ali vsaj ustreznega nadomestka (emulatorja) aplikacije in/ali okolja. Ves čas hrambe mora zagotavljati tudi ustrezne aplikacije za preverljivost digitalnega podpisa, četudi v tem času niso več povsem varne (npr. zaradi zloma algoritma) ali niso več dostopne na tržišču.

3.2.3.2 Koncept varnega arhiviranja

Različnost poslovnih procesov zahteva različne koncepte arhiviranja. Glede na funkcionalno vlogo varnostnih storitev ločimo dva koncepta arhiviranja:

- centralizirano arhiviranje;
- decentralizirano arhiviranje.

V modelu centraliziranega arhiviranja (angl. Centralized Archival Model) so varnostne storitve TAS centralni del arhiva. Njihove naloge so (EESSI, str. 39):

- preverjanje ustreznosti formata dokumenta in podpisa (posamezni TAS podpirajo le v naprej dogovorjene formate dokumentov oz. podpisov);
- zbiranje dodatnih informacij, potrebnih za kasnejšo validacijo podpisa;
- zanesljivo in varno arhiviranje podpisanih dokumentov;
- vzdrževanje statusa elektronskega podpisa skozi čas (večkratno časovno žigosanje).

Centraliziran arhiv skrbi za arhiviranje dokumenta in podpisa. Sistem lahko hkrati sprejme le en dokument in ga nato arhivira ločeno od drugih dokumentov. Dokumente lahko sprejema preko omrežja v realnem času (angl. on-line) in po končani transakciji uporabnikom vrne potrdilo o prejemu. Slabost modela je v tem, da z dokumentom upravlja arhiv: s tem postane negotova zaupnost vsebine dokumenta, v kolikor je le-ta potrebna. Takšen tip arhiva mora spoštovati zaupno naravo gradiva; postopanje mora biti določeno z zakonom ali pogodbo med stranko in arhivom. V nasprotnem primeru model ni primeren za hrambo podatkov zaupne narave, profesionalnih skrivnosti ali tajnih nalog. Za takšne vsebine je s tehničnega vidika primernejši model decentraliziranega (porazdeljenega) arhiviranja.

Model decentraliziranega arhiviranja (angl. Decentralized Archival Model) je sestavljen iz več komponent. Varnostne storitve TAS so ena izmed pomembnih komponent v sistemu arhiviranja. Le-ta skrbi za naslednja opravila:

- preverjanje formata podpisa (ali TAS podpira prispeli format);
- zbiranje kakršnihkoli dodatnih informacij potrebnih za kasnejšo validacijo podpisa;
- zanesljivo in varno arhiviranje podpisa;
- vzdrževanje statusa elektronskega podpisa skozi čas (večkratno časovno žigosanje).

Decentraliziran arhiv skrbi zgolj za arhiviranje elektronskega podpisa, medtem ko je dokument arhiviran ločeno od njega. Sistem lahko hkrati sprejme le en podpis in ga arhivira neodvisno od drugih podpisov. Dokument lahko ostane na uporabnikovi strani, zato njegova zasebnost ni ogrožena. Prednost modela je v neodvisnosti arhiviranja od formata dokumenta.

Rešitev je primerna predvsem za podjetja, ki imajo urejene lastne elektronske arhive, in nikakor ni primerna za dolgoročno arhiviranje gradiva. Ker sta dokument in digitalni podpis shranjena na fizično ločenih lokacijah, je kritična točka hrambe tudi identifikacija dokumenta. Za povezovanje dokumentov s pripadajočim podpisom, mora skrbeti poseben mehanizem.

3.2.4 Predstavitveni sloj

Nenehen razvoj na področju informacijske tehnologije povzroča probleme prikazovanja starejših elektronskih zapisov zaradi nekompatibilnosti s sodobno tehnologijo. Problem se potencira, kadar govorimo o hrambi dokumentov z dokazno vrednostjo. Nehote se porodi ideja, da je poleg arhiviranja vsebine potrebno hraniti še originalno strojno in programsko opremo, kar na dolgi rok ni praktično. Za hrambo strojne opreme bi potrebovali dodaten prostor, upravljanje opreme bi postajalo vse bolj nepregledno itd.

Zaenkrat še ne poznamo enostavne rešitve, ki bi zagotavljala trajen dostop do dokumentov. V svetu potekajo raziskave v več smereh. Trenutno najperspektivnejši tehniki sta:

- emulacija zastarele opreme na novejših platformah na nivoju strojne in programske opreme, ter operacijskih sistemov;
- migracija podatkov v sodobnejšo obliko.

V literaturi (Arhiv Republike Slovenije, str. 63) se omenja tudi nov teoretski pristop: povezovanje podatkov in programske opreme (BS 7978), ki je v fazi razvoja.

a) Emulacija

Emulacija je premeščanje starejšega elektronskega gradiva na opremo, ki posnema originalno tehnično okolje na drugi - novejši tehnologiji oz. platformi. Namenske naprave za posnemanje, t.i. emulatorji, omogočajo prikaz originalne vsebine iz preteklih časovnih obdobij s postopkom, ki spremeni le tehnološko okolje. Ker gradivo, vključno z digitalnim podpisom, ostaja nespremenjeno, se ohranja celovita funkcionalnost izvornega objekta.

Emulacija je ponovljiv postopek, zato omogoča sprotno posodabljanje emulatorjev. Rešitev je primerna tudi za dolgoročno hrambo digitalno podpisanih dokumentov. Slabost emulacije je potreba po arhiviranju emulatorjev: zaradi vse večje količine in potrebe po hrambi tovrstnih objektov nastaja problem kompleksnosti upravljanja z njimi.

b) Migracija podatkov v posodobljeno obliko

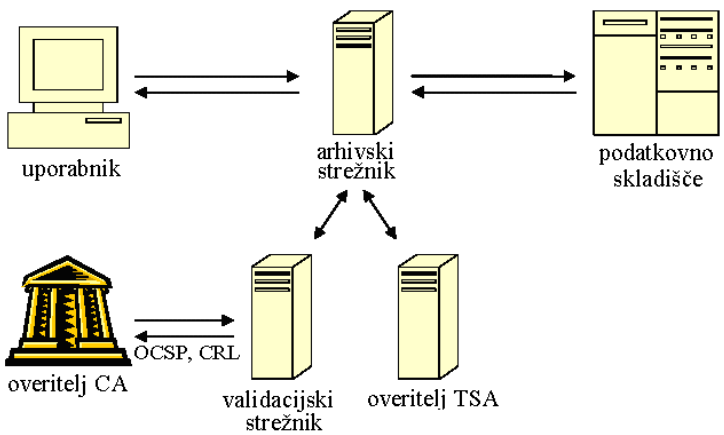
Migracija podatkov je transformacija digitalnih informacij iz zastarelih v nove formate, ki so kompatibilni s sodobnejšo opremo (tehnološko konfiguracijo oz. platformo). Strateški pristop predvideva migracijo številnih formatov v vsestranske standardizirane formate, ki bodo imeli daljšo življenjsko dobo. Migracija kljub temu ni zanesljiva rešitev. Obsežne migracije lahko vodijo do izgube ali spremembe posameznih bitov in s tem tudi do izgube nekaterih funkcionalnosti. Za primer lahko uporabimo digitalni podpis (poglavje 2.1.2), kjer je nespremenljivost na nivoju bita pomembna za dokazovanje verodostojnosti. Poleg tega lahko, zaradi nenehnega napredovanja tehnologije, proces vodi v nadaljnje migracije, zato je primeren le za krajše časovno obdobje.

Trenutno najbolj obetaven koncept reševanja problema berljivosti vsebine predstavlja t.i. migracija na zahtevo. Rešitev sledi ideji, da se potrebo po migraciji zniža na najmanjšo možno raven. Dokumente se hrani v standardiziranih formatih, ki omogočajo ločeno hrambo vsebine in opisnih podatkov. Hramba vsebine v originalni obliki omogoča varovanje celovitosti. Postopek migracije se za potrebe prikaza izvrši na zahtevo po objektu iz arhiva.

3.3 Javni elektronski arhivi

Hramba digitalno podpisanih objektov je kompleksno področje, ki ga posameznik težko obvladuje. Profesionalne institucije lahko zagotovijo bolj strokovno hrambo (opremo, strokovne delavce itd.) tovrstnega gradiva kot posameznik in s tem dosegajo tudi večjo javno vero v celovitost objektov. Glede na potrebo po nenehnem varovanju elektronskega gradiva, bo zaradi interesa nekaterih strokovnih skupin (pravnikov, arhivistov itd.), in širše javnosti, potrebno ustanoviti javne elektronske arhive, ki lahko delujejo kot samostojne ustanove ali kot oddelek v že obstoječih javnih arhivskih ustanovah.

Slika 20: Infrastruktura sistema za varno arhiviranje



Vir: http://www.gzs.si/e-poslovanje/dokumentacija/eSLOG-Elektronski_arhiv_0.99(v_pripravi).pdf

Osnova javnega elektronskega arhiva je varen arhiv, ki temelji na elementih varne infrastrukture javnih ključev (slika 20). Z uporabo varnostnih mehanizmov (za digitalno podpisovanje, za časovno žigosanje, za validacijske mehanizme itd.) in varnih protokolov zagotavlja varno interakcijo med uporabnikom in arhivom (npr. prevzem gradiva), ohranjanja celovitost objektov in vzdržuje veljavnost pripadajočih varnostnih atributov v času predpisane hrambe.

Varni elektronski arhivi morajo skrbeti za naslednje aktivnosti:

(1) nadzor nad dostopom:
- overjanje uporabnikov;
- klasifikacija uporabnikov;
- dodeljevanje pravic (branje, pisanje ipd.) za dostop za posamezne uporabnike;
- beleženje dostopa in aktivnosti posameznih uporabnikov;

(2) upravljanje dokumentarnega in arhivskega gradiva:
- pomoč komitentom pri odbiranju gradiva;
- sprejem gradiva;
- klasifikacija gradiva;
- obdelava gradiva;
- hramba gradiva;

(3) upravljanje s postopki:
- formalizacija postopkov;
- ohranjanje berljivosti gradiva;
- skrb za trajno veljavo dokaznih vrednosti;
- hramba varnostnih atributov;

(4) Zaščita gradiva
- zaščita dostopa do gradiva;
- zaščita komunikacije;
- zaščita vsebine pred spremembami;
- zaščita nosilcev vsebine pred poškodbami;
- zaščita pred izgubo podatkov.

Na javne elektronske arhive lahko gledamo iz različnih zornih kotov. Poleg varnostno-tehničnih izhodišč, ki so bila obravnavana v prejšnjih poglavjih, so osnovna izhodišča za uspešno delovanje takšne ustanove (Novak, str. IV-7):

- neodvisnost infrastrukture, kar pomeni da specifična strojna in programska oprema nima neposrednega vpliva na dolgoročno stabilnost;
- modularnost, kar pomeni da sistem sestoji iz komponent, ki jih lahko zamenjamo z minimalnimi vplivi na ostale komponente sistema;

- povezljivost, kar predstavlja zmožnost, da dinamično obravnava potrebe po širitvi kapacitet ter njihovo celovito upravljanje v sorazmerju z naraščajočo količino elektronske dokumentacije;
- razširljivost, to je sposobnost, da bo uporabljeni sistem obvladoval še druge, morda danes neznane pojavne oblike elektronske dokumentacije.

Z vidika izvršilne odgovornosti mora javni elektronski arhiv delovati v skladu s splošno in/ali mednarodno sprejetimi standardi in veljavno zakonodajo. Poskrbeti mora za ustrezno fizično okolje (npr. temperaturo in vlago skladišča, prezračevanje, požarno varnost, varnostne kopije ipd.), ter opravljati redne meritve. Uporabljeni postopki in rezultati morajo biti dokumentirani.

Varen elektronski arhiv prevzema tudi proceduralno odgovornost, torej mora opravljati nadzor nad dostopom do podatkov, mehanizmi in celotnim sistemom. Za obveščanje o problemih mora biti poskrbljeno na sistemskem nivoju. Sistem mora vsebovati ustrezne redundance opreme, izdelan mora biti tudi plan ravnanja v primerih izgube ali uničenja podatkov in vzpostavitvi prejšnjega stanja (angl. Desaster Recovery Plan).

Javni elektronski arhiv lahko uspešno izpolnjuje svoje poslanstvo le, če je ustrezno organiziran. Delovati mora v skladu s politiko delovanja, ki natančneje opisuje potek sprejema, hrambe in izdaje gradiva. Odnose med ustanovo elektronskega arhiva in komitenti morajo urejati pogodbe, v katerih so natančno določeni pogoji sodelovanja (npr. formati gradiva, način upravljanja, dostop ipd).

Varen e-arhiv je lahko le finančno stabilna ustanova, saj le takšna lahko zagotovi dolgoročno hrambo arhivskega gradiva. Finančno stanje se mora redno preverjati, zagotovljene morajo biti tudi ustrezne finančne rezerve.

3.4 Zaključek poglavja 3

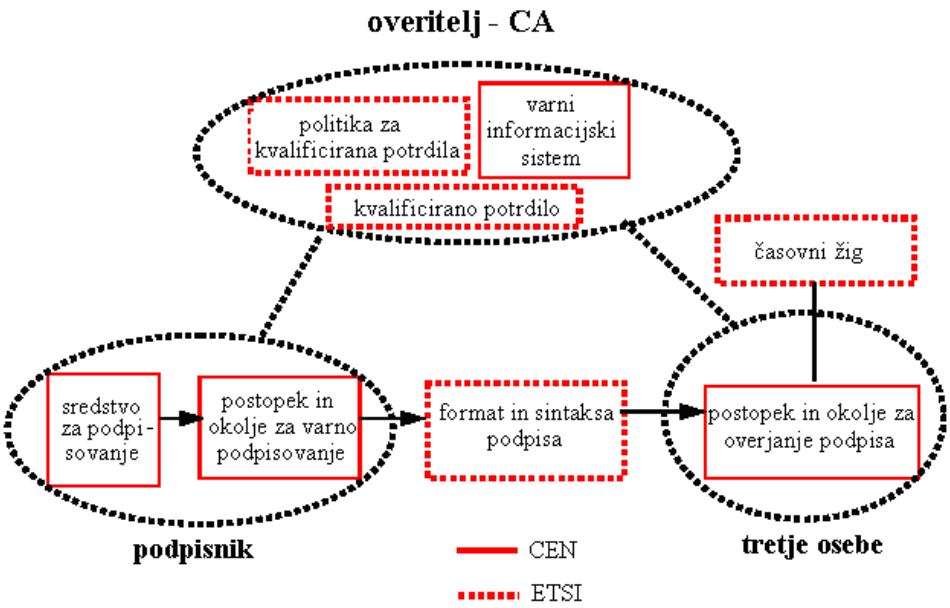
Medtem, ko so osnovni varnostni mehanizmi že dobro uveljavljeni v praksi, je področje elektronskega arhiviranja še v povojih. V praksi se že uporablja elektronska hramba za krajša časovna obdobja (nekaj let). V tem poglavju opisani problemi se nanašajo predvsem na daljša časovna obdobja.

Na podlagi problemov dolgoročnega elektronskega arhiviranja so nastali tu predstavljeni teoretični pristopi k njihovem reševanju, ki podajajo smernice razvoja. Za njihovo implementacijo v praksi so potrebni tehnični standardi in priporočila, ki so podani v naslednjem poglavju.

4 TEHNIČNI STANDARDI IN PRIPOROČILA ZA DELOVANJE VARNIH ELEKTRONSKIH ARHIVOV

Za splošno uporabo tehničnih produktov so potrebni tehnični standardi. Za določitev splošnih okvirjev in enotnih tehničnih standardov na področju varnega elektronskega poslovanja in elektronskega podpisa v Evropi je ICTSB (angl. Information and Communication Technologies Standards Board), ki skrbi za koordinacijo delovanja evropskih organizacij za standardizacijo, leta 1999 ustanovila organizacijo EESSI (angl. The European Electronic Signature Standardizatio Iniciative). Ta je leta 2003 izpolnila svoje poslanstvo in objavila priporočila za zahtevane standarde v skladu z Direktivo 1999/93/EC in pripadajočimi aneksi, zato jo je krovna organizacija ICTSB leta 2004 razpustila. Še vedno potekajo nekatere aktivnosti v smeri implementacije direktive v tehnične standarde. To delo sta si razdelili predvsem Evropski komite za standardizacijo CEN/ISSS in Evropski inštitut za telekomunikacijske standarde ETSI TC SEC/ESI.

Slika 21: Razdelitev področij standardizacije med ETSI in CEN



Vir: http://www.gzs.si/e-poslovanje/dokumentacija/e-SLOG_Zahteve_za_CA_1.1.pdf

CEN (fr. Comite European de Normalisation) je organizacija, katere poslanstvo je priprava standardov na področju informatike. Njene delavnice se odvijajo preko t.i. sistema standardizacije informacijske družbe ISSS (angl. Information Society Standardization System). V njeni pristojnosti je priprava priporočil za naslednja področja:

- varen informacijski sistem;
- varno podpisovanje (sredstva, postopek in okolje);
- overjanje podpisa (postopek in okolje).

Tabela 4: Standardi organizacije CEN

CWA 14167	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
Part 1	System Security Requirements
Part 2	Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
Part 3	Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
Part 4	Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
CWA 14169	Secure Signature-creation devices "EAL 4+"
CWA 14170	Security requirements for signature creation applications
CWA 14171	General guidelines for electronic signature verification
CWA 14172	EESSI Conformity Assessment Guidance
Part 1	General introduction
Part 2	Certification Authority services and processes
Part 3	Trustworthy systems managing certificates for electronic signatures
Part 4	Signature-creation applications and general guidelines for electronic signature verification
Part 5	Secure signature-creation devices
Part 6	Signature-creation device supporting signatures other than qualified
Part 7	Cryptographic modules used by Certification Service Providers for signing operations and key generation services
Part 8	Time-stamping Authority services and processes
CWA 14355	Guidelines for the implementation of Secure Signature-Creation Devices
CWA 14365	Guide on the Use of Electronic Signatures
Part 1	Legal and Technical Aspects
Part 2	Protection Profile for Software Signature Creation Devices
CWA 14890	Application Interface for smart cards used as Secure Signature Creation Devices
Part 1	Basic requirements
Part 2	Additional Services

Vir: http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp

Slovenija je članica CEN-a s svojim inštitutom za standardizacijo SIST[23].

ETSI (angl. European Telecomunications Standards Institute) je neprofitna organizacija, ki se ukvarja z razvojem standardov in tehnične dokumentacije na področju telekomunikacijske in informacijske tehnologije v Evropi. V okviru varnega elektronskega poslovanja je zadolžena za naslednja področja:

- kvalificirana potrdila, vključno s politiko;
- format in sintaksa podpisa;
- področje časovnega žiga.

[23] SIST – Slovenski inštitut za standardizacijo (1991) – naslednik USM (Urada RS za standardizacijo in meroslovje

Tabela 5: Standardi organizacije ETSI

TS 101 456 v1.3.1	Policy requirements for certification authorities issuing qualified certificates
TS 102 042 v1.2.1	Policy requirements for certification authorities issuing public key certificates
TR 102 040 v1.3.1	International Harmonization of Policy Requirements for CAs issuing Certificates
TR 102 047 v1.2.1	International Harmonization of Electronic Signature Formats
TR 102 317 v1.1.1	Process and tool for maintenance of ETSI deliverables
TS 101 903 v1.2.2	XML Advanced Electronic Signatures (XAdES)
TS 101 903 v1.2.1	XML Advanced Electronic Signatures (XAdES) (withdrawn)
TS 101 862 v1.3.1	Qualified Certificate Profile
TS 102 280	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
TR 102 040 v1.2.1	International Harmonization of Policy Requirements for CAs issuing Certificates
TR 102 047	International Harmonization of Electronic Signature Formats
TS 101 733 v1.5.1	Electronic Signature Formats
TR 102 272	ASN.1 format for signature policies
TS 102 231	Harmonized TSP status information
TS 102 158	Policy requirements for CSPs issuing attribute certificates
TR 102 045	Signature policy for extended business model
SR 002 176	Algorithms and Parameters for Secure Electronic Signatures
TR 102 153	Pre study on Certificate Profiles
TR 102 046	Maintenance of ETSI standards from EESSI phase 2 and 3
TS 102 023 v1.2.1	Policy requirements for time-stamping authorities
TR 102 044	Identification of requirements for attribute certification
TS 101 733 v1.4.0	Electronic Signature formats version
TR 102 038	XML format for signature policies
TS 102 023	Policy requirements for time-stamping authorities
TS 102 042	Policy requirements for certification authorities issuing public key certificates
TS 101 456 v1.2.1	Policy requirements for certification authorities issuing qualified certificates
TR 102 030	Provision of harmonized Trust Service Provider status information
TR 102 040	International Harmonization of Policy Requirements for CAs issuing Certificates
TS 101 861 v1.2.1	Time stamping profile
TR 102 041	Signature Policies Report
TS 101 903	XML Advanced Electronic Signatures (XAdES)
TS 101 733 v1.3.1	Electronic Signature Formats

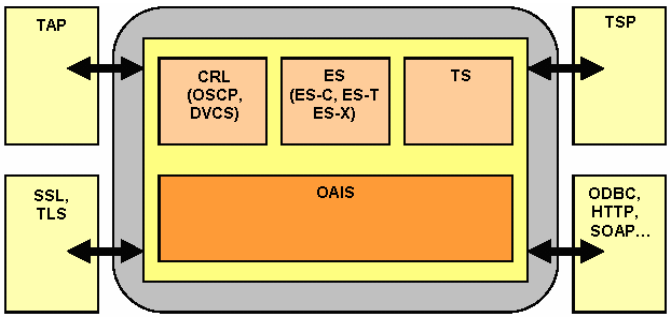
Vir: http://portal.etsi.org/esi/el-sign.asp

Poleg organizacij ETSI in CEN, ki oblikujeta predvsem standarde, osredotočene na postopke in obliko elektronskega podpisa, je potrebno navesti mednarodno organizacijo IETF (angl. Internet Engineering Task Force), ki nadzira in pripravlja tehnične standarde na katerih temelji Internet. Organizacija IETF nima formalnega članstva; udeležba na njenih strokovnih srečanjih je odprta za vse zainteresirane (eksperte, inovatorje,

uporabnike ipd.). Delovne skupine, ki nastanejo v procesu nastajanja posameznega standarda, po opravljeni nalogi usahnejo. Organizacija deluje pod okriljem združenja ISOC (angl. Internet Society), ki odobri oblikovane standarde.

Kljub velikemu številu že sprejetih standardov še vedno primanjkuje standardov, ki bi celovito reševali problematiko elektronskega arhiviranja. Tehnološka priporočila predstavljajo kombinacijo rešitev, ki je sestavljena iz rešitev problemov na posameznih nivojih.

Slika 22: Gradniki varnega elektronskega arhiva



Vir: http://www.gzs.si/e-poslovanje/dokumentacija/eSLOG-Elektronski_arhiv_0.99(v_pripravi).pdf

V nadaljevanju magistrskega dela sledi opis nekaterih standardov, ki so pomembni za varno dolgoročno hrambo elektronskih dokumentov in niso bili opisani v prejšnjih poglavjih.

4.1 Ohranjanje vsebine in atributov

Standardi za ohranjanje vsebine in atributov so namenjeni podaljševanju življenjske dobe elektronskih zapisov. Ker se stroka zaradi ohranjanja celovitosti zapisov zavzema za hrambo v originalni obliki, se je kot "de facto" standard za interpretacijo podatkov uveljavil razširljivi označevalni jezik XML (angl. Extensible Markup Language). V celotnem času predpisane hrambe je potrebno ohranjati tudi morebitne dokazne vrednosti dokumentov. S tega vidika so še posebej pomembni periodični arhivski časovni žigi. Za zagotavljanje vseh potrebnih podatkov za validacijo dokumentov v vsakem trenutku dolgotrajnega arhiviranje je pomembna specifikacija ERS, ki formalizira generiranje, preverjanje in obliko zapisa arhivskih časovnih žigov.

4.1.1 XML

XML je enostaven in izredno fleksibilen jezik za opisovanje t.i. drevesne strukture informacij. Sprva je bil načrtovan za prenos strukturirane vsebine preko spleta, zaradi praktičnosti in drugih prednosti je postal alternativa tudi na področju dolgoročne hrambe elektronskega gradiva. Prvo priporočilo XML 1.0 je objavila skupina XML Working

Group iz konzorcija svetovnega spleta W3C v začetku leta 1998; nato so izdali še novejša priporočila za izdelavo in procesiranje XML-a za različne potrebe.

XML omogoča sistemsko neodvisno interpretacijo podatkov. Podatke ovija v posebne oznake (tag), ki interpretirajo njihov pomen. Oznake niso preddefinirane, zato jih lahko določi uporabnik sam. Določen je le formalen nabor pravil ali t.i. dokumentacijska shema DTD (angl. Document Type Declaration), ki opredeljuje strukturo zapisa, seznam elementov (primarnih gradnikov), atributov, zaznamkov in entitet, vključno z medsebojnimi relacijami. Shema DTD je lahko vgnezdena v dokument ali se nahaja v ločeni datoteki in je v dokument vključena preko reference.

