GOSPODARSKA ZBORNICA SLOVENIJE

IPRI
Inštitut za pravno informatiko

Projekt *e*-SLOG

Elektronsko poslovanje slovenskega gospodarstva

PRAVNA VPRAŠANJA ELEKTRONSKEGA PODPISA, ELEKTRONSKEGA POSLOVANJA IN ELEKTRONSKIH ARHIVOV

v. 1.4 delovna
april 2004

STANJE DOKUMENTA

Namen dokumenta:	Analiza pravnih vprašanj elektronskega podpisa, elektronskega poslovanja in elektronskih arhivov po obstoječi slovenski in evropski zakonodaji
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	*Glej "Vsebina"*
Status:	Delovna
Verzija:	1.4
Datum verzije:	2.april 2004
Avtorji:	Boštjan Berčič, Inštitut za pravno informatiko IPRI
Naslovniki:	Dušan Zupančič (GZS), dusan.zupancic@gzs.si Ariana Grobelnik (GZS), ariana.grobelnik@gzs.si Samo Grčman (GZS), samo.grcman@gzs.si Dr. Aleš Dobnikar (CVI), ales.dobnikar@gov.si Dr. Alenka Žužek (CVI), alenka.zuzek@gov.si Rudi Ponikvar (Hermes Plus), rudi.ponikvar@hermes-plus.si Tine Prislan (Hermes Plus), tine.prislan@hermes-plus.si Roman Puhek (Crea), roman.puhek@crea.si Matej Trampuš (Crea), matej.trampus@crea.si Aljoša Blažič (SETCCE), aljosa@setcce.org Gašper Lavrenčič (SETCCE), gasper@setcce.org Dr. Tomaž Klobučar (SETCCE), tomaz@setcce.org Boštjan Berčič (Inštitut za pravno informatiko), bostjan.bercic@ipri-zavod.si Blaž Kovačič (Inštitut za pravno informatiko), blaz.kovacic@ipri-zavod.si Vesna Ilič (IBM), vesna.Ilic@si.ibm.com Milan Spalevič (IBM), milan.spalevic @si.ibm.com
Zgodovina verzij:	*Glej "Verzija"*

Verzija	**Datum spremembe**	**Opombe**
1.4 delovna	2.4.2004	Zadnje zakonodajne spremembe (novela ZEPEP, vzpostavitev SI-TSA)
1.3 delovna	31. 8. 2003	Izdelava vzorčnih dokumentov (politika e-podpisa, sporazum o e-poslovanju)
1.2 delovna	1.6.2003	
1.1 delovna	1.4.2003	Osnutek dokumenta

VSEBINA

1. UVOD

Elektronski podpis in elektronsko poslovanje je v Sloveniji pravno urejeno od leta 2000, ko je bil sprejet sedanji Zakon o elektronskem poslovanju in elektronskem podpisu. Ta je, skupaj z uredbo, ki je bila sprejeta kasneje, določil pogoje za izdajanje in uporabljanje elektronskih podpisov in potrdil, pravno veljavnost elektronskih dokumentov in elektronskih podpisov, infrastrukturo overiteljev potrdil itd. Zakon se je pri tem skliceval na UNCITRALov vzorčni zakon o elektronskem poslovanju in direktivo EU o elektronskem podpisu. Z razvojem tehnologije in elektronskih storitev pa se v zadnjem času pred regulativo s področja elektronskega poslovanja in elektronskega podpisa pojavljajo novi izzivi, predvsem kako znotraj obstoječe zakonodaje obravnavati vprašanja kot so reševanje e-sporov, obravnavanje računalniških dokazov, trajno elektronsko arhiviranje dokumentov itd.