Dokument je sestavljen iz uvoda in korenskega elementa. Prvi vsebuje identifikacijo, da gre za XML dokument (podana je tudi verzija), podatek, ali je dokument samostojen ali ne, ter način kodiranja. Pri nas se uporablja kodiranje po standardu ISO-8859-2, ki je del UTF-8 kodiranja. Korenski element vsebuje celotno vsebino dokumenta. Strukturo vsebine opisujejo primarni gradniki – elementi. Vsak element zaključujeta začetna in končna oznaka. Vmes se nahaja vsebina, ki je lahko besedilo, ali drugi elementi, sklici znakov ipd.

Primer XML dokumenta:

```
<!-- Ta datoteka vsebuje podatke o delavcih. -->          komentar
<?xml version="1.0"encoding="UTF-8"?>                      uvod
<delavci>                                                  korenski element
  <delavec>
    <ime>
      Janez
    </ime>
    <priimek>
      Novak
    </priimek>
  </delavec>
</delavci>
```

Vsebino elementa lahko opisujejo atributi, ki sestojijo iz imena in vrednosti. Dokument lahko vsebuje tudi komentarje, ki služijo za smiselno dokumentiranje; XML razčlenjevalniki jih prezrejo.
XML učinkovito rešuje tudi interpretacijo varnostnih atributov, zahtevanih za zagotovitev varnostnih mehanizmov. V okviru S-XML (angl. Secure XML) so nastali standardi, kot so XML-DSig za digitalno podpisovanje vsebin, XMLenc za šifriranje XML dokumentov ipd.

Sintaksa **XML-DSig** je priporočilo konzorcija W3C, ki opisuje XML sintakso za digitalni podpis. Zagotavlja avtentikacijo podpisnika ter integriteto podatkov. Kompatibilna je z različnimi internet standardi, kot so protokol SOAP[24](angl. Simple Object Access

[24] SOAP (Simple Object Access Protocol) – protokol za izmenjavo XML sporočil.

Protocol), jezikom SAML[25] (angl. Security Assertion Markup Language) idr.

XML-DSig lahko uporabljamo za podpisovanje podatkov v različnih formatih. Omogoča podpisovanje celotnega dokumenta ali dela dokumenta. V istem dokumentu je lahko tudi več podpisov. To funkcionalnost omogoča strukturiran način označevanja ključnih informacij za pravilno interpretacijo in preverjanje digitalnega podpisa. Prednost ni zgolj v enostavni interpretaciji podatkov, temveč v možnosti hitre in učinkovite obdelave.

Primer XML podpisa (http://www.microsoft.si/slovenija/7ntk/Predstavitve/293.ppt):

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
            <CanonicalizationMethod Algorithm="http://.../REC-xml-c14n-20010315"/>
            <SignatureMethod Algorithm="http://.../xmldsig#rsa-sha1"/>
            <Reference "URI=#SignedObject">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestMethodValue>FPj0eCIUghpBovQbeiZksK3pqwI=</DigestValue>
            </Reference>
    </SignedInfo>
  <SignatureValue>Vazs6K...eVooST2bucTghs=</SignatureValue>
    <KeyInfo>
            <KeyValue xmlns="http://www.w3.org/2000/09/xmldsig#">
            <RSAKeyValue>
                    <Modulus>ykzdntW...IfcpS9xv0=</Modulus>
                    <Exponent>AQAB=</Exponent>
            </RSAKeyValue>
            </KeyValue>
    <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
            <X509Certificate>MIIFIzCCAwug...01y7Q+cvWD4yvkM/6eY=</X509Certificate>
    </X509Data>
    </KeyInfo>
    <Object Id="SignedObject">
    <Package Id="p1" xmlns="">
            ...
    </Package>
  </Object>
</Signature>
```

Korenski element XML podpisa je <Signature> (podpis), ki označuje začetek in konec podpisa. Ta ima podrejene elemente, ki podpis opisujejo, in tudi ti lahko vsebujejo svoje podrejene elemente itd.

Element <SignedInfo> nosi ključne informacije o podpisu in je zaradi velikega števila sebi podrejenih elementov najkompleksnejši podrejeni element korena. Sledi vrednosti oz. rezultate uporabljenih metod (<SignatureValue> - vrednost podpisa) in vsebuje:

[25] SAML (Security Assertion Markup Language) – označevalni jezik z izjavo o varnosti.

- kazalce na vire uporabljenih metod, (npr.: <CanonicalizationMethod> - normalizacijska metoda, <SignatureMethod> - šifrirni algoritem);
- ter kazalce (sklici) na poljubne datoteke, spletna sredstva ali na del dokumenta, kjer so podatki o podpisu (npr. <DigestMethod> - zgoščevalna funkcija, <DigestValue> - zgoščena vrednost oz. prstni odtis).

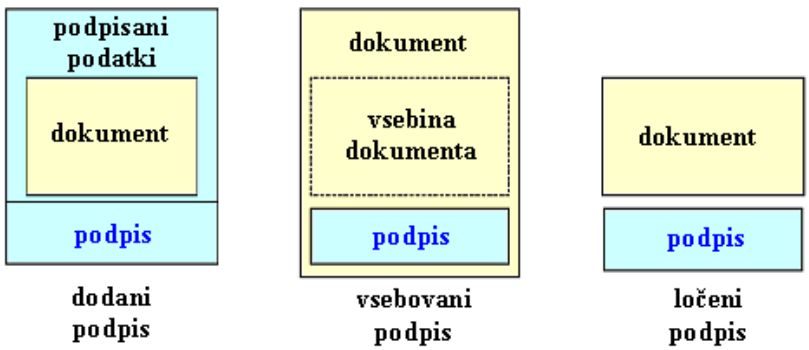
Element <KeyInfo> vsebuje specifične informacije o ključu, ki lahko prejemniku XML podpisa olajšajo njegovo preverjanje. Te informacije so lahko neposredne (javni ključ ali digitalno potrdilo) ali posredne (kazalec na vir informacij). Zaradi nedvoumnosti pri preverjanju veljavnosti podpisa, se morajo vsi podrejeni elementi (<KeyName>, <KeyValue> itd.) nanašati na isti ključ.

Na tem mestu naj omenim, da kljub velikemu naboru podelementov namenjenih digitalnemu potrdilu X.509, je XML podpis popolnoma odprt tudi za druge, še ne razvite, standarde. Vse druge informacije za pravilno interpretacijo podpisa se nahajajo v elementu <Object>. Mednje sodijo informacije o časovnem žigu, vrsti podpisanih podatkov ipd.

Za pisanje posameznih aplikacij lahko, glede na vrsto povezave med dokumentom in podpisom, v okviru XMLdsig standarda izbiramo med tremi temeljnimi oblikami podpisa:

- dodani podpis (angl. Enveloped signature) – podpis je dodan k dokumentu;
- vsebovani podpis (angl. Enveloping signature)– podpis je del podpisanega dokumenta;
- ločeni podpis (angl. Deteched signature) – dokument ni del elementa <Signature>.

Slika 23:Temeljne oblike XMLdsig podpisa



Vir: http://www.setcce.org/natows/slides/E_doc.pdf

4.2 Oblike varnega elektronskega podpisa

Digitalno podpisan dokument lahko skozi svoj življenjski cikel ohranja zadosten nivo varnosti le tako, da se stalno dograjuje. Po priporočilu EESSI lahko, glede na dodane varnostne elemente, opišemo različne oblike elektronskega podpisa:

- pravnomočna oblika elektronskega podpisa;
- oblika varenega elektronskega podpisa po poteku digitalnega potrdila;
- oblika trajno veljavnega elektronskega podpisa.

Osnovna oblika elektronskega podpisa ES (angl. Electronic signature) brez dodatnih varnostnih elementov zagotavlja le minimalen nivo varnosti. Sestoji iz:

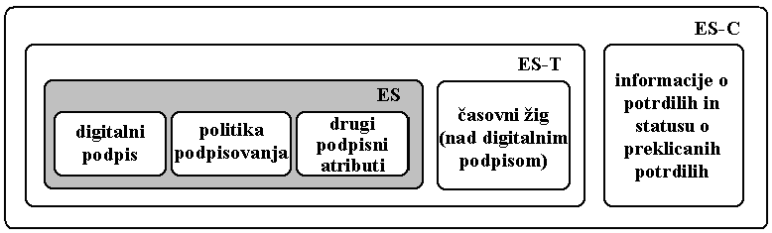
- digitalnega podpisa;
- reference na politiko podpisa (tehnične zahteve,…);
- drugih podpisnih atributov (informacije o podpisniku, lokaciji, datumu in uri podpisa, formatu podpisnih podatkov ipd.).

4.2.1 Oblike podpisa za potrebe kratkoročnega in dolgoročnega arhiviranja

Osnovna oblika digitalnih podpisov za različno dolga arhivna časovna obdobja vključuje digitalni podpis in druge osnovne informacije, ki nastanejo v procesu podpisovanja na strani aplikacije. Vendar takšen podpis omogoča zgolj identifikacijo podpisnika ter zaščito celovitosti. Ker podpis ne vsebuje dokaza o času nastanka, lahko podpisnik tak podpis kasneje zanika. Nedvomen dokaz o obstoju digitalnega podpisa v času veljavnega digitalnega potrdila doda šele časovni žig skupaj s CRL oz. OCSP odzivom, ki mora biti čim bliže času podpisa. Pravnomočna oblika elektronskega podpisa, ki je med drugim predpogoj tudi za varno arhiviranje objekta, mora poleg osnovne oblike vsebovati:

- časovni žig, ki potrjuje obstoj dokumenta ob določenem času;
- reference na podatke o digitalnih potrdilih in statusih preklicanih potrdil.

Slika 24: Pravnomočna oblika elektronskega podpisa



Vir: EESSI, str. 20

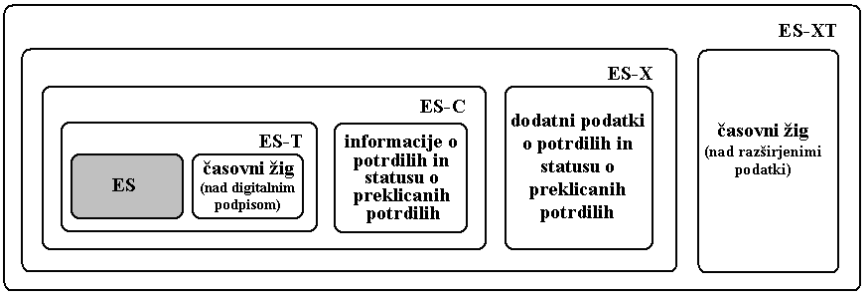
Podpisani dokumenti, ki jih želimo hraniti dlje časa, potrebujejo dodatno zaščito, ki bo omogočala verifikacijo podpisa tudi po časovnem poteku veljavnosti digitalnega potrdila, v primeru predčasnega preklica potrdila in/ali v okoliščinah zmanjšane varnosti podpisa zaradi napredka tehnologije.

Pravnomočni obliki digitalnega podpisa je potrebno dodati:

- vrednosti digitalnih potrdil, vključno s potjo oz. potrdili izdajateljev in njihovimi statusi;

- dobljen niz podatkov je potrebno ponovno zaščititi s časovnim žigom.

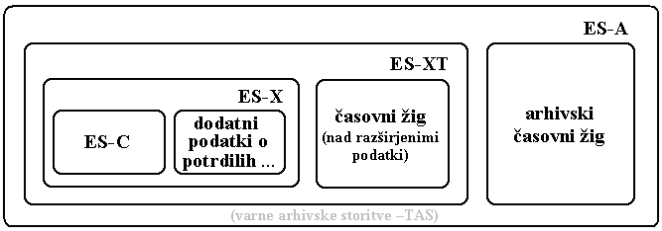
Slika 25: Oblike elektronskega podpisa po poteku certifikatov



Vir: EESSI, str.22

Varnost podpisa je tem večja, čim bližje sta si čas kreiranja podpisa in čas žigosanja. Za trajno veljavnost digitalnega podpisa je potrebno sekvenčno dodajati časovne žige, kreirane z močnejšimi algoritmi še preden je varnost zadnjega časovnega žiga ogrožena. Oblika trajno veljavnega elektronskega podpisa vsebuje dodani arhivski časovni žig ES-A.

Slika 26: Oblika arhiviranega elektronskega podpisa

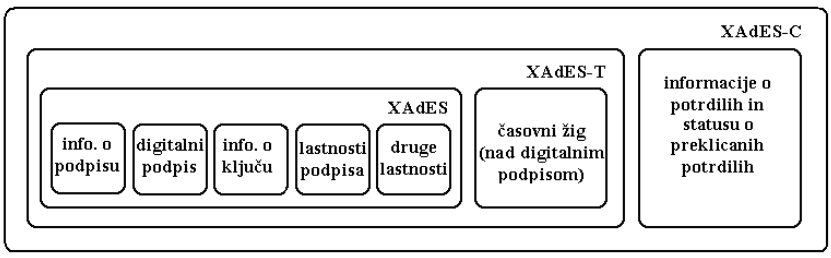


Vir: EESSI, str. 22

4.2.2 Varna oblika XML podpisa

Ekvivalentno lahko opišemo vse oblike digitalnega podpisa tudi za XML format podpisa. Na spodnji sliki je prikazana oblika XML podpisa z vsemi podatki za overjanje.

Slika 27: Trajna oblika XML podpisa



Vir : e-slog – priporočila za format dokumenta, str. 9

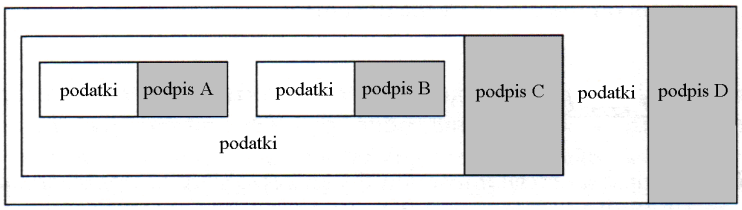
4.2.3 Večfazni elektronski podpis

Opisane oblike digitalnih podpisov ne zadoščajo za vse primere, ki jih srečujemo v praksi, zato je potrebno definirati dodatne oblike digitalnega podpisa, ki bodo omogočala izpolnitev dodatnih zahtev za trajno hrambo dokumentov. V nadaljevanju sta predstavljena dva načina večfaznega podpisovanja; možna je tudi kombinacija obeh.

a) Zaporedno podpisovanje

Zaporedno podpisovanje dokumenta poteka tako, da različni podpisniki podpišejo različne dele dokumenta. Podpisi nastajajo postopoma. Za celoten dokument je odgovorna ena oseba, ki preveri in potrdi veljavnost vseh delnih podpisov, nato doda svoj podpis pod celotnim dokumentom. Enak način podpisovanja se lahko uporabi v okviru dokumenta tudi na nižjih nivojih.

Slika 28: Oblika elektronskega podpisa za zaporedno podpisovanje dokumentov



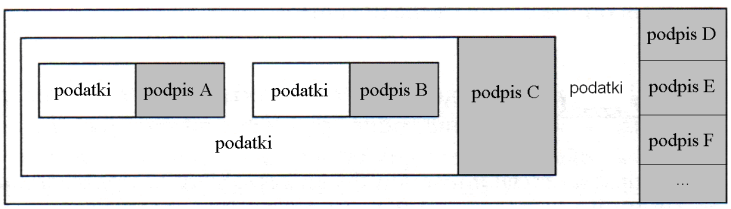
Vir: EESSI, str. 25

Za osnovo privzamemo obliko digitalnega podpisa za arhiviranje (poglavje 4.2.3) in jo nadgradimo v večkratni podpis. Posamezne podpise pod dokumenti oz. deli dokumentov hierarhično sestavimo. Ker se podpisi vršijo nad različnimi podatki, je v vsakem parcialnem podpisu vsebovana drugačna zgoščena vrednost. Prednost takšne oblike podpisa je v tem, da za večfazno podpisovanje ne zahteva novega podpisnega formata.

b) Vzporedno podpisovanje

Vzporedno podpisovanje dokumenta poteka tako, da različni podpisniki podpišejo isti dokument lahko ob različnih časih.

Slika 29: Oblika elektronskega podpisa za vzporedno podpisovanje dokumentov



Vir: EESSI, str. 25

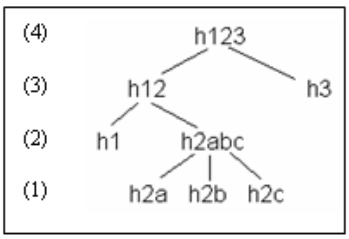
Za osnovo ponovno privzamemo obliko digitalnega podpisa za arhiviranje (poglavje 4.2.3) in jo nadgradimo tako, da omogoča več podpisov pod istim dokumentom hkrati. V tem primeru je v vseh podpisih vsebovana ista zgoščena vrednost. Ta forma je kompleksnejša, zato zahteva novo standardizacijo formata. Problem, ki lahko nastane pri takšni obliki je ta, da nihče izmed podpisnikov ne potrdi ostalih podpisov.

4.2.4 Specifikacija ERS

Specifikacija ERS (angl. Evidence Record Syntax), ki jo najdemo med dokumenti organizacije IETF, opisuje generiranje, preverjanje in obliko dokaznega zapisa o obstoju arhivskega dokumenta ali skupine dokumentov ob določenem času. Zapis vsebuje informacije o arhivskih časovnih žigih, njihovem vrstnem redu in podatke za verifikacijo arhivskih dokumentov.

Osnova ERS zapisa je arhivski časovni žig. Ta nastane v procesu, kjer najprej zberemo podatke in z zgoščevalno funkcijo izračunamo zgoščeno vrednost (poglavje 2.1.2.1). V kolikor operiramo z več skupinami podatkov (več zgoščenimi vrednostmi), lahko te združimo in izračunamo novo zgoščeno vrednost. Ta korak ponavljamo, dokler ne dobimo samo ene zgoščene vrednosti, na vrhu drevesne strukture zgoščenih vrednosti. To vrednost časovno žigosamo.

Primer nastanka drevesne struktura za tri podatkovne skupine, v katerih je razvrščenih pet dokumentov (http://ltans.edelweb.fr/draft-ietf-ltans-ers-03.txt):



Zaradi upadanja varnosti uporabljene tehnologije je potrebno arhivski časovni žig periodično obnavljati z novejšimi, varnejšimi algoritmi. Glede na okoliščine je lahko obnova arhivskega časovnega žiga enostavna ali kompleksna. V prvem primeru se obnovi le predhodni arhivski časovni žig, pri tem je arhivsko gradivo vpleteno v proces zgolj posredno. Takšen način zadošča kadar se varnost tehnologije predhodnega časovnega žiga zniža do kritične meje ali kadar pripadajoče digitalno potrdilo ni več veljavno. V primeru, da predhodno uporabljena tehnologija ni več varna, je potrebno obnoviti celotno strukturo zgoščenih vrednosti in dobljeno vrhnjo zgoščeno vrednost časovno žigosati skupaj s predhodnim arhivskim časovnim žigom.

ERS zapis vsebuje informacije o vseh arhivskih časovnih žigih, njihovem zaporedju in podatke za verifikacijo. Tovrstni podatki morajo vedno obstojati za posamezne arhivirane objekte ne glede na podatke v grupi in ne glede na to, da sta posamezen podatek ali skupina podatkov odstranjena iz arhiva (Jerman Blažič, 2005, str. II-9).

Primer ERS zapisa (http://ltans.edelweb.fr/draft-ietf-ltans-ers-03.txt):

```
EvidenceRecord ::= SEQUENCE {
    version                    INTEGER { v1(1) },
    digestAlgorithms           SEQUENCE OF AlgorithmIdentifier,

    cryptoInfos                [0] CryptoInfos OPTIONAL,
    encryption                 [1] EncryptionMethod OPTIONAL,
    archiveTimeStampSequence          ArchiveTimeStampSequence}
  CryptoInfos ::= SEQUENCE SIZE (1..MAX) OF CryptoInfo

  CryptoInfo ::= SEQUENCE
  {
    cryptoInfoType    OBJECT IDENTIFIER
    cryptoInfoValue   ANY DEFINED BY cryptoInfoType
  }
```

4.2.5 Protokol za interakcijo med uporabnikom in arhivom LTAP

Protokol za arhiviranje objektov LTAP (angl. Long Term Archive Protocol), ki ga je razvila organizacija IETF, formalizira interakcijo med arhivom in zunanjimi uporabniki. Protokol se osredotoča na strukturo zahtevkov in odgovore nanje. Za avtorizacijo udeležencev komunikacije in varen prenos podatkov izkorišča druge protokole.

Protokol LTAP opisuje komunikacijo med uporabnikom in arhivskim strežnikom v zvezi z naslednjimi operacijami:

- arhiviranje podatkov (Archive);
- preverjanje statusa podatkov (Status);
- izvoz podatkov iz arhiva (Export);
- brisanje podatkov (Delete);
- preverjanje veljavnosti podatkov (Verify).

Vsaka operacija temelji na tridelni (asinhroni) transakciji, enemu zahtevku in dveh različnih tipih odgovorov. Uporabnik pošlje arhivu zahtevek za operacijo (npr. za arhiviranje podatkov). Arhiv najprej vrne le odgovor o sprejetju zahteve, končni rezultat operacije vrne kasneje, ko je le-ta na voljo (lahko tudi več ur kasneje). Da bi se izognili implementaciji zahtevnejšega odjemalca, ki sprejema asinhrone odgovore, je možno rezultat operacije naknadno preverjati z zahtevkom o statusu izvedbe zahtevane operacije (Jerman Blažič, 2005, str. 10-II).

4.3 Zaključek poglavja 4

Dosedanja poglavja v glavnem opisujejo varovanje elektronskih dokumentov s tehničnega vidika. Tehnične specifikacije ne zadostujejo za zagotovitev varnega elektronskega arhiviranja. Zadovoljivo varnost lahko dosežemo le s prepletanjem tehnološkega in pravnega vidika, zato je za implementacijo storitev potrebna ustrezna zakonska ureditev.

5 ZAKONSKA UREDITEV ELEKTRONSKEGA POSLOVANJA

Dokumentu daje legitimno vrednost zakonodaja, zato je skladnost tehnologije z veljavnimi zakoni in akti ključnega pomena. Z razvojem informacijske tehnologije se je spremenila v glavnem le oblika komuniciranja, zato tudi v elektronskem svetu še vedno velja večina že uveljavljenih pravnih pravil. Kljub temu je bilo potrebno odpraviti nekaj ovir, ki jih elektronskemu poslovanju postavljajo pravne norme, sprejete v času papirnega poslovanja (npr. pisna oblika, izvirnik ipd.). Nekaj pravnih vprašanj, predvsem tistih, ki se nanašajo na elektronski podpis in arhiviranje elektronskih objektov, je bilo (ali še vedno je) potrebno urediti povsem na novo.

Način elektronskega komuniciranja zmanjšuje pomembnost državnih meja, zato elektronsko poslovanje zahteva zakonodajo, ki je usklajena na mednarodnem nivoju. Za ustrezno zakonodajo v državah EU skrbi evropski pravni red, ki zajema direktive in pripadajoče anekse. Določbe, sprejete na nivoju EU, države članice implementirajo v nacionalno zakonodajo. Praviloma se v zakone in akte na nacionalni ravni implementira direktive EU, medtem ko uredbe povzemajo anekse direktiv. Za poslovanje so pomembne tudi druge listine, kot so politika delovanja ali varnostna politika, interne listine in dogovori, ter bilateralni sporazumi in medsebojne pogodbe.

Tabela 6: Listine, ki dajo dokumentu legitimno vrednost

Evropski pravni red	Nacionalna zakonodaja	stopnja
Direktive	Zakoni in akti	1
Aneksi	Uredbe	2
	Politika delovanja	3
	Interne listine in dogovori	4
	Bilateralni sporazumi in medsebojne pogodbe	5

5.1 Tuji pravni viri

Med prvimi, ki so se lotili zakonskega urejanja elektronskega poslovanja, je bila Organizacija združenih narodov. Njihova Komisija za mednarodno in trgovinsko pravo (angl. United Nations Commission on International Trade Low), v nadaljevanju UNCITRAL, je leta 1996 sprejela vzorčni zakon o elektronskem poslovanju in dve leti kasneje še vzorčni zakon o elektronskem podpisu. Podobno kot UNCITRAL je tudi Evropska unija sprejela dve direktivi, ki se prav tako nanašata na elektronski podpis in elektronsko poslovanje.

Oba dokumenta (Direktiva EU in UNCITRAL-ov vzorčni zakon) za področje elektronskega podpisa sta tehnično orientirana in urejata predvsem potrebno infrastrukturo. Dokumenta za področja elektronskega poslovanja urejata vprašanja ponudb, elektronskega sklepanja pogodb ipd.

5.1.1 UNCITRAL-ov vzorčni zakon o elektronskem poslovanju

Prvi UNCITRAL–ov vzorčni zakon o elektronskem poslovanju [26] iz leta 1996 določa pravni okvir za elektronsko poslovanje. Vsebina temelji na načelih funkcionalne enakovrednosti elektronskega in papirnega okolja, tehnološke nevtralnosti ter avtonomije strank. Vsebuje definicije novih pojmov kot so podatkovno sporočilo, elektronska izmenjava podatkov ipd., odpravlja ovire v zvezi s termini "pisna oblika", "original" ter "lastnoročni podpis" in rešuje vprašanja pravnega priznanja podatkovnega sporočila. Določa tudi nekaj pogojev v zvezi s hrambo sporočil. Implementiran je v mnogih nacionalnih zakonodajah, med drugim tudi v Sloveniji.

5.1.2 Direktiva EU o elektronskem podpisu

Evropski parlament in Svet EU sta decembra 1999 sprejela Direktivo št. 1999/93/EC[27], ki določa pravni okvir za uporabo elektronskega podpisa in digitalnih certifikatov. Dokument pod strogimi pogoji enači elektronski podpis s klasičnim lastnoročnim podpisom in s tem postavlja temelje za postopno nadomeščanje papirnih dokumentov z elektronskimi.

Direktiva definira termine, kot so elektronski podpis in varen elektronski podpis, potrdilo in kvalificirano potrdilo, sredstva in varna sredstva za ustvarjanje elektronskih podpisov itd. Ureja tudi delovanje in odgovornosti overiteljev potrdil in njihovo mednarodno priznavanje v okviru držav EU.

Dokument spremljajo aneksi, v katerih so natančneje navedene varnostne in kvalitativne zahteve oz. priporočila za naslednja področja:

Aneks 1 – zahteve za kvalificirana potrdila;
Aneks 2 – pogoje za delovanje agencij za certificiranje, ki izdajajo kvalificirana potrdila;
Aneks 3 – zahteve za varna sredstva za podpisovanje;
Aneks 4 – priporočila za varno verifikacijo podpisa.

[26] UNCITRAL Model Law on Electronic Commerce with Guide to Enacment 1996 with additional article 5 bis as adopted in 1998 – URL: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

[27] Directive 1999/93/EC of the European Parliament and of the Cuncil of 13 December 1999 on Community Framework for Electronic Signatures – URL: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

5.1.3 Direktiva EU o elektronskem poslovanju

Drugo pomembeno evropsko direktivo na področju elektronskega poslovanja sta Evropski parlament in Svet EU sprejela junija 2000. Dokument z oznako Direktiva št. 2000/31/EC[28] in ureja elektronsko poslovanje na notranjem trgu. Definira termine, kot so elektronske storitve, ponudniki in odjemalci elektronskih storitev ipd. Določa način identifikacije in komunikacije na spletu ter pri tem v veliki meri upošteva varstvo potrošnikov. Dotika se tudi odgovornosti posrednih ponudnikov (telekomunikacijskih ponudnikov, ponudnikov strežniškega prostora, ipd.), ter sodnega varstva za elektronske spore.

5.1.4 UNCITRAL-ov vzorčni zakon o elektronskem podpisu

Drugi UNCITRAL-ov vzorčni zakon o elektronskem podpisu[29], ki je bil sprejet leta 2001, opredeljuje pojme kot so elektronski podpis, digitalno potrdilo, overitelj potrdil itd, ter pod določenimi pogoji pravno enači elektronski in klasični lastnoročni podpis. Vsebuje tudi nekaj določb v zvezi s podpisnikom, overiteljem in tretjo osebo, ter nekaj tehničnih zahtev za posamezne dele infrastrukture varnega okolja poslovanja.

5.2 Slovenska zakonodaja

Republika Slovenija je sledila svetovnim trendom in med prvimi državami v Evropi leta 2000 sprejela **Zakon o elektronskem poslovanju in elektronskem podpisu** (Uradni list RS, št. 57/00). Kasneje, leta 2004, je sprejela še Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu (čistopis: Uradni list RS, št. 98/2004). Zakon dopolnjujeta podzakonska akta **Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje** (Uradni list RS, št. 77/00 in št. 2/01), ter **Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji** (Uradni list RS, št. 99/01), ki natančneje urejata nekatera pravna razmerja in določata nekatere tehnične podrobnosti.

Poleg omenjenih listin je za elektronsko poslovanje pomembna tudi področna zakonodaja. Naj omenim postopkovne zakone in uredbe, ki urejajo kazenski (Kazenski zakonik), pravdni (Pravdni zakonik) in upravni postopek (Zakon o splošnem upravnem postopku). Pomembna sta tudi Zakon o varstvu osebnih podatkov in Zakon o varstvu potrošnikov, za področje arhiviranja še Zakon o arhivskem gradivu in arhivih itd.

[28] Directive 2000/31/EC of the European Parliament and of the Cuncil of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce);
URL: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf.

[29] UNCITRAL Model Law on Electronic Signatureswith Guide to Enacment 2001;
URL: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.

5.2.1 Zakon o elektronskem poslovanju in elektronskem podpisu

Osnovni Zakon o elektronskem poslovanju in elektronskem podpisu - ZEPEP (Uradni list RS, št. 57/00), ki ga je državni zbor sprejel leta 2000, v celoti sledi UNCITRAL-ovemu vzorčnemu zakonu o elektronskem poslovanju in direktivi EU o elektronskem podpisu. V enem dokumentu sta urejeni obe področji, tako elektronsko poslovanje kot tudi elektronski podpis in z njim povezane zadeve. Vsebina je razdeljena v pet poglavij:

1. Splošne določbe (med katerimi najdemo tudi definicije terminov);
2. Elektronsko poslovanje;
3. Elektronski podpis;
4. Kazenske določbe;
5. Prehodne in končne določbe.

Leta 2004 je bila v državnem zboru sprejet Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu ZEPEP-A (Uradni list RS 25/04, str. 2838) poleg nekaterih popravkov oz. dopolnitev razlage izrazov v 2. členu osnovnega zakona (varen časovni žig, storitev informacijske družbe…) ter spremembe nekaj členov, prinaša nov oddelek, v katerem ureja odgovornost ponudnikov storitev v informacijski družbi. Ponudniki so, razen v določenih izjemah, odgovorni za podatke, ki jih posredujejo ali shranjujejo. Za opravljanje tovrstnih storitev ni potrebno pridobiti posebnega dovoljenja.

5.2.1.1 Načela ZEPEP

Zakon ZEPEP temelji na sodobnih načelih (http://www.sigov.si/ca/pravnapojasnila.htm):

- načelo nediskriminacije elektronske oblike;
- načelo odprtosti;
- načelo dvojnosti;
- načelo pogodbene svobode strank;
- načelo varstva osebnih podatkov;
- načelo varstva potrošnikov;
- načelo mednarodnega priznavanja.

Z vidika nediskriminacije sta pomembna 4. in 14. člen ZEPEP, ki izrecno določata, da se podatkom v elektronski obliki ali elektronskemu podpisu ne sme odreči veljavnosti ali dokazne vrednosti zgolj zaradi elektronske oblike. Oba člena, za razliko od ostalih, veljata tudi v zaprtih sistemih, kjer je poslovanje v celoti dogovorjeno s pogodbami med znanim številom strank. Nediskriminacija se kaže tudi v 13. členu ZEPEP, ki elektronsko obliko podatkov enači s klasično, razen za naštete izjeme (pravni posli, s katerimi se prenaša lastninska pravica na nepremičnini, pogodbe o urejanju premoženjskih razmerij med zakoncema, pogodbe o dosmrtnem preživljanju itd.).

Zakon je dovolj splošen in tehnološko nevtralen, da je uporaben za daljše časovno obdobje kljub hitremu in raznolikemu napredku tehnologije. Npr. v 4. alinei 2. člena uvaja pojem varnega elektronskega podpisa, ki je "ustvarjen s sredstvi za varno elektronsko podpisovanje". Prav tako med tehničnimi zahtevami (4. oddelek) navaja pogoje, pod katerimi se elektronsko podpisovanje šteje za varno, medtem ko oblike tehnologije ne predpisuje.

Uporabi raznovrstnih tehnologij sledi tudi načelo dvojnosti oz. dvojnega pristopa. Zakon dopušča vzporedno uporabo različnih tehnoloških rešitev z različno zanesljivostjo in posledično različne pravne posledice. Načelo se kaže tudi v določbah za overitelje. Zakon namreč omogoča njihovo delovanje pod zelo različnimi pogoji.

ZEPEP (1.člen) dopušča pogodbeno svobodo strank, saj dovoljuje tudi zaprte sisteme, v katerih so medsebojna razmerja oz. bistvene značilnosti poslovanja znanega števila strank v celoti urejena s pogodbami. Pogodbene stranke v takšnih sistemih niso vezane na zakonske določbe, z izjemo določb v 4. in 14. členu.

Osebni podatki so v elektronskem poslovanju še bolj izpostavljeni morebitnim zlorabam kot pri klasičnem poslovanju. Prav zato je pomembno, da ZEPEP striktno sledi načelu varstva osebnih podatkov. Zakon sicer ne določa obveznosti overiteljev z vidika varstva osebnih podatkov, vendar dovoljuje uporabo psevdonima v kvalificiranih potrdilih (38. člen) z obvezno navedbo, da gre za psevdonim.

Potrošniki (uporabniki) v splošnem ne razpolagajo z ustreznim tehnološkim znanjem, v elektronskem svetu, zato sami težko uveljavljajo svoje pravice. Zaradi tega je pomembno da ZEPEP sledi načelu varstva potrošnikov in ponudnikom storitev nalaga obveznosti povezane z urejanjem potrošnikovih pravic.

ZEPEP pravno ureja tudi mednarodno priznavanje elektronskih podpisov in potrdil. V 46. členu medsebojno priznava elektronske podpise znotraj Evropske unije in pod določenimi pogoji tudi v tretjih deželah.

5.2.1.2 Elektronsko poslovanje

Pod elektronskim poslovanjem razumemo celoten proces obdelave elektronskih podatkov s pomočjo informacijske tehnologije: od oblikovanja in pošiljanja do prejemanja in shranjevanja podatkov. Zakon natančneje določa elektronsko izmenjavo podatkov za odprte sisteme, znotraj zaprtih sistemov se pogodbene stranke lahko dogovorijo tudi drugače (1. člen). ZEPEP med drugim določa, da je sporočilo odposlano takrat, ko vstopi v informacijski sistem, ki je izven nadzora pošiljatelja (9. člen). Za čas prejema elektronskega sporočila se šteje tisti čas, ko je sporočilo vstopilo v prejemnikov informacijski sistem (10. člen). Stranki, pošiljatelj in prejemnik, se lahko dogovorita, da se

prejem sporočila potrdi (7. člen). Če v tem primeru pošiljatelj ne dobi potrdila o prejemu, po zakonu sporočilo ni bilo poslano. Potrdilo o prejemu ne dokazuje istovetnosti poslanega in prejetega sporočila (8. člen). Zanimiva je določba v zvezi s krajem pošiljanja oz. prejemanja elektronskega sporočila (11. člen). Kraj, od koder je bilo sporočilo poslano, je sedež pravne osebe oz. stalno prebivališče fizične osebe. Prav tako je sedež pravne osebe ali stalno prebivališče fizične osebe tudi kraj prejema sporočila.

ZEPEP se v 12. členu (sicer bolj skopo) dotika tudi hrambe elektronskih objektov. Določeni dokumenti, zapisi ali podatki se lahko hranijo v elektronski obliki, če so v tej obliki dosegljivi in primerni za kasnejšo uporabo in če je zanje mogoče ugotoviti izvor, čas in kraj pošiljanja ali prejema, ter prejemnika. Podatke je potrebno hraniti v obliki, v kateri so bili oblikovani, poslani oz. prejeti, ali v kakšni drugi obliki, ki verodostojno ohranja te podatke. Obvezen pogoj je tudi primerna tehnologija, ki onemogoča spremenljivost ali izbris podatkov. Te določbe ne veljajo za podatke, za katere zakon določa strožje ali posebne pogoje hrambe (izjeme so določene v 13. členu zakona).

5.2.1.3 Elektronski podpis

ZEPEP loči med elektronskim podpisom v splošnem in varnim elektronskim podpisom, ki mora izpolnjevati določene zahteve, zapisane v 2. členu. Klasičnemu lastnoročnemu podpisu je enakovreden le varen elektronski podpis overjen s kvalificiranim potrdilom (15. člen), ki mora izpolnjevati najstrožje pogoje. Tukaj je zakonodajalec nekoliko nedosleden glede določb in tehnike overjanja (Pavliha, 2002, str. 77), saj z digitalnim potrdilom ne overjamo elektronskega podpisa, temveč preverjamo pristnost dokumenta in podpisa.

Tehnične zahteve za varno elektronsko podpisovanje so v zakonu uvrščene v poglavje Potrdila in overitelji in predpisujejo, da morajo sredstva za varno elektronsko podpisovanje izpolnjevati načelo: "To kar vidim je to kar podpišem". To pomeni, da ta sredstva ne smejo preprečiti prikaz podatkov pred podpisom, ter da podpisanih podatkov ne smejo spremeniti.

Sredstva za varno podpisovanje podatkov morajo izpolnjevati tudi naslednje določbe (ZEPEP, Uradni list RS, št. 98/2004):

1. podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena;
2. podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa oz. elektronski podpis je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije;
3. podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom.

Tudi pri preverjanju varnega elektronskega podpisa veljajo podobne določbe. Vsebina, podatki za preverjanje podpisa in rezultati preverjanja morajo biti zanesljivi in pravilno prikazani uporabniku. V času preverjanja mora biti preverjena tudi pristnost in veljavnost potrdila.

5.2.1.4 Potrdila in overitelji

ZEPEP določa, da overitelji za tozadevno delovanje ne potrebujejo posebnega dovoljenja, zadostuje le prijava na ministrstvu, pristojnemu za informacijsko družbo (18. člen). Zakonsko so urejene tudi razmere v primeru prenehanja delovanja (27. člen), ko mora overitelj zagotoviti, da vse pravice in obveznosti glede izdanih potrdil prevzame drug overitelj.

Več členov je namenjenih preklicu elektronskih potrdil. Overitelj mora nemudoma preklicati (20. člen) izdano potrdilo in o tem obvestiti imetnika preklicanega potrdila v primerih, ko preklic potrdila zahteva imetnik potrdila ali njegov pooblaščenec, če so se spremenile okoliščine, ki bistveno vplivajo na veljavnost potrdila (smrt imetnika potrdila, izguba poslovnih sposobnosti,…), v primerih netočnih podatkov, če preklic odredi pristojno sodišče itd. Preklic potrdila mora biti javno objavljen in mora vsebovati čas preklica (24. člen). Natančnost navedbe časa (minuta, sekunda…) ni predpisana. Preklic za nazaj ni dovoljen (24. člen).

ZEPEP posebej obravnava kvalificirana elektronska potrdila in njihove izdajatelje. Natančno je določena vsebina kvalificiranih potrdil (28. člen), zahtevano je tudi zanesljivo ugotavljanje identitete in drugih pomembnih lastnosti osebe, ki zahteva potrdilo (31. člen). Stroge so še zahteve glede usposobljenosti osebja (32. člen), ki ga overitelj kvalificiranih potrdil zaposluje, ter zahteve glede sredstev (33. člen), ki jih tak overitelj uporablja. Zakon še določa odgovornost overiteljev (39. člen) in predpisuje nadzor nad njimi (40. in 41. člen).

Overitelji lahko postanejo akreditirani (42. člen), če dokažejo izpolnjevanje vseh z zakonom in podzakonskimi predpisi predpisanih pogojev. Akreditirane overitelje se vpiše v poseben register, ki ga vodi akreditacijski organ. Overitelji lahko svojo akreditiranost označijo tudi v izdanih potrdilih.

5.2.2 Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 in št. 2/01), ki jo je sprejela Vlada Republike Slovenije, podrobneje določa tehnologijo, kot ZEPEP. Vsebuje podrobnejša pravila o delovanju overiteljev in tehnične pogoje v zvezi digitalnim podpisom in njegovim preverjanjem, časovnim žigom, časovno veljavnostjo digitalnimh potrdili itd. Med drugim določa, da morajo biti elektronsko

podpisani podatki časovnim žigosani še v času veljavnosti pripadajočega kvalificiranega potrdila.

5.3 Elektronsko arhiviranje

Elektronska hramba in arhiviranje elektronskih zapisov je v slovenski zakonodaji še vedno pomanjkljivo urejena. Čeprav področni Zakon o arhivskem gradivu in arhivih dovoljuje uporabo drugih medijev, je prilagojen oz. namenjen regulaciji hrambe klasičnih (papirnih) dokumentov. ZEPEP se hrambe dotika le v 12. točki, kjer dovoljuje hrambo v elektronski obliki pod naslednjimi pogoji (ZEPEP, Uradni list RS, št. 98/2004):

- če so podatki, vsebovani v elektronskem dokumentu ali zapisu, dosegljivi in primerni za kasnejšo uporabo;
- če so podatki shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti, ali v kakšni drugi obliki, ki verodostojno predstavlja oblikovane, poslane ali prejete podatke;