Zelo pomembno med njimi je trajno elektronsko arhiviranje dokumentov, ki je pravzaprav nadgradnja pravnega priznanja veljavnosti elektronskih dokumentov, saj je dokumente potrebno, potem ko enkrat nastanejo, shranjevati. S stališča prava se zastavlja vprašanje, kakšna oblika hranjenja elektronskih dokumentov bo povzročila zaželene pravne učinke: veljavnost in dokazno vrednost takih dokumentov. V nasprotju s svetom papirnih listin, kjer se taka vprašanja manjkrat pojavljajo, saj je papirne listine težje ponarediti, je elektronski zapis oz. dokument samo niz računalniško berljivih znakov, ki se dajo precej lahko ponarediti. Vprašanje je torej, kakšne tehnične ukrepe mora pravo zapovedati, da bo lahko priznalo dolgotrajno veljavnost določenih elektronskih zapisov (pri tem pa so ti zapisi lahko dokumenti o poslovanju, npr. bilance in letni izkazi, lahko pa so tudi elektronska sporočila oz. pogodbe, računalniško generirani zapisi itd.). Obstoječa zakonodaja (tako kot tudi direktiva in vzorčni zakon, po katerih se zakon zgleduje) teh vprašanj včasih ne rešuje zadosti natančno (ZEPEP omenja arhiviranje elektronskih dokumentov v 12. točki), zato bo potrebno zakon oz. uredbo v bodočnosti v tej smeri dopolniti. Še bolj podrobno pa bo materija elektronskega arhiviranja opredeljena v prihajajočem Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih.

Namen tega dokumenta je osvetliti nekatera pravna vprašanja, ki se pojavljajo v zvezi z elektronskim arhiviranjem dokumentov. Pri tem drugo poglavje (Analiza pravnih virov, ki urejajo elektronski podpis in elektronsko poslovanje) prikaže vire, ki so botrovali nastanku Zakona o elektronskem poslovanju in elektronskem podpisu, poda komparativni pregled implementacije teh virov v državah EU ter selektivni pregled neskladnosti posameznih delov slovenske zakonodaje z zakonom in uredbo o elektronskem poslovanju in elektronskem podpisu.

Tretje in četrto poglavje (Arhiviranje elektronskih dokumentov in Elektronski arhivi kot ponudniki elektronskih storitev) se osredotočata na analizo pravnih vprašanj v zvezi z elektronskimi arhivi. Glede na dejstvo, da v trenutku pisanja tega dokumenta ne obstaja celovita pravna ureditev elektronskega arhiviranja, se analiza nanaša na neformalne pravne vire, kot so komentarji, mnenja, standardi, delovna poročila, ki v tem trenutku nastajajo v evropskem prostoru. Obravnavani so elementi pravne veljavnosti elektronskih arhivov, različne ročnosti shranjevanja elektronskih dokumentov, pogoji za ustanavljanje elektronskih arhivov, odgovornosti elektronskih arhivov za integriteto in zaupnost elektronskih dokumentov itd. Bodoča zakonodaja s tega področja bo morala reševati ta (in druga) odprta vprašanja elektronskega arhiviranja dokumentov.

Peto in šesto poglavje (Sporazum o elektronskem poslovanju in Politike elektronskega podpisa) vsebujeta praktična priporočila za sklepanje sporazumov v zvezi z elektronskim poslovanjem, predvsem sporazum o elektronskem poslovanju, ki natančneje opisuje načine elektronskega poslovanje med pogodbenimi strankami ter tako specificira določene zakonske določbe ter posamezne politike elektronskega podpisa, ki natančneje opredeljujejo pooblastila določenih poslovnih vlog v organizaciji ter predpisuje posebne pogoje za veljavnost posameznih dejanj elektronske komunikacije med strankama.

Sedmo poglavje vsebuje terminološki slovar uporabljenih pojmov.