- če je iz shranjenega elektronskega sporočila mogoče ugotoviti, od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema;
- če uporabljena tehnologija in postopki v zadostni meri onemogočajo spremembo ali izbris podatkov, ki ju ne bi bilo mogoče enostavno ugotoviti, oziroma obstaja zanesljivo jamstvo glede nespremenljivosti sporočila.

Oblikovanje, pošiljanje, sprejemanje in shranjevanje elektronskih dokumentov v nekaterih primerih konkretneje urejajo podzakonski akti. V skladu z Uredbo o poslovanju organov javne uprave z dokumentarnim gradivom (Uradni list RS št. 91/2001) morajo organi javne uprave za dokumentarno gradivo, ki vsebuje elektronsko podpisane podatke, zagotoviti ponoven elektronski podpis teh podatkov preden je zanesljivost elektronskega podpisa zmanjšana. Prav tako morajo ločeno od gradiva hraniti podatke o šifriranju ipd.

5.4 Zaključek poglavja 5

V Sloveniji ni več pravnih ovir za uporabo elektronskega podpisa in hrambo elektronskega gradiva. Kljub temu je ponekod potrebno vzporedno hraniti tudi papirno obliko. Sedanja arhivska zakonodaja namreč ne ureja področja varstva elektronskega dokumentarnega in arhivskega gradiva. Ker problematika terja celovito ureditev, je bil v zakonodajni postopek v državnem zboru vložen predlog novega Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih – ZVDAGA. Z menjavo mandata državnega zbora se je v skladu z določili 154. člena Poslovnika državnega zbora postopek končal. Slovenija tako ostaja brez ustrezne zakonodaje na področju elektronske hrambe dokumentarnega in arhivskega gradiva.

6 PREDLOG MODELA VARNEGA OKOLJA ZA E-ARHIVIRANJE

V tem poglavju predstavljam predlog idejnega modela varnega okolja za arhiviranje elektronskih dokumentov. Ker celovitih rešitev za varovanje dokumentov ni, sem idejni model sestavila iz komponent, ki sem jih spoznala ob prebiranju literature, naštete na koncu tega magistrskega dela. Nastali model (integracija obstočeh delnih rešitev) odgovarja na v Uvodu zastavljeno vprašanje: Na kakšen način lahko dosežemo zadovoljivo raven varnosti elektronskih dokumentov? Varnost elektronskih dokumentov lahko zagotovimo le s smiselno in logično povezanimi sklopi, ki skupaj tvorijo celovit sistem za varno ravnanje z elektronskimi dokumenti od nastanka do arhiva. Vsak izmed sklopov mora upoštevati standarde, ki zagotavljajo najvišji nivo varnosti. Celoten sistem mora biti zasnovan tako, da v največji možni meri zmanjšuje možnosti zlorab in napak s strani človeškega faktorja.

V okviru osnovnega cilja, to je varovanje verodostojnosti dokumentov na celotni poti dokumenta, je potrebno zagotoviti naslednje funkcionalnosti:

- digitalno podpisovanje dokumentov in poštnih sporočil;
- razpoznavanje udeležencev varnih komunikacij;
- časovno žigosanje dokumentov;
- varno arhiviranje dokumentov.

Pot do cilja sem razdelila v več funkcionalno in tehnično smiselnih točk:

1. idejni scenarij;
2. identifikacija akterjev;
3. opravila na strani akterjev;
4. osnovna arhitektura predloga;
5. aplikacija za digitalno podpisovanje in preverjanje podpisa;
6. arhivski sistem;
7. model varnega okolja;
8. formalizacija;
9. nadzor

Idejni model je zasnovan zelo splošno in ne upošteva nobenih posebnih okoliščin.

6.1 Idejni scenarij

Oseba A pripravi dokument in ga digitalno podpiše. Dokument pripne v elektronsko pošto in ga v obliki poštnega sporočila pošlje podjetju X. Za takšno rešitev sem se odločila iz dveh razlogov:

(1) Elektronski dokument nastopa kot samostojen objekt, ki ga bo potrebno arhivirati, zato ni primerno digitalno podpisovanje dokumenta kot dela poštnega

sporočila.

(2) Vse priponke, ki prispejo v podjetje X, marajo biti protivirusno pregledane, zato pošiljanje priponke preko spletne aplikacije ni primerno.

Podjetje X prejme sporočilo s pripetim dokumentom ter preveri avtentičnost in celovitost dokumenta. V primeru ustreznega rezultata dokument uvrsti v svoj poslovni proces. V zamišljenem scenariju je morebitna javna objava dokumenta vključena v poslovni proces.

Podjetje X hrani dokument skladno z veljavno zakonodajo. Po izteku zakonskega roka hrambe pošlje dokument v hrambo varnemu javnemu elektronskemu arhivu. Za pošiljanje uporabi namensko aplikacijo in SSL šifrirani komunikacijski kanal. Za takšno rešitev sem se odločila predvsem iz dveh razlogov:

(1) Podjetje X pošilja varnemu elektronskemu arhivu večje število arhivskih dokumentov hkrati, kar poteka avtomatsko. Pošiljanje dokumentov v obliki priponk v poštnih sporočilih je za takšno rabo neprimerno.

(2) Na strani varnega arhiva sprejema arhivsko gradivo namenska aplikacija, ki mora opraviti večje število preverjanj. Uporaba klasične poštne aplikacije v takšnem primeru ni optimalna rešitev.

Arhiv sprejme dokument, preveri njegovo ustreznost in ga arhivira. V času zakonsko predpisane hrambe dokumenta omogoči njegovo uporabo uporabnikom, določenim v pogodbi, ki sta jo predhodno sklenila podjetje X in javni arhiv.

Osnovno izhodišče idejnega scenarija je uporaba infrastrukture javnih ključev. Iz tega izhajajo potrebe po:

- pridobitvi digitalnega potrdila za vse udeležence (akterje) v modelu;
- objavi potrdil v javnem imeniku,
- morebitnem preklicu digitalnega potrdila.

Predpostavljam, da akterji delujejo v skladu z varnostnimi pravili, kot je to hramba privatnega ključa in digitalnega potrdila na varni in prenosljivi napravi, s katere ga ni mogoče kopirati (npr. na pametni kartici). Predpostavljam tudi, da so vse transakcije, predvidene v modelu, opravljene na varen način in vključujejo avtentikacijo obeh strani transakcije.

6.2 Identifikacija akterjev

Iz idejnega scenarija predloga varnega arhiviranja sem izluščila minimalen nabor akterjev:

1. avtor oz. ustvarjalec digitalno podpisanega dokumenta (oseba A);
2. prejemnik digitalno podpisanega dokumenta (podjetje X);
3. varen javni elektronski arhiv (TAA);
4. agencija za registracijo uporabnikov (RA);

5. agencija za overjanje javnih ključev (CA);
6. agencija za časovno žigosanje (TSA);
7. stranke (uporabniki) digitalno podpisanega dokumenta.

6.3 Ravnanje z dokumenti

Zaradi preglednosti je celotna pot dokumenta smiselno razdeljena v štiri dele:

- aktivnosti na strani pošiljatelja;
- aktivnosti na strani prejemnika – produkcijski del;
- aktivnosti na strani prejemnika – arhivske aktivnosti;
- aktivnosti na strani arhiva.

Vsak del poti je opisan kot celota zase in obdelan po enotnem metodološkem pristopu, ki obsega kratek povzetek scenarija, pogoje, ki morajo biti izpolnjeni za izvedbo opravil, ter vrstni red opravil na strani akterja. Posamezne dele povezujejo elementi dokumenta in komunikacijski protokoli. Aktivnosti entitet, ki imajo na poti dokumenta posredno vlogo (certifikatna agencija, agencija za časovno žigosanje), so podrobneje opisane v drugem poglavju tega magistrskega dela.

Prvi del poti – priprava in pošiljanje dokumenta

Povzetek scenarija:
Oseba A pripravi dokument in ga preko elektronske pošte pošlje podjetju X.

Pogoji:

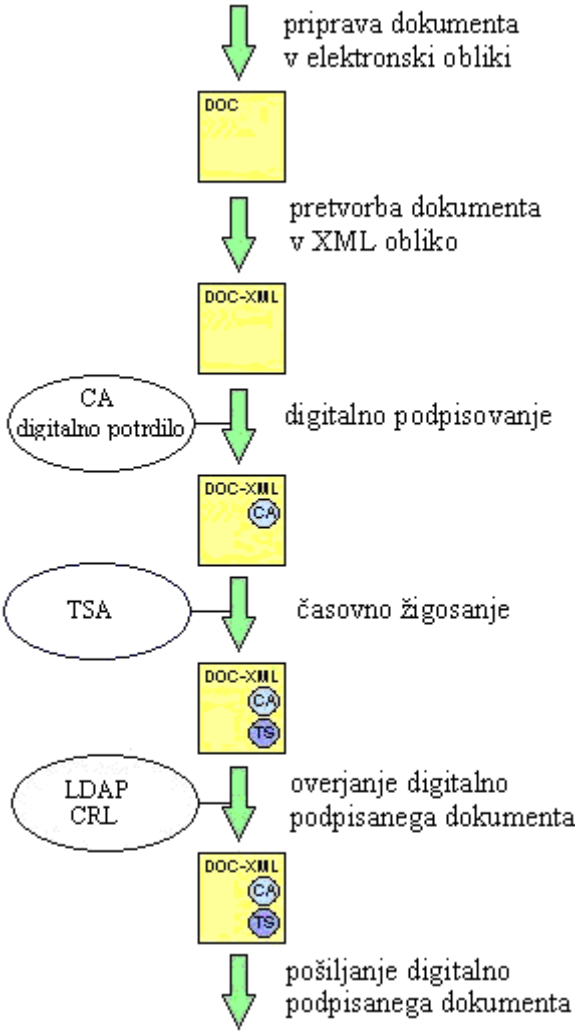
(1) oseba A ima dostop do interneta od doma oz. lokacije na terenu;
(2) oseba A ima veljavno digitalno potrdilo;
(3) podjetje X oz. strežnik podjetja X ima veljavno digitalno potrdilo;
(4) informacijska sistema na obeh straneh transakcije imata implementirano aplikacijo, ki podpira digitalno podpisovanje in overjanje digitalno podpisanih dokumentov;
(5) aplikaciji na obeh straneh transakcije imata uvoženo veljavno digitalno potrdilo oz. ustrezno referenco;
(6) zagotovljeno je navzkrižno potrjevanje digitalnih potrdil uporabnikov (avtorizacija informacijskih virov).

Opravila na strani osebe A:

(1) priprava dokumenta v elektronski obliki,
(2) pretvorba dokumenta v obliko XML,
(3) digitalno podpisovanje dokumenta,
(4) časovno žigosanje dokumenta,
(5) overjanje digitalno podpisanega dokumenta,

(6) vzpostavitev varne povezave s podjetjem X in navzkrižno overjanje digitalnih potrdil;
(7) pošiljanje dokumenta.

Slika 30: Ravnanje z dokumenti – prvi del poti



Drugi del poti – sprejem in objava dokumenta

Povzetek scenarija:
Podjetje X prejme digitalno podpisan dokument in izvede postopek overjanja (ustrezen modul preveri celovitost dokumenta, veljavnost digitalnega potrdila in časovnega žiga). Sistem podjetja X pošlje klientu (osebi X) obvestilo o prejemu dokumenta in rezultatu overitve. Dokument v podjetju X nadaljuje pot v okviru poslovnega procesa.

Pogoji:

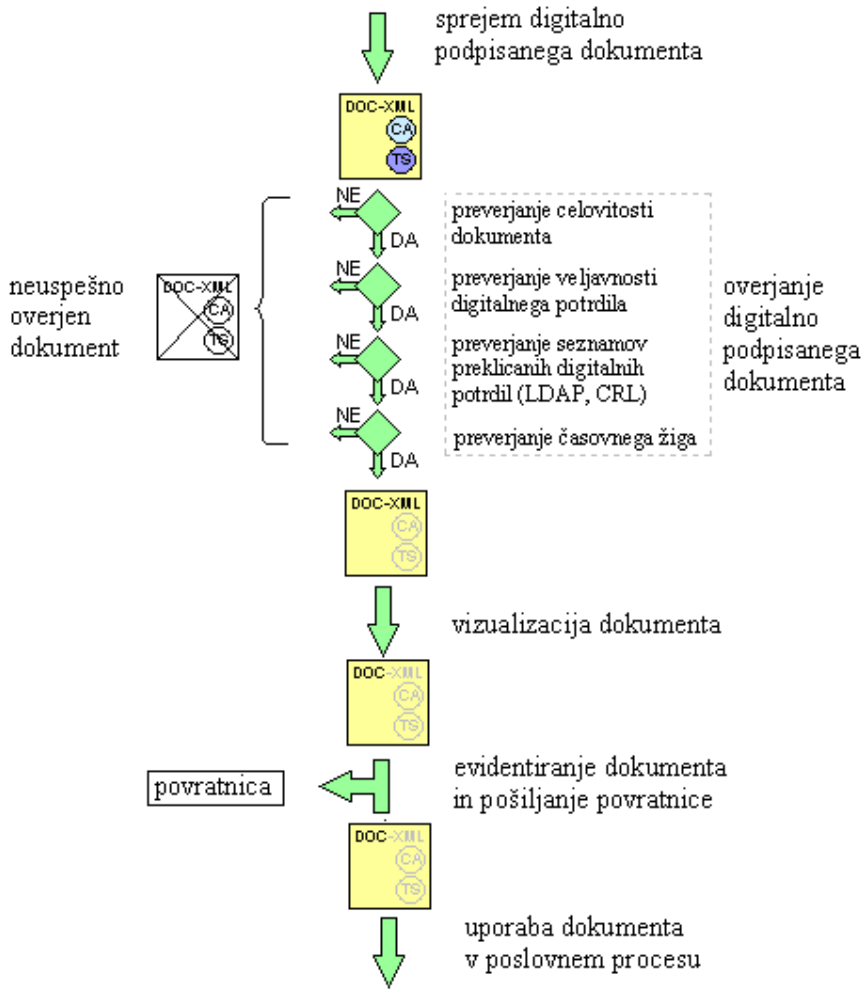
(1) oseba A ima dostop do interneta od doma oz. iz lokacije na terenu;
(2) oseba A ima veljavno digitalno potrdilo;

(3) podjetje X oz. strežnik podjetja X ima veljavno digitalno potrdilo;
(4) informacijska sistema na obeh straneh transakcije imata implementirano aplikacijo, ki podpira digitalno podpisovanje in overjanje digitalno podpisanih dokumentov;
(5) aplikaciji na obeh straneh transakcije imata uvoženo veljavno digitalno potrdilo oz. ustrezno referenco;
(6) zagotovljeno je navzkrižno potrjevanje digitalnih potrdil uporabnikov (avtorizacija informacijskih virov).

Opravila na strani podjetja X:

(1) vzpostavitev varne povezave z osebo A in navzkrižno overjanje digitalnih potrdil;
(2) sprejem digitalno podpisanega dokumenta;
(3) overjanje digitalno podpisanega dokumenta;
(4) vizualizacija dokumenta;
(5) evidentiranje dokumenta in pošiljanje povratnice;
(6) uporaba dokumenta v okviru poslovnega procesa.

Slika 31: Ravnanje z dokumenti – drugi del poti



Tretji del poti – interna hramba dokumenta v skladu z zakonodajo

Povzetek scenarija:
Arhivski sistem podjetja X arhivira uspešno overjen digitalno podpisan dokument in v okviru zakonsko določenega roka hrambe skrbi za njegovo varnost, vključno z izdelavo varnostnih kopij za primer izgube podatkov.

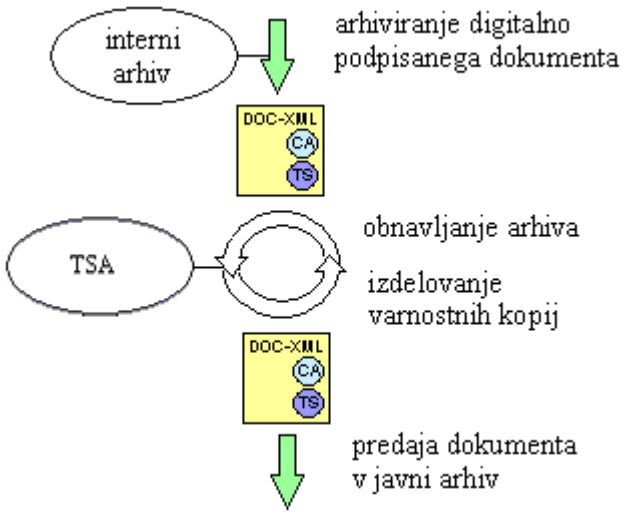
Pogoji:

(1) digitalno podpisan dokument je uspešno overjen;
(2) podjetje X ima ustrezno informacijsko okolje za varno hrambo dokumenta.

Opravila na strani podjetja X:

(1) arhiviranje uspešno overjenega digitalno podpisanega dokumenta;
(2) obnavljanje arhiva;
(3) izdelovanje varnostnih kopij;
(4) vzpostavitev varne povezave z varnim javnim arhivom in navzkrižno overjanje digitalnih potrdil;
(5) predaja dokumenta v javni arhiv.

Slika 32: Ravnanje z dokumenti – tretji del poti



Četrti del poti – sprejem in hramba dokumenta v javnem arhivu

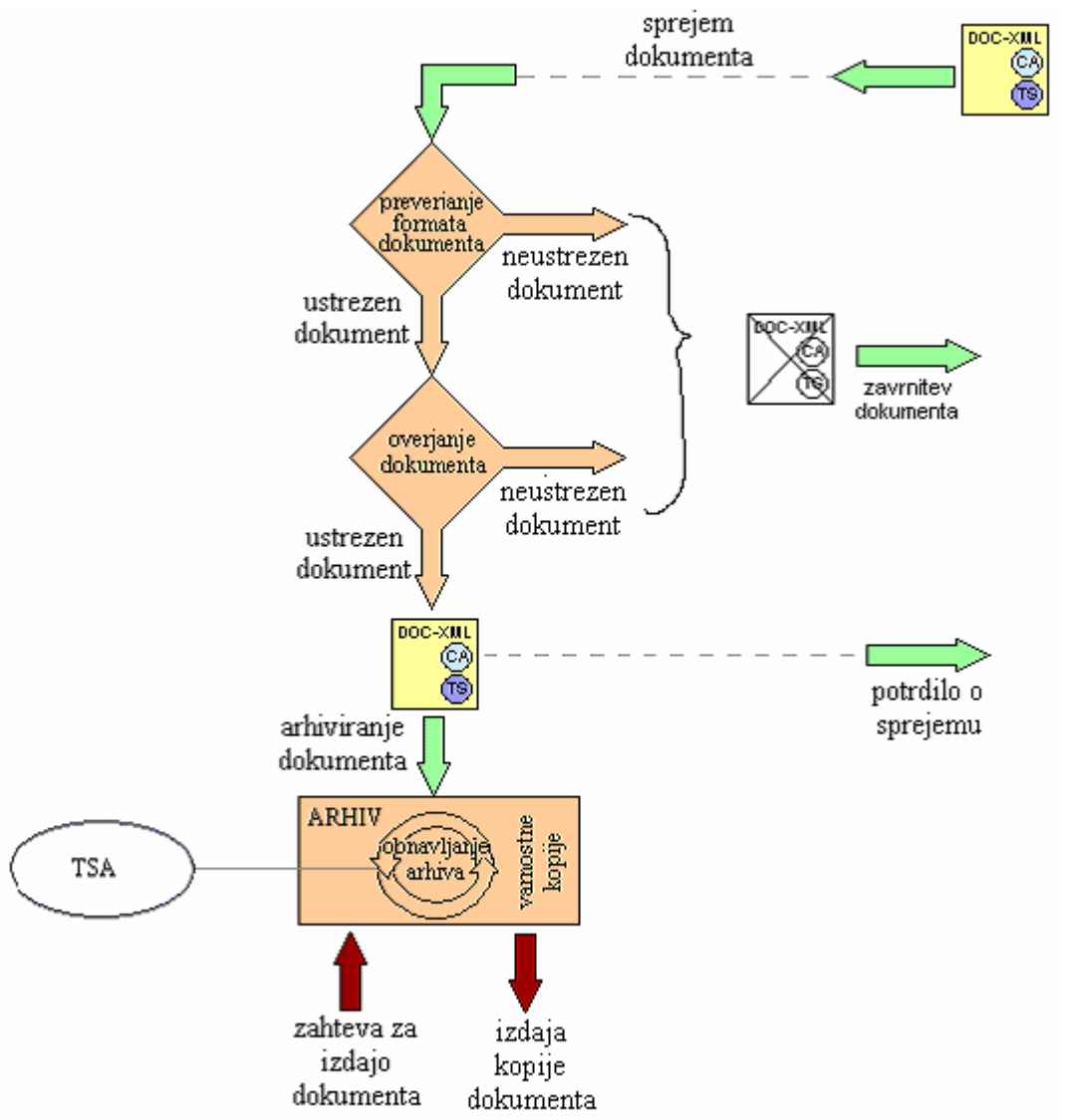
Povzetek scenarija:
Po preteku zakonskega roka hrambe podjetje X pošlje dokument v hrambo javnemu arhivu, s katerim ima sklenjeno pogodbo o sodelovanju. Ob vzpostavitvi komunikacije je potrebna avtorizacija obeh strani transakcije. Informacijski sistem javnega arhiva v skladu s pogodbo najprej preveri ustreznost dokumenta (format dokumenta, format digitalnega podpisa) in izvede postopek overjanja. Če je dokument ustrezen, ga sistem arhivira.

Arhivski sistem v času hrambe skrbi za izvajanje varnostnih ukrepov pred izgubo ali zlorabo dokumenta. Če uporabnik v arhivu naredi poizvedbo po določenem dokumentu, ga iskalni mehanizem poišče in uporabniku vrne kopijo dokumenta.

Pogoji:

(1) med podjetjem X in javnim elektronskim arhivom je sklenjena pogodba o sodelovanju;
(2) zagotovljeno je navzkrižno potrjevanje digitalnih potrdil uporabnikov (avtorizacija informacijskih virov).

Slika 33: Ravnanje z dokumenti - četrti del poti



Opravila na strani varnega javnega arhiva:

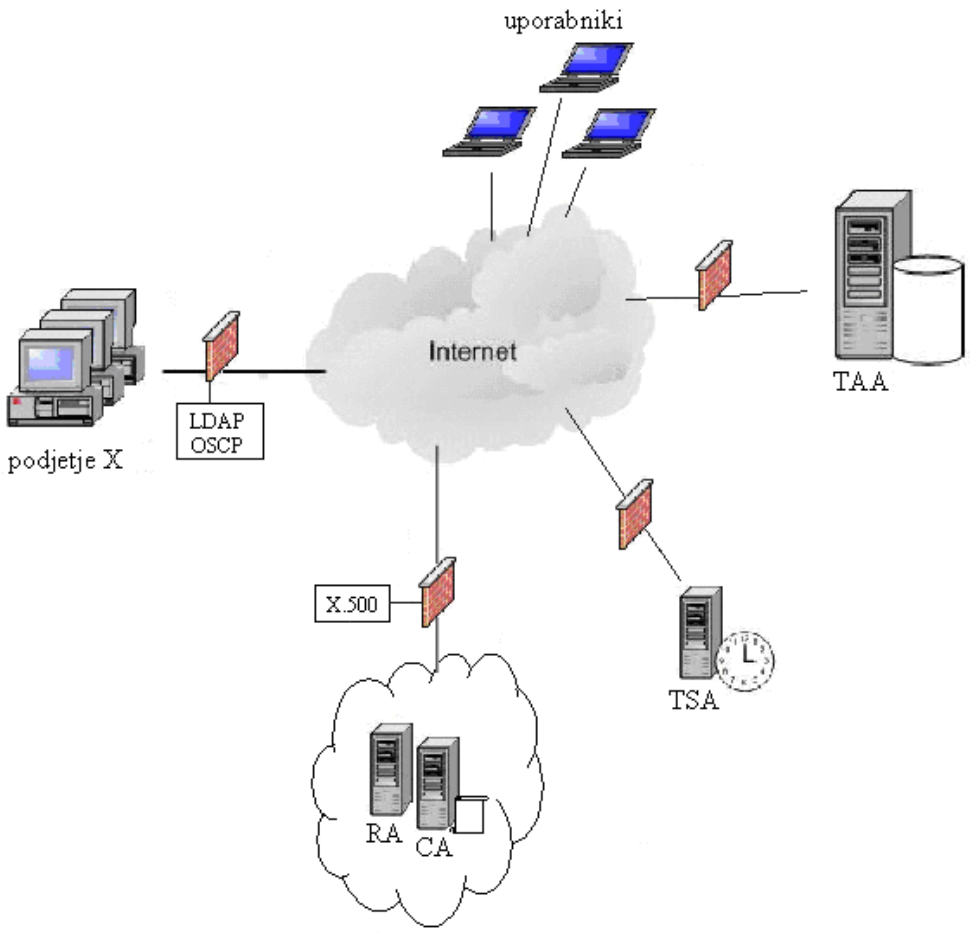
(1) vzpostavitev varne povezave s podjetjem X in navzkrižno overjanje digitalnih potrdil;
(2) sprejem digitalno podpisanega dokumenta;

(3) preverjanje ustreznosti dokumenta glede na pogodbo (format dokumenta, format digitalnega podpisa ipd.);
(4) overjanje digitalno podpisanega dokumenta;
(5) evidentiranje prejetega dokumenta in pošiljanje povratnice;
(6) indeksiranje in dodeljevanje atributov;
(7) arhiviranje digitalno podpisanega dokumenta;
(8) obnavljanje arhiva in izdelovanje varnostnih kopij;
(9) izdajanje kopije dokumenta (v skladu s pogodbo) na zahtevo stranke.

6.4 Osnovna arhitektura predloga

Za realizacijo idejnega scenarija potrebujemo infrastrukturo, ki omogoča varno digitalno podpisovanje dokumentov, varno ravnanje in poslovanje z digitalno podpisanimi dokumenti, ter razpoznavanje uporabnikov. Idejni model vključuje delo namenskih agencij za registracijo in overjanje javnih ključev ter agencijo za izdajanje časovnih žigov. Predvidena je uporaba storitev varnega javnega elektronskega arhiva, čeprav takšne ustanove v Republiki Sloveniji še ni. Osnovna arhitektura celotnega sistema je prikazana na sliki 34.

Slika 34: Osnovna arhitektura modela



Prenosna pot je javno omrežje (Internet). Lokalna omrežja so zaščitena s požarnimi pregradami. Predpostavljam, da imajo vključene namenske agencije in javni elektronski arhiv ustrezne informacijske sisteme in izpolnjujejo zakonske določbe za opravljanje dejavnosti. Za vzpostavitev elektronskega poslovanja z digitalno podpisanimi dokumenti je potrebno zagotoviti ustrezno infrastrukturo še na strani podjetja X. Priporočljivo je, da podjetje X in javni elektronski arhiv namestita lastne imeniške strežnike (LDAP, OSCP) za preverjanje digitalnih potrdil in s tem omogočita delno neodvisnost preverjanja digitalnih potrdil od agencij. To je pomembno predvsem z vidika razpoznavanja uporabnikov znotraj lokalnega omrežja za selektiven dostop do dokumentov tudi v primeru izpada komunikacije z javnim omrežjem. V tem primeru je potrebno zagotoviti medimeniško sinhronizacijo z glavnim X.500 strežnikom, zato LDAP in OSCP strežnika implementiramo v DMZ (angl. Demilitarize Zone) območje.

6.5 Aplikacija za digitalno podpisovanje in preverjanje podpisa

Za digitalno podpisovanje in preverjanje podpisanih dokumentov potrebujemo aplikacijo, ki podpira uporabo digitalnih potrdil. Običajno sta obe sredstvi (za podpisovanje in verifikacijo podpisa) integrirani v poslovne aplikacije in ne obstajata kot samostojni namenski aplikaciji.

Na tržišču je mogoče kupiti aplikacije in posebne programske vmesnike, ki sami po sebi podpirajo digitalno podpisovanje dokumentov z uporabo digitalnih potrdil. Dokumente v PDF formatu lahko podpisujemo na datotečnem sistemu ali preko spleta z Acrobat PDF Writer aplikacijo in brez dodatkov ali z Acrobat Reader aplikacijo in dodatno programsko opremo (Accertia PDF-Sign, Adobe PDF-Signer). Tudi orodja, ki iz drugih tipov dokumentov tvorijo PDF dokumente, imajo možnost digitalnega podpisovanja, ki se doda po končani pretvorbi. Takšno orodje je na primer PDFExec for MS-Word ali PDFExec for MS Office.

Sicer ima tudi MS office zbirka verzije 2003 možnost dodajanja digitalnega podpisa preko poti: Tools > Options > Security > Digital Signatures > Add. V aplikacijo je mogoče dodati tudi namenski gumb, ki skrajša opisano pot na en klik. Od trenutka ko je dokument podpisan, podpis ostaja na dokumentu dokler dokument ponovno ne shranimo. Vsak "Shrani" (angl. Save) ukaz podpis odstrani.

V nekaterih poslovnih sistemih je za digitalno podpisovanje potrebna namenska aplikacija. Ta lahko omogoča:

- podpisovanje in preverjanje dokumenta oz. datoteke,
- podpisovanje in preverjanje elektronske pošte (podpiše se celotna vsebina sporočila, to je vsebina in vse priponke kot ena celota).

Za idejni scenarij, kakršen je opisan v tem magistrskem delu, je zaradi arhiviranja elektronskih dokumentov pomembna namestitev aplikacije, ki omogoča podpisovanje samostojnih dokumentov oz. datotek. V primeru razvoja namenske aplikacije, je potrebno upoštevati naslednja priporočila (e-SLOG - Aplikacije za varno elektronsko podpisovanje in preverjanje podpisa, str. 6):

- podpisnik si pred podpisovanjem lahko ogleda vsebino dokumenta v njemu razumljivi obliki;
- če je dokument sestavljen na način, ki ločuje podatke od njihove predstavitve, mora elektronski podpis varovati tako izvorne podatke, kot njihove predstavitvene podatke;
- podpisnik mora ob podpisu imeti možnost izbire digitalnega potrdila;
- aplikacija za podpisovanje mora biti povezana s poslovno aplikacijo na varen način, tako da preprečuje zlorabo iz okolja (npr. "trojanski konj");
- aplikacija za podpisovanje mora vsebovati razumljiv uporabniški vmesnik;
- aplikacija za podpisovanje mora v primeru, ko se podpisuje le del dokumenta, jasno prikazati, kateri del je predmet podpisa;
- naprava za ustvarjanje podpisa preveri istovetnost podpisnika (npr. preverjanje PIN kode);
- aplikacija mora omogočati lokalno hrambo in pregledovanje dokumentov za podpis, rezultate podpisa in dokumente, katerih podpis preverja;
- uporabnik ima dostop do politike elektronskega podpisa, ki vsebuje vsa določila o podpisovanju in preverjanju podpisa;
- pred podpisom mora biti podpisnik seznanjen z vrednostjo podpisnih atributov, kateri so vključeni v podpis; njihov pomen mora biti natančno opredeljen v politiki podpisovanja (npr. sklic na podpisnikovo digitalno potrdilo ipd.);
- sredstvo za ustvarjanje varnega elektronskega podpisa naj podpira varno namensko strojno opremo (npr. "pametne kartice");
- sredstvo za ustvarjanje varnega elektronskega podpisa ne uporablja podatkov za elektronsko podpisovanje brez vednosti imetnika teh podatkov;
- za vzpostavitev enakovrednosti elektronskega podpisa z lastnoročnim podpisom, mora podpisnik uporabiti kvalificirano digitalno potrdilo;
- format dokumenta za podpis je dokumentiran in po možnosti standardiziran;
- format podpisa je standarden in je dokumentiran;
- sredstvo za ustvarjanje varnega elektronskega podpisa ne spreminja podatkov, ki jih podpisuje;
- sredstvo za ustvarjanje varnega elektronskega podpisa mora podpisnika opozoriti na morebitne skrite podatke (skrito besedilo, makroje ipd.);
- če je podpisnik med podpisovanjem dlje časa neaktiven, se podpisovanje prekine; po prekinitvi se mora postopek začeti znova;
- natančna pravila za izvedbo elektronskega podpisa je potrebno opredeliti v politiki e-podpisa;
- podpisnik mora podpisan elektronski dokument shraniti v elektronski arhiv.

6.6 Tehnološke rešitve za vzpostavitev in delovanje arhivskega sistema

Najšibkejši člen v življenjskem ciklu digitalno podpisanega e-dokumenta je faza arhiviranja. Arhivski sistem mora obvladovati običajne lastnosti arhivov, kot so:

- veliko število objektov;
- nizka aktivnost objektov;
- fiksna vsebina objektov (vsebina se ne spreminja);
- dolga doba trajanja objektov (leta, desetletja ipd.).

Za dolgoročno obvladovanje elektronskih objektov je potrebno upoštevati tako zakonske določbe v zvezi z elektronskim poslovanjem in digitalnim podpisovanjem dokumentov, kot tudi določbe v zvezi dokumentarnim in arhivskim gradivom. Implementirati je potrebno informacijsko arhitekturo, ki bo omogočala visoko nadgradljivost in prilagodljivost sistema raznim spremembam. Kljub nenehni rasti količine objektov mora biti zagotovljeno enostavno upravljanje z minimalnim administriranjem. Z vidika varnosti je potrebno poskrbeti za:

- avtentičnost – zagotovilo, da vsebina ni bila spremenjena;
- dostop v razumno trajajočem času;
- trajnost podatkov - zaščita pred zastarelostjo tehnologije;
- zanesljivost – varovanje pred izgubo podatkov ipd.

V praksi še ni na voljo celovitih rešitev za arhivsko problematiko. Podane so le komponente iz katerih je možno sestaviti konsistentno rešitev. Minimalen nabor komponent, ki jih mora vsebovati rešitev, je naslednji:

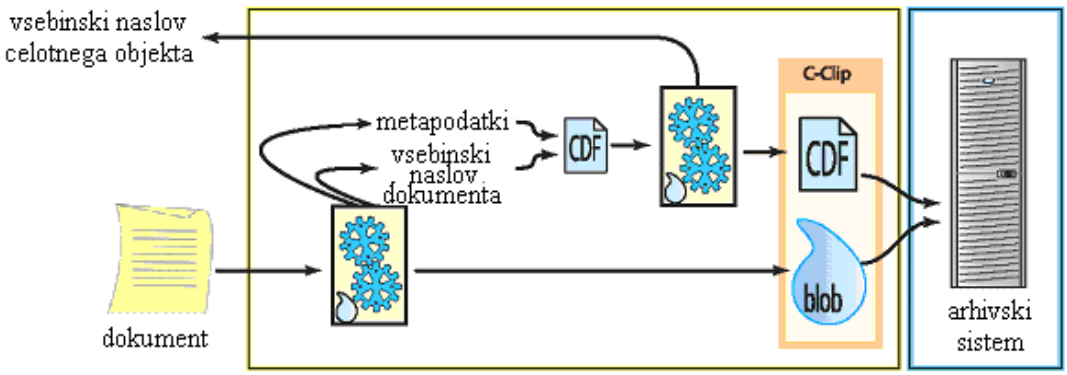
- fizične infrastruktura;
- sistem za upravljanje hrambe (kako in kje bodo informacije shranjene);
- posebne komponente za zagotavljanje verodostojnosti shranjenega gradiva (vključno z mehanizmi za preverjanje);
- sistem za upravljanje z dokumenti;
- opcijske strojne komponente;
- uporabniške vmesnike za komunikacijo med arhivskimi plastmi.

6.6.1 Fizična hramba gradiva