2. ANALIZA PRAVNIH VIROV, KI UREJAJO ELEKTRONSKI PODPIS IN ELEKTRONSKO POSLOVANJE

2.1. Tuji pravni viri

2.1.1 Direktiva EU o elektronskem podpisu

Direktivo EU o elektronskem poslovanju [15] sta Evropski parlament in Svet EU sprejela 13.12.1999. Direktiva opredeljuje, kaj se šteje za elektronski podpis, varen elektronski podpis, nadalje kaj je potrdilo, kvalificirano potrdilo, kaj so podatki za elektronsko podpisovanje, sredstva in varna sredstva za ustvarjanje elektronskih podpisov, podatki in sredstva za preverjanje elektronskega podpisa, overitelji in infrastruktura overiteljev elektronskih potrdil, prostovoljna akreditacija itd. Direktiva v 15 členih ureja najpomembnejša vprašanja elektronskega podpisa, ki so ga morale članice EU (in pristopnice) v svojih zakonodajah implementirati najkasneje do 19.7.2001. Direktiva določa odnos med navadnim, elektronskim in varnim elektronskim podpisom. Prav tako direktiva ureja odgovornost overiteljev potrdil nasproti tretjim osebam, ki so se zanesle na pravilnost podatkov o nosilcih elektronskih podpisov. Direktiva določa še princip tržnega delovanja overiteljev potrdil, shemo prostovoljne akreditacije overiteljev, mednarodno priznavanje potrdil overiteljev iz drugih držav EU, varstvo osebnih podatkov v zvezi z podatki o nosilcih elektronskih podpisov ter tehnične zahteve, ki jih morajo izpolnjevati kvalificirana potrdila, overitelji kvalificiranih potrdil, varna sredstva za ustvarjanje elektronskih podpisov ter priporočila za varno preverjanje elektronskih podpisov. Direktiva vsebuje določbo, da mora Komisija do 19.7.2003 pripraviti predloge morebitnih sprememb direktive in jih predložiti Evropskemu parlamentu in Svetu EU.

2.1.2 Direktiva EU o elektronskem poslovanju

Direktivo EU o elektronskem poslovanju [16] sta Evropski parlament in Svet EU sprejela 8.6.2000. Direktiva ureja trg elektronskih storitev. Direktiva opredeljuje kaj se šteje za storitve elektronske družbe, ponudnike in odjemalce elektronskih storitev, elektronsko komercialno komunikacija itd. Direktiva podrobneje določa, kako se morajo ponudniki elektronskih storitev na spletu identificirati, na kakšen način lahko komunicirajo s potencialnimi strankami, kako se sklepajo elektronske pogodbe z upoštevanjem varstva potrošnikov, kakšne informacije v zvezi z elektronskimi pogodbami morajo ponudniki elektronskih storitev dati na voljo potrošnikom, kakšnim minimalnim zahtevam morajo ustrezati postopki elektronskega naročila blaga itd. Nadalje direktiva določa odgovornost posrednih ponudnikov elektronskih storitev (telekomunikacijskih ponudnikov, ponudnikov strežniškega prostora itd.), vzpostavitev etičnih kodeksov elektronskega poslovanja, alternativno reševanje sporov, ter sodno varstvo za elektronske spore. Direktiva vsebuje določbo, da mora Komisija do 17.7.2003 pripraviti predloge morebitnih sprememb direktive in jih predložiti Evropskemu parlamentu, Svetu EU ter ekonomskemu in socialnemu odboru.

2.1.3 UNCITRALov vzorčni zakon o elektronskem podpisu (2001)

Vzorčni zakon komisije Komisije Združenih narodov za mednarodno trgovinsko pravo [25], podobno kot direktiva EU o elektronskem podpisu opredeljuje pojme kot so: elektronski podpis, digitalno potrdilo, podatkovno sporočilo, overitelj potrdil, oseba, ki se zanaša na resničnost overiteljevih potrdil. Vzorčni zakon določa enakopravno obravnavanje elektronskega in navadnega podpisa, določa pogoje, ki so potrebni, da je elektronski podpis enak lastnoročnemu, določa obnašanje podpisnika, overitelja in tretje osebe pri kreiranju, uporabi, preklicih in zanašanju na elektronski podpis in overiteljeva potrdila. Vzročni zakon prav tako predpisuje določene tehnične zahteve, ki jih morajo izpolnjevati posamezni deli infrastrukture overjanja elektronskih podpisov ter pogoje za mednarodno priznavanje potrdil overiteljev iz različnih držav.