Na tržišču je mogoče kupiti produkte, ki rešujejo fizični sloj arhivske problematike. Dominirajo objektno orientirani rešitve s t.i. vsebinskim naslavljanjem (angl. Content Addressing), ki omogoča individualno hrambo objektov neodvisno od fizične lokacije objekta in razvoja strojne opreme. Vsak objekt dobi unikatno identifikacijo – vsebinski naslov, ki se izračuna iz binarne vsebine objekta z zgoščevalnim algoritmom (poglavje 2.1.2.1). Naslov in atributi objekta (podatki o uporabniku, metapodatki) se shranijo v novi CDF datoteki (angl. C-Clip Descriptor File), ki ima XML obliko. Kreira se vsebinski identifikator CDF datoteke, ki ohranja sled o objektu. Vsebina objekta se shrani v t.i. blob.

Neposreden dostop do vsebinsko naslovljenih objektov je možen preko odprtega aplikacijskega vmesnika API (angl. Application Programming Interface).

Slika 35: Vsebinsko naslavljanje objektov



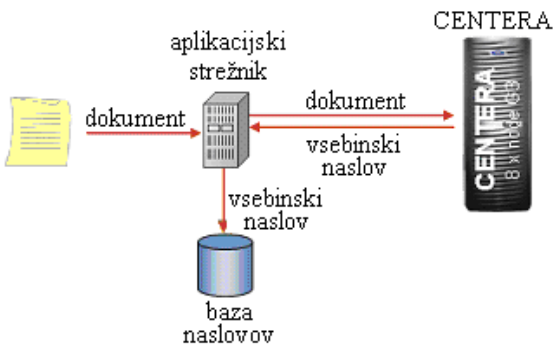
Vir: EMC Corporation, 2005, str. I-9

Vsebinsko naslavljanje digitalnih objektov prinaša naslednje prednosti:

- preverljivost avtentičnosti vsebine – sistem lahko verificira shranjene objekte z enoličnim vsebinskim identifikatorjem;
- eliminacija podvajanja istih vsebin;
- uvajanje WORM (angl. Write Once Read Many) lastnosti optičnih medijev na zasnovi magnetnih diskov (vsaka najmanjša sprememba vsebine bi rezultirala s kreiranjem novega objekta);
- omogočanje uporabe politike upravljanja na nivoju objekta (npr. rok hrambe);
- neodvisnost od fizične lokacije objekta in razvoja strojne opreme;
- enostavno upravljanje – ni potrebe po formatiranju datotečnih sistemov, kreiranju volumnov itd.

Nov pristop k naslavljanju elektronskih objektov je razvila korporacija EMC in ga leta 2002 ponudila na tržišče v produktu Centera (slika 36).

Slika 36: Arhiviranje dokumentov s sistemom Centera

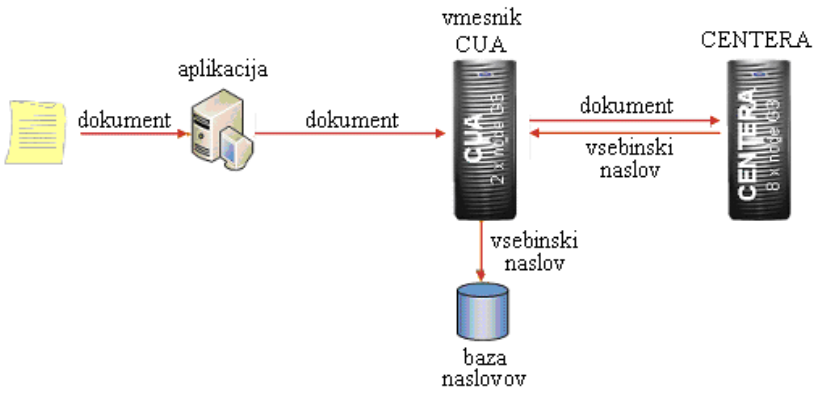


Vir: EMC Corporation, 2004

Centera je objektno orientiran pomnilni sistem (diskovno polje, programska oprema,…) za hrambo velike količine fiksne, to je nespremenljive vsebine. Vsak objekt dobi 128 bitni vsebinski naslov, ki ga izračuna z zgoščevalnim algoritmom MD-5. Pomnilni sistem uporablja RAIN (angl. Redundant Array of Independent Nodes) implementacijo, ki omogoča masovni spomin reda petabajt ter enostavno razširjanje kapacitet z dodajanjem novih modulov. Vse bistvene komponente sistema so podvojene.

Aplikacije, ki so namensko prilagojene, lahko do sistema dostopajo po protokolu TCP/IP (vrata 3682) preko odprtega aplikacijskega vmesnika API (Application Program Interface), ki omogoča povezovanje z različnimi platformami. Mogoča je tudi dodatna implementacija posebnega vmesnika CUA (angl. Centera Universal Access), ki vsebinsko naslovljene objekte uporabniku prikaže na način mrežnega datotečnega sistema.

Slika 37: Arhiviranje dokumentov preko vmesnika CUA



Vir: EMC Corporation, 2004

Pretvorba poteka tako, da

- aplikacija pošlje zahtevo po branju datoteke;
- vmesni sistem v bazi poišče vsebinski naslov iskanega objekta;
- vmesni sistem pošlje zahtevo po objektu v arhivski sistem;
- arhivski sistem vrne iskani objekt;
- vmesni sistem vrne aplikaciji datoteko na mrežnem pogonu.

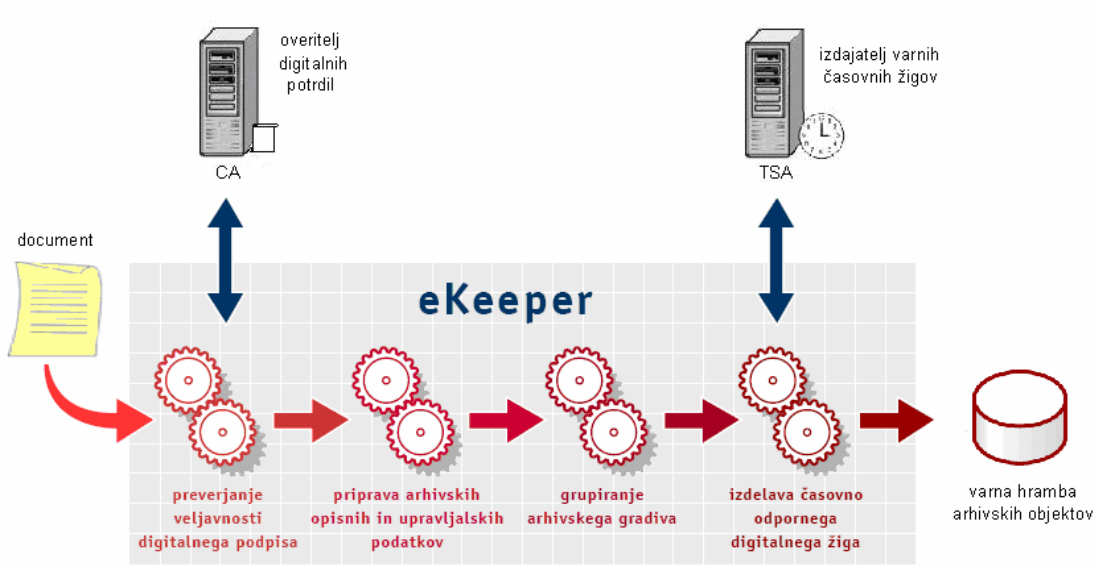
Leta 2004 so bili na tržišče lansirani tudi drugi produkti, ki temeljijo na vsebinskem naslavljanju. Združba Hewlett Packard (HP) je ponudila produkt RISS (angl. Reference Information Storage System) za arhiviranje elektronske pošte in drugih vsebin. Produkt podpira različne poštne aplikacije (npr. Microsoft Exchange, IBM Lotus, SendMail idr.) s katerimi komunicira preko standardnih sporočilnih protokolov. Mrežna arhitektura je osnovana z RAIN implementacijo, ki obsega vhodno-izhodni in zaledni del mreže. Celice vhodno-izhodnega dela prejetemu objektu dodelijo prstni odtis, ki ga izračunajo z algoritmom SHA-1, časovni žig in druge potrebne elemente. Celice zalednega dela objekt indeksirajo, stisnejo in shranijo.

Korporacija Archivas Inc. je leta 2004 na tržišče lansirala produkt ArC (angl. Archives Cluster). Gre za objektno orientiran sistem, ki objekt obravnava kot datoteko, sestavljeno iz vsebine in pripadajočih metapodatkov v XML obliki. Ko sistem ArC prejme objekt mu dodeli identifikacijo ID, ki jo izračuna z MD-5 ali SHA-1 algoritmom. Izračunana identifikacija ne predstavlja naslova objekta, saj se sistem upravlja kot datotečni sistem. ID služi le za ohranjanje integritete. Slabosti so: nizka učinkovitost sistema zaradi dodatnih procesov (npr. verifikacija), visoka cena itd.

6.6.2 Komponenta za zagotavljanje verodostojnosti

Pomembna komponenta, ki skrbi za pravno formalno veljavnost arhiviranega gradiva skozi poljubna časovna obdobja, je rešitev eKeeper, ki sta jo razvila Center za varnostne tehnologije informacijske družbe in elektronsko poslovanje SETCCE (angl. Security Technology Competence Center) in podjetje Infotehna. Gre za programsko rešitev, ki nadgrajuje obstoječe poslovne informacijske sisteme za upravljanje z dokumenti s programskim vmesnikom. Poenostavljen postopek arhiviranja gradiva je prikazan na sliki 38.

Slika 38: Postopek za varno arhiviranje



Vir: http://www.setcce.si/slo/download/eKeeper_brochure_slo.pdf

Sistem sloni na uporabi infrastrukture javnih ključev, ter na enem mestu združuje vse mehanizme za dolgoročno zaščito gradiva. Skrbi za (http://www.setcce.si/slo/download/eKeeper_brochure_slo.pdf):

- zbiranje komplementarnih podatkov;
- pripravo arhivskih opisnih podatkov;
- časovno evidentiranje;
- časovno žigosanje gradiva.

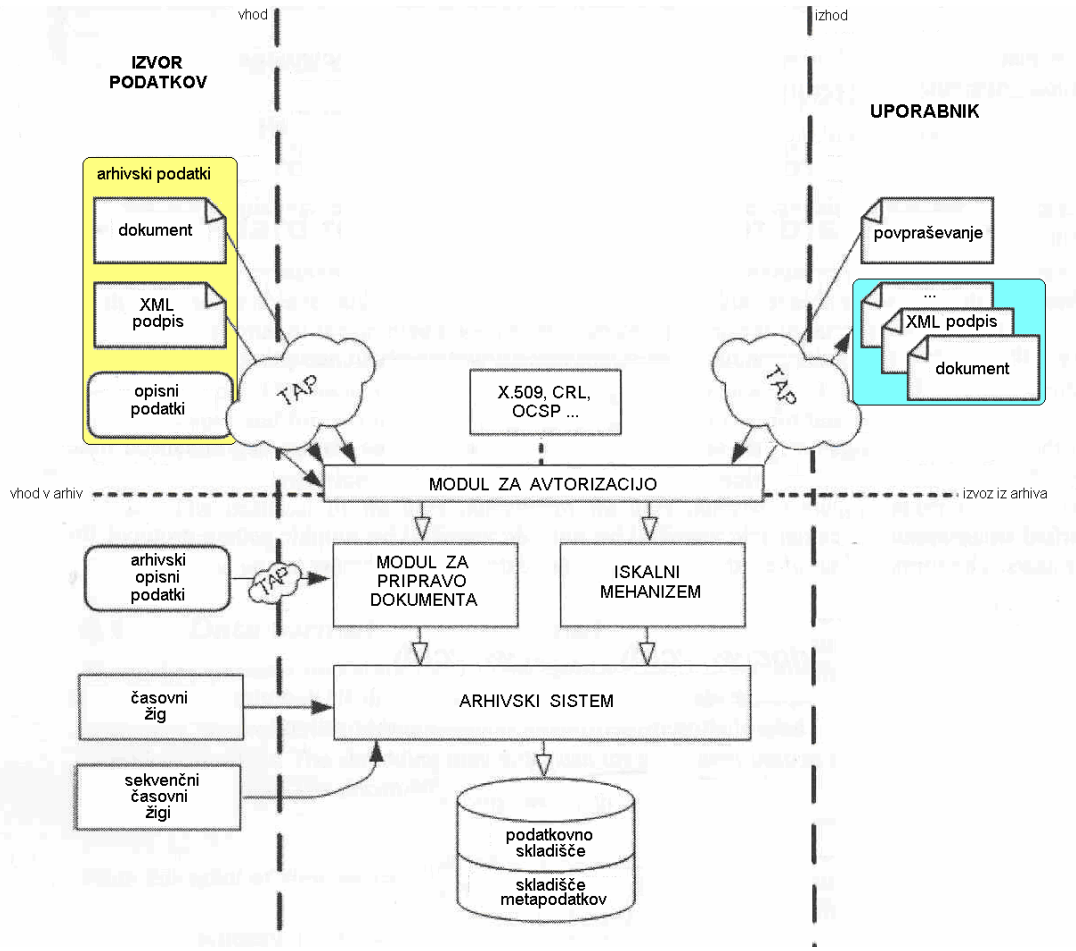
Glavne prednosti rešitve so (http://www.setcce.si/slo/index42d.php):

- skladnost s slovensko zakonodajo in mednarodnimi tehnološkimi standardi;
- možnost arhiviranja poljubnih vrst dokumentov;
- široka možnost za integracijo v poljubne sisteme;
- minimizacija stroškov časovnega žigosanja.

6.6.3 Arhiviranje elektronskega dokumenta

Arhiviranje dokumenta se začne tako, da ustvarjalec arhivu pošlje zahtevo za vzpostavitev komunikacije. Sledi postopek razpoznavanja (avtentikacije) obeh udeležencev in v primeru, da je ta uspešna, ustvarjalec arhivu pošlje primaren dokument, opisne podatke (avtor, čas in kraj nastanka itd.) in morebitni digitalni podpis.

Slika 39: Sprejem elektronskega dokumenta v arhiv



V primeru podpisanega dokumenta, modul za pripravo dokumenta (eKeeper) preveri veljavnost podpisa. Če je podpis veljaven ali če dokument ni digitalno podpisan, se dokument opremi z arhivskimi in evidenčnimi metapodatki. Dokument se časovno žigosa in shrani v pomnilni sistem. O uspešnem oz. neuspešnem arhiviranju dokumenta se obvesti ustvarjalca dokumenta.

Tudi v primeru povpraševanja po arhivskem dokumentu se najprej izvrši razpoznavanje (avtentikacija) obeh strani udeležencev komunikacije. To je še posebej pomembno takrat, kadar lahko do dokumenta dostopajo le določeni uporabniki. Arhiv najprej vrne le odgovor (potrdilo) o sprejetju zahteve, kopijo iskanega dokumenta vrne kasneje.

Za vzdrževanje arhiva in iskanje dokumenta je pomemben pravilen izbor metapodatkov. Ti so lahko tekstovni, numerični, alfanumerični, datumski ali logični. Arhivski sistem ne sme omejevati obsega metapodatkov, ki je v primerih dolgoročne hrambe lahko zelo velik. Minimalen oz. obvezen nabor metapodatkov mora biti določen. Za potrebe posameznih procesov se lahko metapodatke prekonfigurira. Vrednosti se lahko avtomatsko pridobijo (podedujejo) od starševskih elementov v hierarhiji klasifikacijskega načrta.

6.7 Model varnega okolja

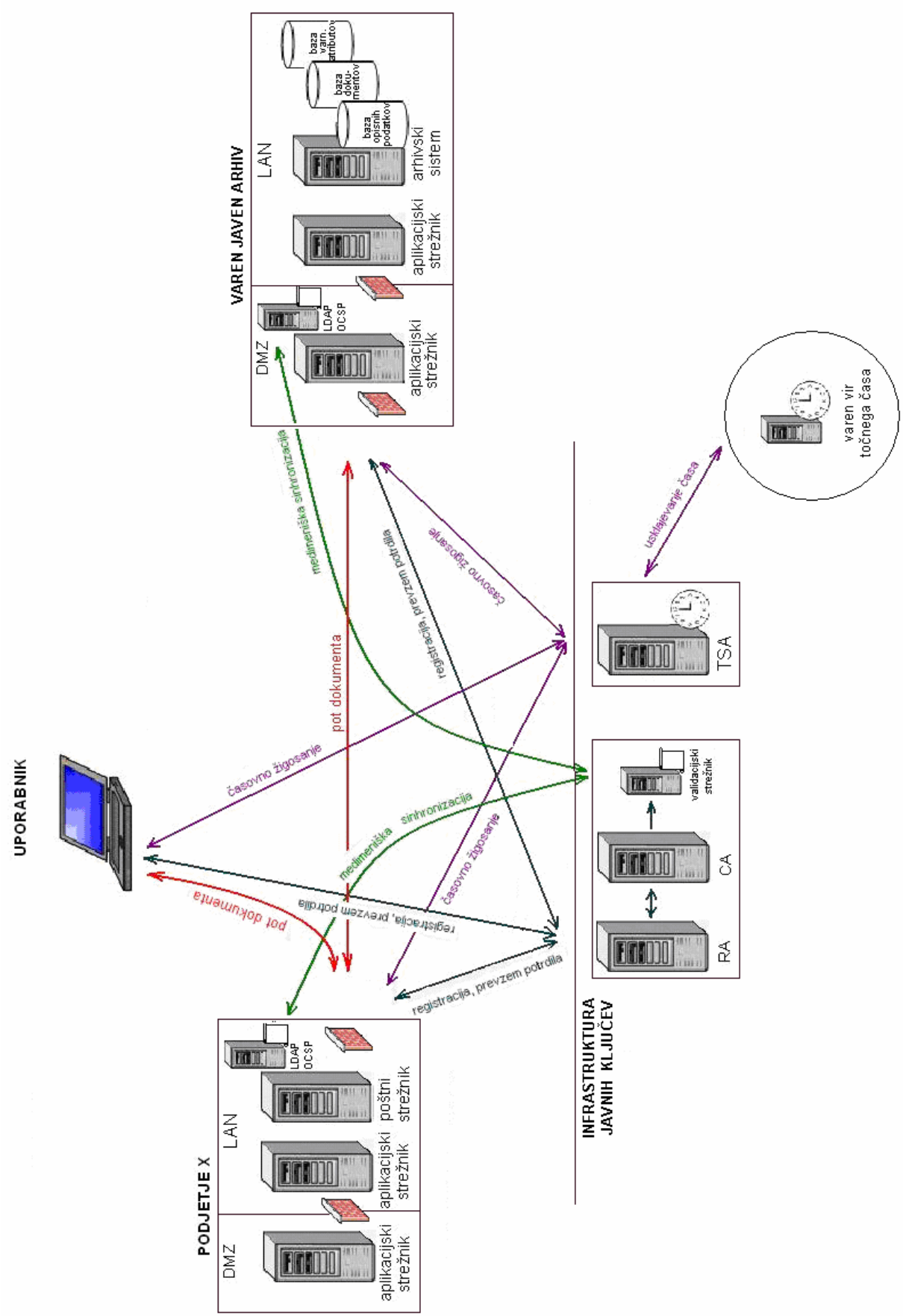
Na podlagi dosedanjih ugotovitev sem sestavila predlog modela za varno okolje elektronskih dokumentov, ki ga predstavljam na sliki 40. Pri izdelavi modela sem izhajala iz naslednjih predpostavk:

- overitelj digitalnih potrdil CA (oz. CA/RA) deluje v skladno s slovensko zakonodajo;
- overitelj časovnih žigov deluje v skladno s slovensko zakonodajo;
- odnosi med entitetami v modelu so urejeni s pogodbami;
- vse komunikacije so varne.

V aktivni fazi (nastanek, obdelava itd.) življenjskega cikla dokumenta je pomembna prilagoditev informacijskega sistema uporabnika in podjetja X, da lahko za varovanje dokumenta koristita storitve infrastrukture javnih ključev. Za dolgoročnejšo hrambo digitalno podpisanega dokumenta je pomembno časovno žigosanje dokumenta v čim krajšem časovnem razmaku z digitalnim podpisom. Imeniški strežnik (LDAP, OCSP), ki se nahaja v DMZ območju podjetja X, je pogrešljiva komponenta. Služi zgolj za večjo neodvisnost preverjanja veljavnosti digitalnih potrdil od glavnega validacijskega strežnika, ki je komponenta infrastrukture javnih ključev. Vključitev lokalnega imeniškega strežnika zahteva zagotovitev dodatne storitve: medimeniško sinhronizacijo.

V pasivni fazi (hramba, arhiviranje) življenjskega cikla je najpomembnejša entiteta varen javen arhiv, ki prav tako koristi storitve infrastrukture javnih ključev. Za sprejem gradiva je namenjen aplikacijski strežnik v DMZ območju, po protivirusnem pregledu se gradivo lahko prenese na aplikacijski strežnik v lokalnem LAN omrežju. Tudi ta lahko implementira svoj lokalni imeniški strežnik, ki ima enako funkcionalnost kot imeniški strežnik podjetja X.

Slika 40: Model varnega okolja



6.8 Formalizacija postopkov

Ob postavitvi varnih informacijskih sistemov, zlasti s storitvami arhiviranja, je potrebna formalizacija vseh postopkov in procesov.

(1) V okviru digitalnih potrdil je potrebno določiti:

- vrsto in namen uporabe digitalnega potrdila;
- odgovornosti lastnika digitalnega potrdila;
- postopek za pridobitev in prevzem digitalnega potrdila;
- postopek preklica potrdila;
- postopek obnovitve potrdila po preteku njegove življenjske dobe;
- pravila za hrambo zasebnega ključa in potrdila;
- postopek sinhronizacije lokalnega imenika z imenikom na glavnem validacijskem strežniku;
- postopek preverjanja veljavnosti digitalnih potrdil;
- politiko uporabe digitalnih potrdil za posamezne aplikacije.

(2) V okviru poslovnega procesa je potrebno določiti:

- formate dokumentov, ki jih poslovna aplikacija podpira;
- formate digitalnih podpisov, ki jih poslovna aplikacija podpira;
- postopek sprejema dokumentov;
- način evidentiranja dokumentov;
- postopek uvrstitve dokumentov v poslovni proces;
- politiko dostopanja do dokumentov;
- postopek dostopanja do dokumentov;
- politiko varovanja podatkov;
- plan okrevanja v primeru izgube podatkov.

(3) Za potrebe arhiva je potrebno določiti:

- formate dokumentov, ki jih arhiv podpira;
- formate digitalnih podpisov, ki jih arhiv podpira;
- postopek sprejema dokumentov;
- način evidentiranja dokumentov;
- postopke priprave dokumentov za arhiviranje;
- postopke vzdrževanja arhiva (opreme, nosilcev ipd.);
- postopek časovnega žigosanja;
- politiko dostopanja do arhivskih dokumentov;
- postopek dostopanja do arhivskih dokumentov;
- politiko varovanja podatkov;
- plan okrevanja v primeru izgube podatkov.

6.9 Vrste nadzora v modelu varnega okolja

Kvaliteten sistem si težko predstavljamo brez učinkovitega nadzora. Nadzor mora biti reden in vsestranski. Predvideti ga je potrebno že v fazi načrtovanja sistema. Celoten nadzor lahko razdelimo v več delnih nadzorov:

- nadzor nad dostopom;
- kontrolne sledi;
- nadzor nad napakami.

a) Nadzor nad dostopom

Varnost elektronskih dokumentov lahko vključuje selektivni dostop in nadzor nad dostopom do dokumentov. Informacijski sistemi, skozi katere dokumenti potujejo, morajo omogočati dodeljevanje dostopnih pravic na nivoju skupin dokumentov.

Zahteve:

- dostop do gradiva se omeji na določene vloge za uporabnike oz. uporabniške skupine (posamezen uporabnik je lahko član več skupin);
- uporabi se koncept uporabniškega profila - datoteke, kjer se določi pravice za akcije (branje, brisanje) nad določenimi podatki (gradivom, metapodatki), ki jih uporabnik oz. skupina lahko izvaja;
- kreiranje uporabniškega profila in dodeljevanje pravic lahko izvaja le administrator;
- za najvišji nivo varnosti je za vsako dostopanje do sistema potrebno križno razpoznavanje obeh strani komunikacije;
- za vse akcije v zvezi z dokumentom se beleži kontrolne sledi;
- v primeru, da želi uporabnik dostopati do dokumentov, za katere nima ustreznih pravic, mu je potrebno, v skladu z nivojem varnosti, ponuditi enega izmed naslednjih odgovorov (Arhiv Republike Slovenije, 2005, str. 25):
  - prikazati naslov in metapodatke;
  - prikazati obstoj podatkov (npr. izpis številke dokumenta);
  - ne prikazati nikakršnih informacij o dokumentih ali na kakršenkoli način namigovati na njihov obstoj.

Nadzor nad dostopom ima na različnih delih opisane poti digitalno podpisanega dokumenta (poglavje 6.3) različno vlogo. Na prvem delu poti oz. pred podpisom dokumenta je nadzor nad dostopom pomemben zaradi možnosti spreminjanja dokumenta ali brisanja dokumenta. Po podpisu dokumenta je (ne)spremenljivost dokumenta mogoče preverjat, zato je ta vloga manjša. Zaradi drugačne narave informacijskega sistema (podjetje X, arhivski sistem) se poveča potencialno število uporabnikov, zato je nadzor nad dostopom še vedno potreben. V praksi je dostop do gradiva mogoče nadzorovati s konceptom aplikacijskega profila. Za vsakega uporabnika ali aplikacijo, ki lahko dostopa

do dokumenta ali skupine dokumentov, se kreira t.i. profil, v katerem je zapisano uporabniško ime, geslo za dostop, pravice za izvajanje operacij (branje, pisanje, brisanje…) ipd. Informacije se izvozi v PEA (angl. Pool Entry Authorisation) datoteko, kopija se zapiše tudi na aplikacijski strežnik.

b) Kontrolirane sledi

Kontrolne sledi so opisi dejanj v zvezi s posameznim dokumentom, podatki o uporabnikih, ki so izvajali ta dejanja ter datum in čas dogodka. Skupek kontrolnih sledi tvori zgodovino dokumenta. Kateri parametri se beležijo in koliko časa se te zapise ohranja določa politika upravljanja in/ali zakonodaja.

Zahteve:

- sistem ne sme omogočati spreminjanja ali uničenja kontrolnih sledi;
- kontrolne sledi se beležijo avtomatsko;
- kontrolne sledi naj se ohranja vsaj toliko časa, kolikor časa se hrani elektronski dokument,
- do podatkov v kontrolni sledi je mogoče dostopati na zahtevo;
- sistem naj vsakodnevno izdela poročilo o kršitvah in poskusih kršitev dostopa.

c) Varovanje podatkov in nadzor nad napakami

Varovanje podatkov mora biti zanesljivo, zato se v praksi uporablja večnivojsko varovanje podatkov in nadzor nad napakami. Večina sistemov omogoča avtomatsko iskanje napak, nekateri tudi avtomatsko odpravo najdenih napak. Pomembno je, da nas sistem o najdenih napakah obvešča preko namensko izdelanih poročil.

Varovanja pred izgubo podatkov zaradi okvar se zagotovi na sistemskem nivoju arhiva. Zaščita je zasnovana tako, da sistem periodično preverja morebitno pomanjkljivost shranjenih objektov in (če je mogoče) najdene napake samodejno odpravi. V praksi se na sistemu uporabljata predvsem dva koncepta varovanja pred izgubo podatkov zaradi okvar:

- zrcaljenje vsebine (angl. Content Protection Mirrored);
- parna kontrola (angl. Content Protection Parity).

Zrcaljenje je zanesljivejša metoda varovanja, ki podvoji primarno vsebino in kopijo shrani fizično ločeno od primarnega objekta. Obe lokaciji, primarna in sekundarna, sta priključeni na ločenih napajalnih verigah oz. ločenih UPS (angl. Uninterruptible Power Suplly). Sistem samodejno preverja dostopnost do podatkov in v primeru ugotovljene napake generira nove kopije. Postopek se imenuje regeneracija in se običajno izvaja ob izpadu enega izmed diskov.

Nekoliko hitrejša je metoda parne kontrole, ki košček vsebine razbije na šest delov – fragmentov in izračuna parno kontrolo. Vsak posamezen fragment se zapiše na drug t.i. node. V primeru, da je eden izmed fragmentov poškodovan, ga je mogoče obnoviti s pomočjo parne kontrole.

Za primer izgube podatkov zaradi naravnih nesreč (angl. Desaster Recovery) je potrebno zagotoviti dodatno varovanje z redno izdelavo varnostnih kopij na fizično oddaljeni lokaciji. Pogostost izdelave varnostnih kopij se določi z varnostno politiko. Izdelati je potrebno plan za vzpostavitev prejšnjega stanja sistema (vključno s podatki) iz varnostnih kopij, ki ga lahko vzpostavi le administrator.

6.10 Zaključek poglavja 6

Opisan idejni model za varovanje dokumentov od nastanka do arhiva je integracija komponent, ki vsaka zase izpolnjuje določene zahteve po varnosti. Model je mogoče posplošiti in ga uporabiti tudi v drugačnih scenarijih. Razlika med scenariji se nanaša na prve faza življenjskega cikla dokumenta, ki s tehnološkega vidika ne predstavljajo večjega problema. Najšibkejši člen v procesu je faza hrambe, zato je temu delu potrebno posvečati največ pozornosti skozi celoten življenjski cikel elektronskega dokumenta.

7 SKLEP

Elektronsko poslovanje zahteva ustrezno ravnanje z dokumenti v njihovem celotnem življenjskem ciklu. V primeru upravljanja dokumentov z elementi verodostojnosti je potrebno zagotoviti temelje za primerno varovanje že ob nastanku dokumenta. V kasnejših fazah življenjskega cikla je pomembna uporaba varnih transakcij in še posebej varna hramba oz. arhiviranje dokumentov.

Osnovni cilj varnega ravnanja z dokumenti je zagotavljanje njihove nespremenljivosti in s tem ohranjanje legitimnosti dokumentov. Legitimnost dokumentov lahko dosežemo le znotraj varnega okolja, kjer se prepletajo ustrezna tehnološka infrastruktura, izbira ustreznega medija in pravno-formalna osnova (zakonodaja, politika upravljanja ipd.). Tehnologija, ki zadovoljuje zakonske zahteve (ZEPEP, Uradni list RS, št. 98/2004) po varnosti dokumentov je infrastruktura javnih ključev. Ta sestoji iz verige overiteljev CA, varnostnih mehanizmov in digitalnih potrdil. Cilj vzpostavitve takšne infrastrukture je nedvoumno povezovanje digitalnih potrdil s podpisniki dokumentov. Ključne prednosti, ki jih omogoča uporaba digitalnih potrdil, so:

- šifriranje oz. dešifriranje dokumentov in elektronske pošte,
- digitalno podpisovanje dokumentov in elektronske pošte;
- prepoznavanje uporabnika pri dostopih do aplikacij ali podatkov in pri vzpostavljanju varnih povezav.

Varno okolje v širšem pomenu besede zagotavlja še varno hrambo oz. arhiviranje dokumentov. Arhiviranje je nenadomestljiva družbeno koristna strokovna dejavnost, ki zahteva strokovno ravnanje z vsemi vrstami gradiva, tudi sodobnega, to je elektronskega. Ključen element pri tem je časovni žig, ki prav tako zahteva uporabo digitalnega potrdila. Cilja nadgradnje osnovnega varnega okolja sta:

- ohranjanje vsebine;
- ohranjanje elementov za verifikacijo varnostnih atributov dokumenta.

Kriptografske tehnike za varovanje dokumentov in protokoli za varne transakcije se sicer uporabljajo že več let, vendar razmah elektronskega poslovanja ovirajo problemi trajnejše hrambe elektronskega gradiva. Tehnologija (mediji, metode itd.) ni časovno preizkušena, zakonodaja je pomanjkljiva, primanjkuje tudi standardov. Problematiko je smotrno reševati celovito. Strategija reševanja je zato osredotočena na koncepte in ne na posamezne faze ali produkte. Dosedanje izkušnje kažejo na to, da so ključne funkcije, ki so potrebne za trajnejšo hrambo, uporabo in obstoj dokumentov, naslednje:

- berljivost oz. prikaz vsebine dokumentov (neodvisno od tehnologije);
- zaščita celovitosti dokumenta in veljavnosti pripadajočih varnostnih atributov;
- fizično varovanje dokumentov.

Pomemben dosežek pri zagotavljanju dolgoročne berljivosti in fleksibilnosti elektronskega gradiva, je bil razvoj XML strukture, ki omogoča neodvisnost interpretacije dokumenta od tehnologije. Za pravilno interpretacijo in preverjanje digitalnega podpisa tudi z uporabo novejših tehnologij se trenutno uporablja različica XMLSign. Na podlagi XML sintakse so bili razviti tudi drugi podporni standardi (kot na primer SOAP za komuniciranje med aplikacijami).