2.1.4 UNCITRALov vzorčni zakon o elektronskem poslovanju(1996)

Vzorčni zakon Komisije Združenih narodov za mednarodno trgovinsko pravo [24] vsebuje definicije pojmov: podatkovno sporočilo, elektronska izmenjava podatkov, pošiljatelj podatkovnega sporočila, naslovnik podatkovnega sporočila, posrednik podatkovnega sporočila, informacijski sistem. Vzorčni zakon določa enakost pisne in elektronske oblike dokumentov ter enakost elektronskega in navadnega podpisa. Vzorčni zakon določa kdaj se (elektronsko) podatkovno sporočilo lahko šteje za ekvivalent originalu v papirnem svetu, kdaj se podatkovno sporočilo lahko uporabi kot dokaz na sodišču, kako je podatkovno sporočilo potrebno hraniti, da ustreza zahtevam hranjenja dokumentov v papirnem svetu.

Vzorčni zakon nadalje določa, kako se sklepajo pogodbe v elektronski obliki, predvsem kako poteka izmenjava podatkovnih sporočil, na kakšen način se ugotavlja identiteta pošiljatelja podatkovnega sporočila (pripadnost podatkovnih sporočil), kdo lahko, poleg samega pošiljatelja, na za pošiljatelja pravno zavezujoč način pošlje podatkovno sporočilo (zastopniki in elektronski zastopniki), potrditev sprejema sporočil ter določitev kraja in časa odpreme in sprejema podatkovnih sporočil.

2.2. Materiji elektronskega podpisa in elektronskega poslovanja

Tako Komisije Združenih narodov za mednarodno trgovinsko pravo kot Evropska unija sta sprejeli vsak po dve direktivi oz. vzorčna zakona s področja elektronskega podpisa in elektronskega poslovanja. Vzorčni zakon in direktiva o elektronskem podpisu sta naravnana precej tehnično in urejata predvsem infrastrukturo, ki je potrebna za izdajanje, uporabljanje, certificiranje in preklic elektronskih podpisov oz. potrdil ter porazdelitev odgovornosti (glede na dolžnost skrbnega ravnanja) med udeležence elektronskega podpisovanja: podpisnika, overitelja in tretjo osebo, ki ji je elektronski podpis namenjen. Direktiva oz. vzorčni zakon ne govorita o elektronskem poslovanju, saj je to urejeno v drugem paru dokumentov. Elektronsko poslovanje je načelno neodvisno od konkretne tehnološke infrastrukture, saj je infrastruktura javnih ključev samo ena od rešitev (čeprav se najbolj uporablja). Poleg tega je uporaba elektronskega podpisa širša kot samo v elektronskem poslovanju oz. elektronskem sklepanju pogodb. Elektronski podpis (s časovnim žigom) se namreč lahko uporablja povsod, kjer je potrebno ugotavljati avtentičnost, istovetnost in čas nastanka (kakršnihkoli) računalniških zapisov, ne samo sporočil (npr. letni računovodski izkazi, ali pa podpisovanje izvršljivih programskih komponent, ki se naložijo z interneta) ter kadar je potrebno na dolgi rok take zapise shranjevati (npr. podpisovanje izvorne kode, podpisovanje računalniških dokazov itd.).

Pri elektronskem poslovanju, ki je urejeno v drugem paru dokumentov, pa je predvsem potrebno urediti vprašanja elektronskega sklepanja pogodb, ponudbe in sprejema ponudbe v elektronski obliki, kraja in časa nastanka elektronske pogodbe itd. Tu gre predvsem za temeljna vprašanja civilnega prava, ki so običajno zakodirana v civilnih zakonikih (npr. BGB v Nemčiji, CC v Franciji,...), poleg tega pa še za vrsto vprašanj v zvezi z potrošniškim pravom, kadar gre za masovno sklepanje pogodb, kot bo to v primeru ponudnikov elektronskih storitev. Tu bo šlo predvsem za vprašanja, kakšne (minimalne) splošne pogoje poslovanja morajo nuditi ponudniki elektronskih storitev, kako lahko komunicirajo s potrošniki, kakšna je odgovornost posrednikov elektronskih storitev itd., kar ponavadi obravnavajo potrošniški zakoni oz. zakoni namenjeni regulaciji trga.