Zaradi kompleksne problematike dolgoročnega ohranjanja celovitosti je dokumente potrebno varovati na več nivojih. V okviru stabilnostnega sloja varujemo celovitost dokumenta z ohranjanjem veljavnosti varnostnih atributov. To pomeni, da zagotovimo verodostojno preverjanje digitalnega podpisa in časovnega žiga tudi v času, ko uporabljena digitalna potrdila niso več veljavna. Rešitev, ki skrbi za pridobivanje oz. kreiranje potrebnih podatkov za dolgoročno verifikacijo je eKeeper. Na nivoju fizičnega varovanja celovitosti dokumentov je pomembna uporaba WORM (angl. Write Once Read Many) medijev, ki zagotavljajo samo enkraten zapis in s tem preprečujejo spreminjanje vsebine. Do nedavnega je bila lastnost WORM značilnost optičnih medijev. Nov koncept naslavljanja (vsebinsko naslavljanje) objektov omogoča WORM zapisovanje tudi na magnetne diske. Tako prvi, kot tudi drugi nosilci so izpostavljeni zastarevanju. Za dolgoročno hrambo gradiva je potrebno rutinsko menjavanje medijev še pred iztekom njihove življenjske dobe oz. periodično prepisovanje elektronskega gradiva na nove medije. Fizično varovanje dokumentov obsega še druge ukrepe kot so zrcaljenje vsebine, parna kontrola, izdelava varnostnih kopij itd.

V praksi še ni na voljo celovitih rešitev varnega okolja, zato idejno rešitev sestavlja več povezanih in medsebojno odvisnih sklopov. Za najvišji nivo varnosti je pomembna implementacija zanesljivih oz. preizkušenih metod in produktov, ki lahko vzpostavijo javno vero v dokumente. Izrednega pomena je varno ravnanje z osebnimi potrdili, ki vključuje tudi hrambo zasebnega ključa. Pomembno je tudi dokumentiranje in sledljivost ključnih dejavnosti na celotni poti dokumenta. Model, ki je pedstavljen v poglavju 6, je splošen in je primerna rešitev za varovanje elektronskih dokumentov v različnih podjetjih. Z izdelavo idejnega modela, je dosežen cilj tega magistrskega dela.

Vsa dosedanja tehnologija zagotavlja le časovno omejeno hrambo elektronskih dokumentov. Ta doba se lahko podaljša z izgradnjo javnih varnih arhivov, ki bodo sposobni skrbeti za izvajanje vseh vzdrževalnih akcij, ki podaljšujejo življenjsko dobo dokumentov (npr. periodično časovno žigosanje, prepisovanje vsebin na novejše nosilce ipd.). Za celovito rešitev varnega okolja je v prvi vrsti potrebno zagotoviti ustrezne standarde in zakonsko podlago. Natančno je potrebno definirati postopke in razmerja med posameznimi procesi. Rešitve naj bodo univerzalne in naj nudijo široko uporabnost. Pomembno je, da rešitve minimizirajo možnost zlorabe ali napake človeškega faktorja. Nadaljnje novosti in izboljšave naj bodo naravnane k pridobitvam za uporabnike

Dolgoročna hramba digitalno podpisanih dokumentov in posledično tudi tehnologija digitalnega podpisa sta v fazi razvoja oz. sprememb, zato ni mogoče določiti predvideti vseh potreb ali določiti vseh zahtev. Časovno obdobje hrambe, ki ga dosegajo klasični (papirni) dokumenti, se za elektronske dokumente zdi nedosegljiva. Če pomislimo na tehnološki razvoj v zadnjih desetletjih 20. stoletja (elektronsko poslovanje, poleti v vesolje itd.), postanejo še tako neverjetne stvari verjetne in zato je realno pričakovati, da bodo nastale tudi rešitve in tehnologije za varno hranjenje digitalno podpisanih dokumentov.

8 LITERATURA

1. Center Vlade RS za informatiko: Varnostni vidik aplikacij z uporabo digitalnih potrdil SIGEN-CA in SIGOV-CA. [URL: http://www.si-ca.si/dokumenti/priporo%E8ila-PKI-aplikacije-v1.0.pdf], avgust 2003.
2. Churchhouse Robert F.: Codes and chipers: Julius Caesar, the Enigma and the Internet. Cambridge: Cambridge University Press, 2002. Str. 240.
3. Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (Blue Book ccsds 650.0-B-1). [URL: http://public.ccsds.org/publications/archive/650x0b1.pdf], January 2002.
4. Cryptography, Certificates, and Secure Communications. [URL: http://www.microsoft.com/technet/security/topics/cryptographyetc.mspx], 10.9.2005.
5. Dumortier Jos, Van den Eynde: Electronic Signatures and Trusted Archival Services. K.U. Leuven – ICRI, [URL: http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=], 8.4.2005.
6. Electronic Signatures and Infrastructure. [URL: http://portal.etsi.org/esi/el-sign.asp], 5.8.2005.
7. e-SLOG dokumentacija. [URL: http://www.gzs.si/Nivo3.asp?IDpm=2306], 7.5.2004.
8. European Committee for Standardization. [URL: http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp], 5.8.2005.
9. Graff Jon: Cryptography and E-Commerce. New York: J. Wiley & Sons, 2001. Str. 222.
10. Jerman Blažič Aljoša:Dolgoročno varno arhiviranje poslovnega gradiva. DOK_SIS 2005, Kranjska gora. Str. II/1-13.
11. Jerman Blažič Aljoša: Informacijska varnost. Monitor, Ljubljana, junij 2004. Str. 60 – 68.
12. Jerman Blažič Aleksej: Varnost in XML.Monitor, Ljubljana, maj 2002. Str. 36 – 40.
13. Jerman Blažič Borka, et al.: Elektronsko poslovanje na internetu. Ljubljana, Gospodarski vestnik, 2001. 206 str.
14. Jurišič Aleksander, Tonejc Jernej: Pametne kartice in varnost. Monitor, Ljubljana, junij 2001. Str. 66 – 75.
15. Jurišič Aleksander, Tonejc Jernej: Zasebno življenje javnih ključev. Monitor, Ljubljana, julij – avgust 2001. Str. 44 – 51.
16. Kolar Robert: Varnost v IP VPN omrežjih z uporabo tehnologije Ipsec. [URL: http://www.ltfe.org/pdf/Varnost_IPsec.pdf], 8.4.2005.
17. Kroflič Jernej, Jerman Blažič Aljoša: Varno arhiviranje elektronskih zapisov in storitve elektronskih notariatov [URL: http://www.infotehna.si/Datoteke/SLO/pdf/clanek/varno%20arhiviranje.pdf], 29.8.2006.
18. Lah Pavla: Uporaba kriptografije v internetu. [URL: http://www.sigov.si/tecaj/kripto/],

15.12.2004.
19. Lioy Antonio: e-documents. [URL: http://www.setcce.org/natows/slides/E_doc.pdf], 27.8.2005.
20. Lupovici Catherine, Masanes Julien: Metadata for long term-preservation, [URL: http://www.kb.nl/coop/nedlib/results/D4.2/D4.2.htm], July 2000.
21. Makarovič Boštjan, et al.: Internet in pravo. Ljubljana, Založba Pasadena, 2001. 220 str.
22. Mao Wanbo: Modern Cryptography: theory and practice. Upper Saddle River: Prentice Hall PTR, 2004. 707 str.
23. Model zahtev za upravljanje elektronskih dokumentov. Ljubljana, Arhiv Republike Slovenije, 2005. 96 str.
24. Novak Miroslav: Arhivska strokovna izhodišča vzpostavitve slovenskega javnega e-arhiva, DOK_SIS 2004, Kranjska gora. Str IV/1-15.
25. Overitelj digitalnih potrdil. [URL: http://www.gov.si/ca/index.htm], 10.7.2005.
26. Pavliha Marko in Jerman Blažič dr. Borka s soavtorji: Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. Ljubljana: GV založba, 2002. 222 str.
27. Perenič Gorazd: Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje z Uvodnimi pojasnili. Ljubljana: Multigraf d.o.o., 2001. 85 str.
28. Posvet INDO 2003 (zbornik referatov). Portorož, 22. – 24. september 2003.
29. Posvet INDO 2004 (zbornik referatov). Portorož, 13. – 15. september 2004. 500 str.
30. Posvetovanje DOK_SIS 2001 (zbornik referatov). Portorož, 23. – 25.maj 2001.
31. Posvetovanje DOK_SIS 2002 (zbornik referatov). Portorož, 22. – 24.maj 2002.
32. Posvetovanje DOK_SIS 2003 (zbornik referatov). Portorož, 21. – 23.maj 2003.
33. Posvetovanje DOK_SIS 2004 (zbornik referatov). Portorož, 26. – 28.maj 2004.
34. Posvetovanje DOK_SIS 2005 (zbornik referatov). Portorož, 14.-16.september 2005.
35. Setcce: eKeeper - Varen elektronski arhiv. [URL: http://www.setcce.si/slo/download/eKeeper_brochure_slo.pdf], 12.1.2006.
36. Setcce: eKeeper - verodostojen elektronski arhiv. [URL: http://www.setcce.si/slo/index42d.php], 12.1.2006.
37. SOAP, HTTP Binding. [URL: http://www.w3schools.com/soap/soap_httpbinding.asp], 20.1.2005.
38. SSL/TLS Layers. [URL: http://202.41.85.117/~hussam/sslws03.mspx.html#EGAA], 5.2.2005.
39. Sylvester Peter:LTAP. [URL: http://www3.ietf.org/proceedings/05aug/slides/ltans-4/sld4.htm], August 2005.
40. Tanja Logar: Varnost interneta. [URL: http://ecom.fov.uni-mb.si/ecomSLO/Studenti/Predmeti/Prezentacije/Varnost%20interneta.ppt], 10.12.2004.
41. Technology Positioning. [URL: http://www.udo.com/compete/index_right.html], 27.5.2005.
42. The OCLC/RLG Working Group on Preservation Metadata: A Metadata Framework to

Support the Preservation of Digital Objects,
[URL: http://www.oclc.org/research/projects/pmwg/pm_framework.pdf], June 2002. 52 str.
43. Theory of Public Key Infrastructure.
[URL: http://www.isaca.be/Presentations/RT020525_PKITheory.pdf], May 2002.
44. Tomažič Sašo: Varnost v telekomunikacijah in kako jo zagotoviti,
[URL: http://www.lkn.fe.uni-lj.si/lknpub/Clanki/2003/Varnost%20v%20telekomunikacijah.pdf], 2003.
45. Tongish Steve: Archival Storage Trends and Challenges.
[URL: http://www.plasmon.com/downloads/pdf/archivaltrends.pdf], May 2004.
46. Trusted Digital Repositories: Attributes and Responsibilities (An RLG-OCLC Report).
[URL: http://www.rlg.org/longterm/repositories.pdf], May 2002.
47. UNCITRAL Model Low on Electronic Signatures with Guide to Enactment 2001.
[URL: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf], New York, 2002.
48. Varnost v omrežjih.
[URL: http://lt.fe.uni-lj.si/gradiva/kso2/p_varnost_v_omrezjih_ip_v1.1.pdf], 10.12.2004.
49. Zupančič Dušan, Vizjak Jure: Podpora kriptografiji v .NET frameworku.
[URL: http://www.kompas-xnet.si/Portals/0/2106delavnica.PDF], 2004.
50. Žagar Klemen: Implementacija varnostnih mehanizmov pri izmenjavi poslovnih dokumentov. [URL: http://www.microsoft.si/slovenija/7ntk/Predstavitve/293.ppt], maj 2002.
51. Žumer mag. Vladimir, Nose Boris, Gazvoda Tone: Elektronsko arhiviranje poslovne dokumentacije. Ljubljana, GV Izobraževanje, 2004. 36 str.
52. Žumer mag. Vladimir: Arhiviranje zapisov. Ljubljana: GV založba, 2001. 480 str.

9 VIRI

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspect of information society services, in paricular electronic commerce in the Internal Market. Official Journal of the European Communities, L178/1 - L178/16, 17.7.2000.
2. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature. Official Journal of the European Communities, L13/12 - L13/20, 19.1.2000.
3. EESSI Expert Team Final Report: European Electronic Signature Standardisation Initiative. [URL: http://www.ictsb.org/EESSI/Documents/Final-Report.pdf], july 1999.
4. EMC Corporation: Centera API Reference Guide Versio 2.4. February 2005. 318 str.
5. EMC Corporation: Centera Product Guide Versio 2.4. February 2005. 104 str.
6. EMC Corporation: Centera Programmers Guide Versio 2.4. February 2005. 106 str.
7. Interna gradiva Državnega zbora Republike Slovenije.

8. Internet Draft: Evidence Record Syntax (ERS). [URL: http://ltans.edelweb.fr/draft-ietf-ltans-ers-03.txt], October 2005.
9. Internet Draft: Long Term Archive Protocol (LTAP). [URL: http://www.ietf.org/internet-drafts/draft-ietf-ltans-ltap-01.txt], February 2006.
10. iSlovar. [URL: http://www.islovar.org/iskanje_enostavno.asp], 15.12.2004.
11. Pahor David: Leksikon računalništva in informatike. Ljubljana, Založba Pasadena. 2002, 786 str.
12. NIST: Decret No. 040602169-5002-02. [URL: http://cryptome.org/nist051905.txt], 20 May 2005.
13. Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji, Uradni list RS, št. 99/2001.
14. Reference Model for an Open Archival Information System (OAIS). CCSDS 650.0-B-1, Consultative Committee for Space Data Systems, January 2002.
15. Register overiteljev v Republiki Sloveniji. [URL: http://mid.gov.si/mid/mid.nsf/V/K581418FEF1C225D7C1256E060030BDF5/$file/Register_Overiteljev.html], 9.9.2004.
16. Trusted Archival Services. Phase #3, Final Report, European Electronic Signature Standardization Initiative, August 2000.
17. Trusted Digital Repositories:Attributes and Responsibilities, An RLG-OCLC Report. [URL: http://www.rlg.org/legacy/longterm/repositories.pdf], may 2002.
18. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Uradni list RS, št. 77/2000, 2/2001.
19. Wikipedia - The Free Encyclopedia [URL: http://en.wikipedia.org/wiki/Main_Page], 15.12.2004.
20. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), Uradni list RS, št. 57/2000.
21. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB), Uradni list RS, št. 98/2004.
22. Zakon o spremembah Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP-A), Uradni list RS, št. 25/2004.

PRILOGA 1: Slovarček uporabljenih tujih strokovnih izrazov in kratic

Application Programming Interface	API	programski aplikacijski vmesnik
Certificate Authority	CA	Overitelj -agencija za overjanje javnih ključev
Certificate Revocation List	CRL	Seznam preklicanih potrdil
Comite European de Normalisation	CEN	Evropski komite za standardizacijo
Content Addressing		vsebinsko naslavljanje objektov
Cryptographic Message Authentication Code	MAC	koda za overitev sporočila
Data Validation and Certification Server Protocols	DVCS	Protokol za preverjanje podatkov in potrdil
Data Validation Certificate	DVC	potrdilo o validaciji podatkov
Digital Signature		Digitalni podpis
Electronic signature	ES	elektronski podpis
European Electronic Signature Standardization Initiative	EESSI	Evropska iniciativa za standardizacijo elektronskega podpisa
European Telecomunications Standards Institute	ETSI	Evropski inštitut za telekomunikacijske standarde
Evidence Record Syntax	ERS	Specifikacija, ki opisuje generiranje, preverjanje in obliko arhivskega časovnega žiga
Extensible Markup Language	XML	razširljiv označevalni jezik
Hardware Security Module	HSM	Strojni varnostni modul
Hash Function		zgostitvena funkcija
Hypertext Transport Protocol Secure	HTTPS	protokol za varno internetno povezavo
Information and Communication Technologies Standards Board	ICTSB	Iniciativa treh evropskih organizacij za standardizacijo (CEN, CENELEC, ETSI)
Information Society Standardization System	ISSS	del evropskega komiteja za standardizacijo, ki se ukvarja s standardizacijo informacijskih tehnologij
Internet Engineering Task Force	IETF	Delovna skupina, ki nadzira tehnične standarde na katerih temelji Internet
Internet Society	ISOC	mednarodna nevladna organizacija za koordinacijo Interneta in njegovih tehnologij ter aplikacij
Lightweight Directory Access Protocol	LDAP	protokol za dostop do imenikov
Long Term Archive Protocol	LTAP	Protokol za dolgoročno arhiviranje

Message Digest		zgoščena vrednost ali prstni odtis
On-line Certificate Status Protocol	OCSP	protokol za sprotno preverjanje statusa digitalnega potrdila
Open Archival Information System	OAIS	Odprt referenčni model za arhiviranje informacijskih objektov
Public Key Infrastrukture	PKI	Infrastruktura javnih ključev
Public-key cryptography standard	PKCS	kriptografski standard
Redundant Array of Independent Disc	RAID	skupina diskov v računalniškem sistemu
Redundant Array of Inexpencive Nodes	RAIN	vrsta arhitekture pomnilnega sistema
Registration Authority	RA	Agencija za registracijo
Request for Comments	RFC	dokument, ki opisuje tehnične vidike Interneta
Secure Multi-Purpose Internet Mail Extensions	S/MIME	standard za varno izmenjavo elektronske pošte
Secure Socket Layer	SSL	protokol za varno povezavo med strežnikom in odjemalcem
Security Technology Competence Center	SETCCE	Center za varnostne tehnologije informacijske družbe in elektronsko poslovanje
Simple Object Acces Protocol	SOAP	Protokol za enostaven dostop do objektov
Time Stamp	TS	Časovni žig
Time Stamp Authority	TSA	Overitelj časovnih žigov
Transport Layer Security	TLS	protokol za varno povezavo med strežnikom in odjemalcem
Trusted Archival Services	TAS	varne arhivske storitve
Ultra Density Optical	UDO	vrsta podatkovnega diska
United Nations Commission on International Trade Low	UNCITRAL	Komisija Združenih narodov za mednarodno in trgovinsko pravo
Virtual Private Network	VPN	navidezno zasebno omrežje
What You See Is What You Sign	WYSIWYS	koncept "kar si videl, si podpisal"
Wireless Transport Layer Security	WTLS	protokol za varno brezžično povezavo med strežnikom in odjemalcem
Write Once Read Many	WORM	Tehnologija, ki zagotavlja enkratno zapisovanje in neomejeno branje

PRILOGA 2: Zakon o elektronskem poslovanju in elektronskem podpisu

(Uradni list RS, št. 98/2004)

Na podlagi 153. člena Poslovnika državnega zbora je Državni zbor Republike Slovenije na seji dne 21. maja 2004 potrdil uradno prečiščeno besedilo Zakona o elektronskem poslovanju in elektronskem podpisu, ki obsega:

- Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Uradni list RS, št. 57/2000 z dne 23.6.2000),

- Zakon o spremembah in dopolnitvah Zakona o organizaciji in delovnem področju ministrstev - ZODPM-C (Uradni list RS, št. 30/01 z dne 26.4.2001) in

- Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu – ZEPEP-A (Uradni list RS, št. 25/04 z dne 19.3.2004).

Številka: 043-03/00-2/3
Ljubljana, dne 21. maja 2004
EPA 1286-III

Predsednik
Državnega zbora
Republike Slovenije
Borut Pahor

ZAKON O ELEKTRONSKEM POSLOVANJU IN ELEKTRONSKEM PODPISU

URADNO PREČIŠČENO BESEDILO (ZEPEP-UPB1)

Prvo poglavje

SPLOŠNE DOLOČBE

1. člen

(1) Ta zakon ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih, če zakon ne določa drugače.

(2) Če ni dogovorjeno drugače, določbe tega zakona, z izjemo določb 4. in 14. člena, ne veljajo v zaprtih sistemih, ki so v celoti urejeni s pogodbami med znanim številom pogodbenih strank.

2. člen

(1) Posamezni izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:
1. podatki v elektronski obliki so podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način;
2. elektronsko sporočilo je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto;
3. 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;
4. varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve:
- da je povezan izključno s podpisnikom;
- da je iz njega mogoče zanesljivo ugotoviti podpisnika;
- da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
- da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi;
5. časovni žig je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času; varni časovni žig pa elektronsko podpisano potrdilo overitelja, ki izpolnjuje pogoje iz prejšnje točke;
6. pošiljatelj elektronskega sporočila je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila;
7. naslovnik elektronskega sporočila je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo;
8. prejemnik elektronskega sporočila je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila;
9. posrednik elektronskega sporočila je oseba, ki za drugo osebo pošlje, prejme, shrani elektronsko sporočilo ali nudi druge storitve v zvezi z elektronskim sporočilom;
10. podpisnik je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis;
11. informacijski sistem je programska, strojna, komunikacijska in druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki;
12. podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
13. sredstvo za elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;
14. sredstvo za varno elektronsko podpisovanje je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena tega zakona;

15. podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;
16. sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;
17. oprema za elektronsko podpisovanje je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov;
18. potrdilo je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto;
19. kvalificirano potrdilo je potrdilo iz prejšnje točke, ki izpolnjuje zahteve iz 28. člena tega zakona in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona;
20. overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi;
21. storitev informacijske družbe je storitev, ki se običajno zagotavlja za plačilo, na daljavo, z elektronskimi sredstvi in na posamezno zahtevo prejemnika storitev pri čemer pomeni:
- na daljavo, da se storitev zagotavlja, ne da bi bili strani sočasno prisotni;
- z elektronskimi sredstvi, da se storitev na začetku pošlje in v namembnem kraju sprejme z elektronsko opremo za obdelavo (vključno z digitalnim stiskanjem) in shranjevanje podatkov in v celoti pošlje, prenese in sprejme po žici, radiu, optičnih sredstvih ali drugih elektromagnetnih sredstvih;
- na posamezno zahtevo prejemnika storitev, da se storitev zagotavlja s prenosom podatkov na posamezno zahtevo.
Storitve informacijske družbe vključujejo zlasti storitve prodaje blaga ali storitev, dostopa do podatkov ali oglaševanja na svetovnem spletu ter storitve dostopa do komunikacijskega omrežja, prenosa podatkov ali shranjevanja prejemnikovih podatkov v komunikacijskem omrežju. Storitve radijske in televizijske radiodifuzije niso storitve informacijske družbe po tem zakonu;
22. ponudnik storitev informacijske družbe je fizična ali pravna oseba, ki ponuja storitve iz prejšnje točke tega člena.

3. člen

Osebe lahko uredijo svoja razmerja pri ustvarjanju, pošiljanju, prejemanju, shranjevanju ali drugi obdelavi elektronskih sporočil drugače, kot je določeno v tem zakonu, če iz posamezne določbe tega zakona ali iz njenega smisla ne izhaja kaj drugega.

4. člen

Podatkom v elektronski obliki se ne sme odreči veljavnosti ali dokazne vrednosti samo zato, ker so v elektronski obliki.

Drugo poglavje

ELEKTRONSKO POSLOVANJE

1. oddelek

Elektronsko sporočilo

5. člen

(1) Velja, da elektronsko sporočilo izvira od pošiljatelja:
- če ga pošlje pošiljatelj sam, ali
- če ga pošlje oseba, ki jo pooblasti pošiljatelj, ali
- če ga pošlje informacijski sistem, ki ga upravlja pošiljatelj sam, ali kdo drug po njegovem nalogu, da deluje samodejno, ali
- če je naslovnik za potrditev izvora sporočila uporabil med prejemnikom in pošiljateljem v ta namen vnaprej dogovorjeno tehnologijo in postopek.

(2) Določba prejšnjega odstavka ne velja za primere:
- če je pošiljatelj obvestil prejemnika, da elektronsko sporočilo ni njegovo in je prejemnik imel čas, da ustrezno ravna, ali
- če je prejemnik vedel ali bi bil moral vedeti, če bi ravnal kot dober gospodar oziroma dober gospodarstvenik, ali če bi uporabil dogovorjeno tehnologijo in postopek, da elektronsko sporočilo ni pošiljateljevo.

6. člen

Prejemnik je upravičen šteti vsako prejeto elektronsko sporočilo kot posamično sporočilo in ravnati v skladu s tem, razen v primeru, če je bilo elektronsko sporočilo podvojeno in je prejemnik to vedel ali bi bil moral vedeti, če bi ravnal kot dober gospodar oziroma dober gospodarstvenik ali če bi uporabil dogovorjeno tehnologijo in postopek.

7. člen

(1) Če je pošiljatelj ob ali pred pošiljanjem elektronskega sporočila ali v samem elektronskem sporočilu zahteval ali se s prejemnikom dogovoril, da se prejem sporočila potrdi, ter navedel, da elektronsko sporočilo pogojuje s potrdilom o prejemu, se šteje, kot da elektronsko sporočilo ni bilo poslano, dokler pošiljatelj ne prejme potrdila o prejemu.

(2) Če pošiljatelj ne navede, da elektronsko sporočilo pogojuje s potrdilom o prejemu in potrdila o prejemu ne prejme v določenem ali dogovorjenem roku ali če ta ni bil določen ali dogovorjen v razumnem roku, lahko pošiljatelj obvesti prejemnika, da ni prejel potrdila o prejemu, in določi razumen rok, v katerem mora prejeti potrdilo o prejemu. Če tudi v tem roku potrdila o prejemu ne prejme po predhodnem obvestilu prejemniku, se šteje elektronsko sporočilo za neposlano.

(3) Če se pošiljatelj s prejemnikom ni dogovoril o obliki potrdila o prejemu elektronskega sporočila, se za potrdilo šteje kakršnakoli samodejna ali druga potrditev prejemnika oziroma kakršnokoli ravnanje prejemnika, ki zadostuje, da pošiljatelj izve ali bi bil lahko izvedel, da je bilo elektronsko sporočilo prejeto.

8. člen

Če pošiljatelj od prejemnika prejme potrdilo o prejemu elektronskega sporočila, se šteje, da je naslovnik prejel to elektronsko sporočilo, ne šteje pa se, da je poslano elektronsko sporočilo enako prejetemu.

9. člen

Če ni drugače dogovorjeno, se šteje, da je elektronsko sporočilo odposlano, ko vstopi v informacijski sistem izven nadzora pošiljatelja ali osebe, ki je elektronsko sporočilo poslala v imenu pošiljatelja in v skladu z njegovo voljo.

10. člen

(1) Če ni drugače dogovorjeno, se šteje za čas prejema elektronskega sporočila tisti čas, ko elektronsko sporočilo vstopi v prejemnikov informacijski sistem.

(2) Če ni drugače dogovorjeno, se ne glede na določbo prejšnjega odstavka šteje za čas prejema elektronskega sporočila, če je prejemnik posebej določil informacijski sistem za prejem elektronskih sporočil, čas, ko elektronsko sporočilo vstopi v ta informacijski sistem, ali če je elektronsko sporočilo poslano drugemu informacijskemu sistemu, čas, ko je prejemnik elektronsko sporočilo prevzel.

(3) Določbe prejšnjega odstavka veljajo tudi, če se informacijski sistem nahaja v drugem kraju, ki se po tem zakonu šteje za kraj prejema elektronskega sporočila.

11. člen

(1) Če ni drugače dogovorjeno, se za kraj, od koder je bilo elektronsko sporočilo poslano, šteje kraj, kjer ima pošiljatelj svoj sedež oziroma stalno prebivališče v času pošiljanja, za kraj prejema elektronskega sporočila pa kraj, kjer ima prejemnik sedež oziroma stalno prebivališče v času prejema.

(2) Če pošiljatelj oziroma prejemnik nima stalnega prebivališča, se za kraj, od koder je bilo elektronsko sporočilo poslano oziroma kjer je bilo prejeto, po prejšnjem odstavku šteje njegovo prebivališče v času pošiljanja oziroma prejema elektronskega sporočila.

2. oddelek

Podatki v elektronski obliki

12. člen

(1) Kadar zakon ali drug predpis določa, da se določeni dokumenti, zapisi ali podatki hranijo, se lahko hranijo v elektronski obliki:
- če so podatki, vsebovani v elektronskem dokumentu ali zapisu, dosegljivi in primerni za kasnejšo uporabo in
- če so podatki shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti, ali v kakšni drugi obliki, ki verodostojno predstavlja oblikovane, poslane ali prejete podatke in
- če je iz shranjenega elektronskega sporočila mogoče ugotoviti, od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema in
- če uporabljena tehnologija in postopki v zadostni meri onemogočajo spremembo ali izbris podatkov, ki ju ne bi bilo mogoče enostavno ugotoviti, oziroma obstaja zanesljivo jamstvo glede nespremenljivosti sporočila.

(2) Obveznost hrambe dokumentov, zapisov ali podatkov iz prejšnjega odstavka se ne nanaša na podatke, katerih edini namen je omogočiti, da bo elektronsko sporočilo poslano ali prejeto (komunikacijski podatki).

(3) Kadar zakon ali drug predpis določa, da se določeni podatki predložijo ali shranijo v izvirni obliki, se šteje, da je elektronska oblika sporočila ustrezna, če ustreza pogojem iz prvega odstavka tega člena.

(4) Določbe tega člena ne veljajo za podatke, za katere ta zakon določa strožje ali posebne pogoje hrambe.

13. člen

(1) Kadar zakon ali drug predpis določa pisno obliko, se šteje, da je elektronska oblika enakovredna pisni obliki, če so podatki v elektronski obliki dosegljivi in primerni za kasnejšo uporabo.
(2) Določbe prejšnjega odstavka ne veljajo za:
1. pravne posle, s katerimi se prenaša lastninska pravica na nepremičnini ali s katerimi se ustanavlja druga stvarna pravica na nepremičnini;
2. oporočne posle;
3. pogodbe o urejanju premoženjskih razmerij med zakoncema;
4. pogodbe o razpolaganju s premoženjem oseb, ki jim je odvzeta poslovna sposobnost;
5. pogodbe o izročitvi in razdelitvi premoženja za življenja;
6. pogodbe o dosmrtnem preživljanju in sporazume o odpovedi neuvedenemu dedovanju;
7. darilne obljube in darilne pogodbe za primer smrti;
8. kupne pogodbe s pridržkom lastninske pravice;
9. druge pravne posle, za katere zakon določa, da morajo biti sklenjeni v obliki notarskega zapisa.

3. oddelek

Odgovornost ponudnikov storitev informacijske družbe

13.a člen

(1) Za opravljanje storitev informacijske družbe ni potrebno posebno dovoljenje.

(2) Ponudniki storitev informacijske družbe so odgovorni za podatke, ki jih posredujejo ali shranjujejo v skladu z določbami tega oddelka, če predpisi, ki urejajo njihovo odgovornost na področju davkov, varstva osebnih podatkov, varstva konkurence, odvetništva in notariata ter iger na srečo, ne določajo drugače.

(3) Od ponudnikov storitev informacijske družbe ni dovoljeno zahtevati splošnega spremljanja ali zavarovanja podatkov v elektronski obliki, ki jih posredujejo ali shranjujejo ali jim naložiti ukrepov, ki bi jih obvezali k aktivnemu poizvedovanju o dejstvih ali okoliščinah, ki kažejo na nezakonitost posamezne dejavnosti ali podatkov.

(4) Ponudniki storitev informacijske družbe iz tega oddelka so pri zagotavljanju varnosti delovanja svojih informacijskih sistemov in posredovanja podatkov v elektronski obliki dolžni ravnati s skrbnostjo dobrega strokovnjaka.

(5) Vlada Republike Slovenije na predlog ministra, pristojnega za informacijsko družbo, določi izvajalca nalog za zagotavljanje varnosti delovanja informacijskih sistemov in posredovanje podatkov v elektronski obliki (v nadaljnjem besedilu: izvajalec nalog). Ponudniki storitev informacijske družbe so dolžni izvajalca nalog obveščati o dejavnostih in podatkih, ki ogrožajo varnost delovanja informacijskih sistemov in z njim sodelovati. Izvajalec nalog zbira informacije o dejavnostih in podatkih, ki ogrožajo varnost delovanja informacijskih sistemov in podatkov v elektronski obliki, obvešča javnost, sodeluje z organi za zagotavljanje varnosti delovanja informacijskih sistemov in posredovanja podatkov v elektronski obliki drugih držav, opozarja na ogrožanje varnosti in predlaga rešitve za njihovo odpravo. Način izvajanja nalog podrobneje določi Vlada Republike Slovenije v aktu o določitvi izvajalca nalog.

13.b člen

(1) Kadar je del storitve informacijske družbe prenos podatkov v elektronski obliki v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve ali zagotavljanje dostopa do komunikacijskega omrežja, ponudnik storitve ni odgovoren za posredovane podatke, pod pogojem, da:
- ne sproži prenosa podatkov;
- ne izbere naslovnika posredovanih podatkov in
- ne izbere ali spremeni vsebine posredovanih podatkov.

(2) Prenos in zagotavljanje dostopa iz prejšnjega odstavka vključujeta samodejno, vmesno in prehodno shranjevanje posredovanih podatkov v elektronski obliki, če je to namenjeno izključno njihovem prenosu v komunikacijskem omrežju in če se podatki ne shranjujejo dlje, kot je to običajno potrebno za njihov prenos.

13.c člen

Kadar je del storitve informacijske družbe prenos podatkov v elektronski obliki v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve, ponudnik storitve ni odgovoren za samodejno, vmesno in začasno shranjevanje teh podatkov, če je to namenjeno izključno bolj učinkovitemu prenosu podatkov drugim prejemnikom storitve na njihovo zahtevo, pod pogojem, da:
- ne spremeni vsebine podatkov;
- ravna v skladu s pogoji za dostop do podatkov;
- ravna v skladu s pogoji o sprotnem dopolnjevanju podatkov, določenimi v splošno priznanih in uporabljenih industrijskih standardih;
- njegovo ravnanje ne nasprotuje zakoniti uporabi tehnologij za pridobivanje informacij o rabi podatkov, ki je določena v splošno priznanih in uporabljenih industrijskih standardih in
- brez odlašanja odstrani ali onemogoči dostop do podatkov, ki jih je hranil, takoj ko je obveščen o tem, da je bil prvotni vir teh podatkov odstranjen iz omrežja, ali da je bil dostop do njega onemogočen, ali da je sodišče ali upravni organ odredil odstranitev ali mu onemogočil dostop.

13.d člen

(1) Kadar je del storitve informacijske družbe shranjevanje podatkov, ki jih zagotovi prejemnik storitve, ponudnik storitve ni odgovoren za podatke, ki jih je shranil na zahtevo prejemnika storitve, pod pogojem, da:
1. ne ve, da gre za protipravno dejavnost ali podatke in mu glede odškodninskih zahtevkov niso znana dejstva ali okoliščine iz katerih je razvidna protipravnost ali
2. takoj ko izve za protipravnost ali se je zaveda, nemudoma odstrani ali onemogoči dostop do teh podatkov.

(2) Določbe prejšnjega odstavka se ne uporabljajo v primerih, ko prejemnik storitve ravna v okviru pooblastil ali pod nadzorom ponudnika storitev.

Tretje poglavje

ELEKTRONSKI PODPIS

1. oddelek

Splošne določbe

14. člen

Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.

15. člen

Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.

16. člen

Osebe, ki hranijo dokumente, ki so elektronsko podpisani z uporabo podatkov in sredstev za podpisovanje, morajo hraniti komplementarne podatke in sredstva za preverjanje elektronskega podpisa enako dolgo, kot se hranijo dokumenti.

17. člen

Uporaba podatkov za elektronsko podpisovanje brez vednosti podpisnika ali imetnika potrdila, ki se nanaša na te podatke, je prepovedana.

2. oddelek

Potrdila in overitelji, ki jih izdajajo

18. člen

(1) Overitelj za opravljanje svoje dejavnosti ne potrebuje posebnega dovoljenja.

(2) Overitelj mora začetek opravljanja dejavnosti prijaviti ministrstvu, pristojnemu za informacijsko družbo (v nadaljnjem besedilu: ministrstvo), najmanj osem dni pred začetkom. Ob začetku opravljanja dejavnosti ali ob spremembi dejavnosti mora overitelj ministrstvo seznaniti s svojimi notranjimi pravili glede elektronskega podpisovanja in overjanja ter s svojimi postopki in infrastrukturo.

(3) Overitelj, ki opravlja storitve varnega elektronskega podpisovanja, mora v svojih notranjih pravilih upoštevati varnostne zahteve, določene s tem zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi.

(4) Overitelj mora izpolnjevati zahteve iz svojih notranjih pravil tako ob začetku kot tudi neprekinjeno ves čas izvajanja dejavnosti.

19. člen

(1) Overitelj mora nemudoma obvestiti ministrstvo o vseh okoliščinah, ki ga ovirajo ali mu onemogočajo izvajanje dejavnosti v skladu z veljavnimi predpisi ali njegovimi notranjimi pravili.

(2) Overitelj mora nemudoma obvestiti ministrstvo o možnem začetku stečaja ali prisilne poravnave.

20. člen

(1) Overitelj mora preklicati potrdilo iz 18. točke 2. člena tega zakona v času njegove veljavnosti v skladu s svojimi notranjimi pravili, ki urejajo preklice potrdil, vendar vedno nemudoma:
- če preklic potrdila zahteva imetnik potrdila ali njegov pooblaščenec, ali
- ko overitelj izve, da je imetnik potrdila izgubil poslovno sposobnost, umrl, prenehal obstajati ali da so se spremenile okoliščine, ki bistveno vplivajo na veljavnost potrdila, ali
- če je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov, ali
- če so bili podatki za preverjanje elektronskega podpisa ali informacijski sistem overitelja ogroženi na način, ki vpliva na zanesljivost potrdila, ali
- če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa in je overitelj s tem seznanjen, ali
- če overitelj preneha z delovanjem ali mu je delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj, ali
- če preklic odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

(2) Overitelj mora v svojih notranjih pravilih določiti, kdaj in na kakšen način se obvešča o izdaji oziroma preklicu potrdila.

(3) Ne glede na notranja pravila mora overitelj vedno nemudoma obvestiti imetnika preklicanega potrdila. Podatke o preklicu mora posredovati vsaki osebi, ki jih zahteva, ali jih javno objaviti, če overitelj vodi register preklicanih potrdil.

21. člen

Ministrstvo mora nemudoma zagotoviti preklic potrdil overitelja, če overitelj preneha z delovanjem ali je njegovo delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj, če overitelj potrdila ne prekliče.

22. člen

(1) Imetnik potrdila mora podatke za elektronsko podpisovanje hraniti s skrbnostjo dobrega gospodarja ali dobrega gospodarstvenika in jih uporabljati v skladu z zahtevami tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter preprečiti nepooblaščen dostop do teh podatkov.

(2) Imetnik potrdila mora zahtevati preklic svojega potrdila, če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila izgubljeni ali ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

23. člen

Če potrdilo vsebuje podatke o tretji osebi, ki ni imetnik potrdila, je tudi ta upravičena zahtevati preklic potrdila iz razlogov, določenih v drugem odstavku prejšnjega člena.

24. člen

(1) Preklic potrdila učinkuje med imetnikom potrdila in overiteljem od trenutka preklica. Preklic potrdila učinkuje med tretjimi osebami in overiteljem od trenutka objave ali, če preklic ni javno objavljen, od trenutka, ko tretje osebe zanj zvedo.

(2) V preklicu potrdila mora biti naveden čas preklica.

(3) Preklic vedno velja od trenutka preklica naprej. Preklic za nazaj ni dovoljen.

25. člen

Za časovni žig in storitve, povezane z njim, se smiselno uporabljajo določbe tega zakona, ki urejajo potrdilo, za varen časovni žig in storitve, povezane z njim, pa določbe tega zakona, ki urejajo kvalificirano potrdilo.

26. člen

Overitelj mora voditi dokumentacijo o varnostnih ukrepih v skladu s tem zakonom in predpisi, izdanimi na njegovi podlagi, ter o vseh izdanih in preklicanih potrdilih tako, da bodo podatki vedno dostopni ter njihova verodostojnost in nespremenljivost vedno preverljiva, in sicer najmanj pet let od posameznega dogodka ali dejanja.

27. člen

(1) Overitelj mora pred prenehanjem delovanja o tem nemudoma obvestiti ministrstvo in imetnike od njega izdanih potrdil, ter zagotoviti, da vse njegove pravice in obveznosti glede izdanih potrdil prevzame drug overitelj ali da prekliče veljavna potrdila.

(2) Vso dokumentacijo, ki jo je doslej vodil, mora predati drugemu overitelju, ki bo prevzel vse pravice in obveznosti prejšnjega overitelja glede izdanih potrdil, oziroma ministrstvu, če takega overitelja ni.

3. oddelek

Kvalificirana potrdila in overitelji, ki jih izdajajo

28. člen

(1) Iz kvalificiranega potrdila mora biti ugotovljivo:
- navedba, da gre za kvalificirano potrdilo;
- ime ali firma in država stalnega prebivališča ali sedeža overitelja;
- ime oziroma psevdonim imetnika potrdila z obvezno navedbo, da gre za psevdonim;
- dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo, ki pa ne smejo biti v nasprotju z namenom uporabe psevdonima;
- podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila;
- začetek in konec veljavnosti potrdila;
- identifikacijska oznaka potrdila;
- varen elektronski podpis overitelja, ki je potrdilo izdal;
- morebitne omejitve v zvezi z uporabo potrdila;
- morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja.

(2) Če ni drugače dogovorjeno, potrdilo ne sme vsebovati podatkov, ki jih varuje poseben zakon.

(3) Kvalificirana potrdila, izdana za potrebe osebnih dokumentov, vsebujejo poleg podatkov iz prvega odstavka tega člena tudi osebno identifikacijsko oznako, ki se lahko v ta namen sklicuje ali poveže s Centralnim registrom prebivalstva. Vlada Republike Slovenije podrobneje določi način določanja osebne identifikacijske oznake, vzpostavitev in vodenje registra osebnih identifikacijskih oznak ter pogoje in način sklicevanja ali povezovanja s Centralnim registrom prebivalstva v skladu s predpisi, ki urejajo varstvo osebnih podatkov.

29. člen

Overitelj, ki izdaja kvalificirana potrdila, mora zagotavljati storitve v zvezi z elektronskim podpisovanjem s skrbnostjo dobrega strokovnjaka.

30. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora zagotoviti vodenje registra preklicanih potrdil, ki mora vsebovati zlasti identifikacijsko oznako preklicanega potrdila, da se ga da natančno identificirati. Register ne sme vsebovati podatkov o vzrokih za preklic ali kakršnih koli podatkov, ki niso vsebovani v potrdilu, razen datuma in časa preklica. Register mora biti varno elektronsko podpisan in podpis overjen s kvalificiranim potrdilom z najmanj enako zanesljivostjo kot potrdila, ki se preklicujejo v registru.

(2) Overitelj mora zagotoviti možnost takojšnjega in varnega preklica kvalificiranega potrdila, kot tudi možnost natančne določitve trenutka izdaje in preklica kvalificiranega potrdila.

(3) Overitelj, ki izdaja kvalificirana potrdila in preneha z delovanjem, mora zagotoviti, da drug overitelj, ki izdaja kvalificirana potrdila, vodi preklicana kvalificirana potrdila v svojem registru.

(4) Če overitelj, ki preneha z delovanjem, ne zagotovi hrambe dokumentacije in vodenja preklicanih kvalificiranih potrdil pri drugem overitelju, to zagotovi na njegove stroške ministrstvo.

31. člen

Overitelj, ki izdaja kvalificirana potrdila, mora s pomočjo uradnega osebnega dokumenta s fotografijo za fizične osebe ali z uradno potrjenimi dokumenti za pravne osebe zanesljivo ugotoviti identiteto in druge pomembne lastnosti osebe, ki zahteva potrdilo.

32. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora zaposlovati osebje s potrebnim strokovnim znanjem, izkušnjami in usposobljenostjo na področju opravljanih storitev, še posebej na področju upravljanja ter poznavanja tehnologije elektronskega poslovanja in ustreznih varnostnih postopkov, da zagotovi izpolnjevanje vseh določb tega zakona.

(2) Osebje se mora ravnati po administrativnih in upravljavskih postopkih in predpisih, skladnih z uveljavljenimi pravili stroke.

(3) Vlada Republike Slovenije s podzakonskim predpisom določi vrsto in stopnjo zahtevane strokovne izobrazbe, leta izkušenj ter morebitna dodatna opravljena usposabljanja za izpolnjevanje zahtev iz prvega odstavka tega člena.

33. člen

(1) Overitelj mora uporabljati zanesljive sisteme in opremo, ki so zaščiteni pred spreminjanjem in ki zagotavljajo tehnično in kriptografsko varnost postopkov, v katerih se uporabljajo.

(2) Overitelj mora izvajati varnostne ukrepe zoper ponarejanje potrdil ter v primerih, ko overitelj oblikuje podatke za elektronsko podpisovanje, zagotavljati zaupnost podatkov ves čas postopka oblikovanja takih podatkov.

(3) Overitelj ne sme shranjevati podatkov za elektronsko podpisovanje imetnika potrdila.

(4) Overitelj mora za shranjevanje potrdil uporabljati zanesljive sisteme, ki omogočajo enostavno odkrivanje sprememb ter hkrati omogočajo, da:
1. lahko samo pooblaščene osebe vnašajo nove podatke in spreminjajo obstoječe;
2. je omogočeno preverjanje pristnosti podatkov;
3. so potrdila javno dostopna samo, če je overitelj predhodno dobil dovoljenje imetnika potrdila;
4. uporabnik lahko enostavno opazi kakršnekoli tehnične spremembe, ki bi ogrozile izpolnjevanje teh varnostnih zahtev.

(5) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev iz tega člena.

34. člen

Overitelj, ki izdaja kvalificirana potrdila, mora zavarovati svojo škodno odgovornost. Najnižji znesek zavarovalne vsote predpiše Vlada Republike Slovenije z uredbo.

35. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora shranjevati vse pomembne podatke o kvalificiranih potrdilih, še posebej zaradi dokazovanja overitev v sodnih, upravnih in drugih postopkih, vsaj toliko časa, kot bodo hranjeni podatki, podpisani z elektronskim podpisom, na katerega se nanaša kvalificirano potrdilo, najmanj pa pet let od izdaje potrdila.

(2) Za pomembne podatke o kvalificiranih potrdilih se štejejo zlasti podatki o načinu ugotovitve istovetnosti imetnika potrdila, času in načinu izdaje potrdila, vzroku, času in načinu morebitnega preklica potrdila, roku veljavnosti potrdila ter vseh sporočilih, ki se nanašajo na veljavnost potrdila, izmenjanih med overiteljem in imetnikom.

(3) Podatki iz prvega in drugega odstavka tega člena se lahko shranjujejo v elektronski obliki.

36. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora osebo, ki zahteva potrdilo, pred izdajo potrdila obvestiti o vseh pomembnih okoliščinah uporabe potrdila.

(2) Obvestilo mora vsebovati:
1. podroben povzetek vsebine veljavnih predpisov ter notranjih pravil in drugih pogojev, ki se nanašajo na uporabo potrdila;
2. podatke o morebitnih omejitvah uporabe potrdila;
3. podatke o obstoju prostovoljne akreditacije;
4. podatke o postopkih za reševanje pritožb in mirno razreševanje sporov;
5. podatke o ukrepih imetnika potrdila, potrebnih za varnost elektronskega podpisovanja in preverjanja elektronskih podpisov, ter o ustrezni tehnologiji;
6. opozorilo, da bo morda potrebno elektronsko podpisane podatke ponovno elektronsko podpisati, in sicer preden bo varnost

obstoječega elektronskega podpisa s časom zmanjšana;
7. opozorilo, da mora imetnik kvalificiranega potrdila sam sporočiti spremembe obveznih podatkov kvalificiranega potrdila iz 28. člena tega zakona.

(3) Obvestilo mora biti napisano v lahko razumljivem jeziku ter v pisni obliki.

(4) Ustrezni deli obvestila morajo biti na njihovo zahtevo dostopni tudi tretjim osebam, ki se zanašajo na potrdilo.

4. oddelek

Tehnične zahteve za varno elektronsko podpisovanje

37. člen

(1) Sredstva za varno elektronsko podpisovanje morajo z uporabo ustreznih postopkov in infrastrukture zagotavljati naslednje:
1. podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena;
2. podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa, elektronski podpis pa je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije;
3. podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom.

(2) Sredstvo za varno elektronsko podpisovanje ne sme spremeniti podatkov, ki se podpisujejo, ali preprečiti prikaza podatkov podpisniku pred podpisom.

(3) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev glede sredstev za varno elektronsko podpisovanje iz tega člena.

38. člen

(1) Med postopkom preverjanja varnega elektronskega podpisa mora biti z uporabo ustreznih postopkov in infrastrukture zagotovljeno naslednje:
1. podatki, ki se uporabljajo za preverjanje elektronskega podpisa, morajo biti enaki podatkom, ki so prikazani uporabniku;
2. podpis mora biti zanesljivo preverjen in rezultati preverjanja ter identiteta podpisnika pravilno prikazani uporabniku;
3. uporabnik lahko zanesljivo ugotovi vsebino podpisanih podatkov;
4. pristnost in veljavnost potrdila morata biti preverjeni v času preverjanja podpisa;
5. raba psevdonima mora biti jasno označena;
6. vse spremembe, ki kakorkoli vplivajo na varnost elektronskega podpisa, morajo biti ugotovljene.

(2) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev glede postopkov in infrastrukture iz prejšnjega odstavka.

5. oddelek

Odgovornost overiteljev

39. člen

(1) Overitelj odgovarja vsaki osebi, ki se upravičeno zanaša na kvalificirano potrdilo, ki ga je overitelj izdal, za:
- točnost podatkov v potrdilu v trenutku izdaje potrdila ter da potrdilo vsebuje vse predpisane podatke za kvalificirano potrdilo;
- zagotovilo, 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;
- zagotovilo, da delujejo podatki za elektronsko podpisovanje in podatki za preverjanje elektronskega podpisa komplementarno v primeru, če overitelj oblikuje oboje podatke;
- takojšen preklic potrdila in objavo preklica, če za preklic obstajajo razlogi;
- izpolnjevanje zahtev tega zakona in na njegovi podlagi izdanih podzakonskih predpisov glede varnih elektronskih podpisov in kvalificiranih potrdil.

(2) Overitelj lahko v kvalificiranem potrdilu označi meje uporabnosti ali najvišje transakcijske vrednosti določenega potrdila in ne odgovarja za posledice uporabe potrdila izven tako določenih meja, če so omejitve prepoznavne tretjim osebam.

(3) Overitelj je odgovoren, če ne dokaže, da je škoda nastala brez njegove krivde.

6. oddelek

Nadzor

40. člen

(1) Inšpekcijsko nadzorstvo nad izvajanjem določb tega zakona opravlja ministrstvo.

(2) V okviru inšpekcijskega nadzorstva ministrstvo:
- preverja, ali so zahteve zakona in na njegovi podlagi izdanih podzakonskih predpisov ustrezno prenesene v notranja pravila overiteljev;
- preverja, ali overitelj ves čas izvajanja dejavnosti izpolnjuje zahteve iz tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter svojih notranjih pravil;
- v primeru zagotavljanja kvalificiranih potrdil nadzoruje uporabo ustreznih postopkov in potrebne infrastrukture;
- nadzoruje zakonitost izdajanja, hranjenja in preklica potrdil;

- nadzoruje zakonitost izvajanja drugih storitev overiteljev.

(3) Ministrstvo vodi elektronski javni register overiteljev v Republiki Sloveniji. V register overiteljev se vpišejo overitelji, če izpolnjujejo pogoje iz tega zakona. V register overiteljev se na njihovo zahtevo vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Republiki Sloveniji.

(4) Register overiteljev varno elektronsko podpiše ministrstvo. Podatki za preverjanje kvalificiranega potrdila ministrstva se objavijo na spletnih straneh ministrstva skupaj z registrom overiteljev.

41. člen

(1) Pri opravljanju inšpekcijskega nadzorstva je inšpektor upravičen:
- pregledovati dokumentacijo in akte, ki se nanašajo na poslovanje overiteljev;
- pregledovati prostore, v katerih se opravljajo storitve overjanja, ter informacijsko tehnologijo, infrastrukturo in drugo opremo ter tehnično dokumentacijo overiteljev;
- preverjati ukrepe in postopke overitelja.

(2) Inšpektor ima pravico za največ petnajst dni zaseči dokumentacijo, če je to potrebno za zavarovanje dokazov ali za natančno ugotovitev nepravilnosti. O tem mora izdati potrdilo.

(3) Podatke o potrdilih, osebne podatke in podatke, ki so varovani po posebnem zakonu, s katerimi se inšpektor seznani pri izvajanju inšpekcijskega nadzorstva, je dolžan varovati kot tajne.

(4) Inšpektor z odločbo:
- prepove uporabo neprimernih postopkov in infrastrukture;
- začasno prepove delovanje overitelja, delno ali v celoti;
- prepove delovanje overitelja, če overitelj ne izpolnjuje zahtev tega zakona in na njegovi podlagi izdanih predpisov in če milejši ukrepi niso ali ne bi bili uspešni;
- naloži preklic potrdil, če je verjetno, da so bila potrdila ponarejena.

(5) Zoper odločbo iz prejšnjega odstavka je dovoljena pritožba, o kateri odloči Vlada Republike Slovenije. Pritožba zoper odločbo iz druge alinee prejšnjega odstavka ne zadrži njene izvršitve.

(6) Prepoved delovanja ne vpliva na veljavnost pred tem izdanih potrdil.

7. oddelek

Prostovoljna akreditacija

42. člen

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

(2) V register akreditiranih overiteljev se na njihovo zahtevo vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Republiki Sloveniji.

(3) Overitelji, ki so vpisani v register akreditiranih overiteljev (akreditirani overitelji), lahko poslujejo z navedbo svoje akreditiranosti.

(4) Overitelji, ki so vpisani v register akreditiranih overiteljev, lahko označijo to dejstvo v izdanih potrdilih.

43. člen

(1) Akreditacijski organ vodi javni elektronski register pri njem prostovoljno akreditiranih overiteljev.

(2) Register akreditiranih overiteljev varno elektronsko podpiše akreditacijski organ. Podatki za preverjanje kvalificiranega potrdila akreditacijskega organa se objavijo na spletnih straneh akreditacijskega organa skupaj z registrom akreditiranih overiteljev.

44. člen

(1) Akreditacijski organ izvaja nadzor in ukrepe glede akreditiranih overiteljev.

(2) Akreditacijski organ:
- izdaja splošna priporočila za delovanje overiteljev ter priporočila in standarde za delovanje akreditiranih overiteljev v skladu z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi;
- preverja, ali so zahteve zakona in na njegovi podlagi izdanih podzakonskih predpisov ustrezno prenesene v notranja pravila akreditiranih overiteljev;
- preverja, ali overitelj ves čas izvajanja dejavnosti izpolnjuje zahteve tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter svojih notranjih pravil;
- nadzoruje uporabo ustreznih postopkov in infrastrukture pri akreditiranih overiteljih;
- nadzoruje zakonitost izdajanja, hranjenja in preklica potrdil akreditiranih overiteljev;
- nadzoruje zakonitost izvajanja drugih storitev akreditiranih overiteljev.

(3) Akreditacijski organ lahko priporoči:
- spremembo notranjih pravil akreditiranega overitelja;

- akreditiranemu overitelju prenehanje nadaljnje uporabe neprimernih postopkov in infrastrukture.

(4) Če overitelj ne upošteva priporočil akreditacijskega organa, ga akreditacijski organ z odločbo izbriše iz registra akreditiranih overiteljev.

(5) Zoper odločbo iz prejšnjega odstavka je v petnajstih dneh po prejemu odločbe dovoljena pritožba, o kateri odloči minister, pristojen za informacijsko družbo.

(6) Odločbo o pritožbi je minister dolžen izdati v tridesetih dneh po prejemu pritožbe. Odločba o pritožbi je dokončna.

45. člen

(1) Za opravljanje nalog akreditacijskega organa Vlada Republike Slovenije, na predlog ministra, pristojnega za informacijsko družbo, določi pristojni organ za opravljanje nalog akreditacijskega organa ali za opravljanje teh nalog podeli javno pooblastilo, oziroma koncesijo.

(2) Organ iz prejšnjega odstavka ne sme biti overitelj.

8. oddelek

Veljavnost tujih potrdil

46. člen

(1) Kvalificirana potrdila overitelja s sedežem v Evropski uniji so enakovredna domačim kvalificiranim potrdilom.

(2) Kvalificirana potrdila overiteljev s sedežem v tretjih državah so enakovredna domačim:
1. če overitelj izpolnjuje pogoje iz 29. do 36. člena tega zakona in je prostovoljno akreditiran v Republiki Sloveniji ali eni izmed držav članic Evropske unije;
2. če domači overitelj, ki izpolnjuje pogoje iz 29. do 36. člena tega zakona, jamči za taka potrdila enako, kot bi bila njegova;
3. če tako določa dvostranski ali večstranski sporazum med Republiko Slovenijo in drugimi državami ali mednarodnimi organizacijami;
4. če tako določa dvostranski ali večstranski sporazum med Evropsko unijo in tretjimi državami ali mednarodnimi organizacijami.

(3) Potrdila overiteljev s sedežem v Evropski uniji, ki jih po tem zakonu ni mogoče opredeliti kot kvalificirana, se obravnavajo enako kot domača v skladu z določbami tega zakona.

Četrto poglavje

KAZENSKE DOLOČBE

47. člen

(1) Z globo od 500.000 tolarjev do 5,000.000 tolarjev se za prekršek kaznuje overitelj, če:
1. ne ugotovi zanesljivo identitete ali drugih pomembnih lastnosti osebe, ki zaprosi za kvalificirano potrdilo (31. člen);
2. izda kvalificirano potrdilo, ki ne vsebuje vseh zahtevanih podatkov oziroma vsebuje podatke, ki jih ne bi smelo vsebovati (28. člen);
3. ne prekliče potrdila ali kvalificiranega potrdila v primerih, ko to zahteva zakon ali njegova notranja pravila (20. in 23. člen);
4. v preklicu ne navede časa preklica potrdila ali kvalificiranega potrdila ali če potrdilo ali kvalificirano potrdilo prekliče za nazaj (20. in 24. člen);
5. prosilca za potrdilo ali kvalificirano potrdilo ne obvesti o vseh predpisanih podatkih (36. člen);
6. pred prenehanjem delovanja ne obvesti ministrstva in ne zagotovi, da skrb za vsa veljavna potrdila ali kvalificirana potrdila prevzame drug overitelj ali jih ne prekliče (27. člen);
7. ne preda vse dokumentacije drugemu overitelju oziroma ministrstvu (27. člen);
8. ne obvesti ministrstva o možnem začetku stečaja ali prisilne poravnave ali o drugih okoliščinah, ki mu preprečujejo izpolnjevanje predpisanih zahtev (19. člen);
9. ne vodi predpisane dokumentacije (26. člen);
10. ne omogoči inšpektorju vpogleda ali zasega svoje dokumentacije ali ne posreduje potrebnih informacij in pojasnil (41. člen);
11. ne prijavi začetka opravljanja dejavnosti ali ne predloži notranjih pravil (18. člen);
12. izdaja kvalificirana potrdila in ne vodi ali pomanjkljivo vodi register preklicanih potrdil (30. člen);
13. izdaja kvalificirana potrdila in ne izvaja ustreznih varnostnih ukrepov za preprečitev nepooblaščenega zbiranja ali kopiranja podatkov za elektronsko podpisovanje s svoje strani ali s strani tretjega (33. člen);
14. navkljub prepovedi opravljanja dejavnosti s strani ministrstva dejavnost še naprej opravlja (41. člen);
15. neupravičeno uporablja označbo akreditiranega overitelja (42. člen).

(2) Z globo od 50.000 tolarjev do 100.000 tolarjev se kaznuje za prekršek tudi odgovorna oseba pravne osebe ali samostojnega podjetnika posameznika, ki stori prekršek iz prejšnjega odstavka.

(3) Če je overitelj posameznik, se za prekršek iz prvega odstavka tega člena kaznuje z globo od 100.000 tolarjev do 300.000 tolarjev.

48. člen

Z globo od 50.000 tolarjev do 150.000 tolarjev se kaznuje za prekršek imetnik potrdila oziroma njegova odgovorna oseba, če gre za pravno osebo ali samostojnega podjetnika posameznika, če:
1. ne zahteva preklica potrdila ali kvalificiranega potrdila (22. člen);
2. uporablja podatke za elektronsko podpisovanje v nasprotju z zahtevami tega zakona in na njegovi podlagi izdanih podzakonskih predpisov (22. člen).

49. člen

Z globo od 50.000 tolarjev do 150.000 tolarjev se kaznuje za prekršek posameznik, ki brez vednosti podpisnika ali imetnika potrdila uporabi njegove podatke za elektronsko podpisovanje (17. člen).

Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Uradni list RS, št. 57/2000) vsebuje naslednje prehodne in končne določbe:

Peto poglavje

PREHODNE IN KONČNE DOLOČBE

50. člen

(1) Vlada Republike Slovenije izda podzakonski predpis, s katerim podrobneje uredi:
1. merila za ugotavljanje zanesljivosti in za ugotavljanje izpolnjevanja tehničnih zahtev iz 33., 37. in 38. člena tega zakona;
2. strokovno izobrazbo, znanje in izkušnje iz 32. člena tega zakona;
3. minimalno zavarovalno vsoto, s katero mora razpolagati overitelj za kritje odgovornosti;
4. obliko, objavo in dostopnost notranjih pravil overiteljev;
5. časovno veljavnost kvalificiranih potrdil, rok za ponoven elektronski podpis že podpisanih elektronskih podatkov in postopek v zvezi s tem;
6. področje uporabe, zahteve in dopustna odstopanja pri opravljanju storitev v zvezi z varnimi časovnimi žigi;
7. vrsto in obliko označbe akreditiranega overitelja;
8. tehnične pogoje za elektronsko poslovanje v javni upravi.

(2) Vlada Republike Slovenije izda podzakonske predpise iz prejšnjega odstavka najkasneje v šestdesetih dneh po objavi tega zakona v Uradnem listu Republike Slovenije.

51. člen

Minister, pristojen za informacijsko družbo, lahko natančneje predpiše način izvajanja posameznih določb tega zakona.

52. člen

Do uveljavitve zakona, ki bo uredil pogoje za elektronsko poslovanje pri overjanju podpisa pred notarjem ali drugim pristojnim organom, se za te primere ne uporablja določba 15. člena tega zakona.

53. člen

4. točka drugega odstavka 46. člena tega zakona se začne uporabljati z dnem sprejema Republike Slovenije v članstvo Evropske unije.

54. člen **- upoštevan ZEPEP-A**
(črtan)

55. člen

Ta zakon začne veljati šestdeseti dan po objavi v Uradnem listu Republike Slovenije.

Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu – ZEPEP-A (Uradni list RS, št. 25/04) vsebuje naslednje prehodne in končne določbe:

PREHODNE IN KONČNE DOLOČBE

26. člen

(1) Vlada Republike Slovenije določi organ iz petega odstavka 13.a člena zakona najkasneje v treh mesecih po uveljavitvi tega zakona.

(2) Vlada Republike Slovenije izda predpis iz tretjega odstavka 28. člena zakona najkasneje v enem letu po uveljavitvi tega zakona.

27. člen

(1) Globe, določene s tem zakonom, se do začetka uporabe Zakona o prekrških (Uradni list RS, št. 7/03), v postopku o prekršku izrekajo kot denarne kazni, v razponih, določenih v prvem in drugem odstavku 22. člena, 23. in 24. členu tega zakona.

(2) Za prekrške, določene v tretjem odstavku 22. člena tega zakona, se do začetka uporabe zakona iz prejšnjega odstavka, kaznuje overitelj posameznik z denarno kaznijo od 100.000 do 150.000 tolarjev.

(3) Določbe tega zakona, ki urejajo globe za prekršek, ki ga stori odgovorna oseba samostojnega podjetnika posameznika, se uporabljajo od začetka uporabe Zakona o prekrških (Uradni list RS, št. 7/03).

28. člen

Ta zakon začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.