Različne zakonodaje držav članic EU, ki so navedene v naslednjem oddelku, so zato na različne načine implementirale omenjeno materijo. Najbolj čista rešitev bi bila implementacija (tehnične) materije elektronskega podpisa in infrastrukture overiteljev v svojem zakonu ter implementacija materije elektronskega poslovanja z ustreznimi spremembami v civilnih zakonikih (in drugih zakonih, npr. z upravnega področja). Podobno bi bilo v prihodnosti verjetno najbolj smiselno, da bi bila (pretežno tehnična) materija trajnega arhiviranja elektronskih dokumentov implementirana s spremembami zakona o elektronskem podpisu oz. uredbe, posamezni področni zakoni pa bi bili spremenjeni v smislu, da bi dovoljevali tudi elektronsko hranjenje dokumentov oz. e-arhive.

Skoraj vse države EU so sprejele poseben zakon, ki ureja samo vprašanja elektronskega podpisa in infrastrukture overiteljev, različne pa so po državah ureditve, kako je dosežena izenačitev elektronske in pisne oblike. Slovenija je v tem oziru izjema, ker vsebuje ZEPEP poleg tega tudi določbe o elektronskem poslovanju, ki bi vsebinsko bolj sodile v OZ.

2.3. Enakovrednost pisne in elektronske oblike

Ena od najpomembnejših pravnih posledic zakona o elektronskem poslovanju je izenačitev elektronske in pisne oblike (4., 14. in 15.člen ZEPEP). Ne glede na to, kako je ta izenačitev dosežena (s posebnim zakonom, implicitno ali v posameznih zakonih, ki so dotlej omenjali samo pisno obliko) se v zvezi s tem postavi vrsta pravnih vprašanj, npr. kdaj je možno elektronski obliki pripisati enako vrednost kot pisni, kakšno pravno veljavo ima elektronska obličnost glede na druge obličnosti in katere posle se lahko (oz. ne more) sklepati v elektronski obliki.

Prvo vprašanje v zvezi z implementacijo materije elektronskega podpisa v državah EU je, ali je načelno možno sklepati pogodbe (in druge pravne posle) v elektronski obliki. Večina držav EU ima konsenzualni model sklepanja pravnih poslov, kar pomeni, da je obličnost (ustno, pisno, s pričami) za samo veljavnost posla načelno nepomembna. S tega vidika je elektronska oblika samo še ena od možnih oblik in je *a priori*, kot vse druge, načelno sprejemljiva za sklepanje pravnih poslov. V skladu z direktivo EU, ki zaradi promoviranja elektronskega poslovanja izrecno prepoveduje diskriminiranje elektronske oblike, pa je večina držav članic v svoje zakone o elektronskem podpisu izrecno uvrstilo tudi omenjeno določbo o prepovedi diskriminacije elektronske oblike.

Če je pravne posle možno sklepati tudi v elektronski obliki pa se postavi naslednje vprašanje: kakšno pravno veljavnost ima elektronska oblika v primerjavi z drugimi oblikami, ki jih dopušča zakon, predvsem ustno, pisno in notarsko obliko.

Direktiva EU predpisuje enakost varnega elektronskega podpisa in pisne oblike. Potemtakem lahko sklepamo, da je v sistemih, kjer se za sklepanje pravnih poslov ne zahteva posebne obličnosti, vsaka druga elektronska oblika, ki ni varna, enakovredna obličnosti, ki je manjša od pisne: ustna. Izmenjavanje ponudb po elektronski pošti se bo tako štelo za enakovredno ustni obliki, npr. telefonu itd. Zanimivo je, da je od pisne še močnejša notarska oblika in da ta velja več, kot elektronski podpis.

Kočno se postavlja še vprašanja, kateri posli se lahko sklepajo v kateri obliki in kakšna vrsta elektronskega podpisa je potrebna za posamezen posel. Za večino pravnih poslov oblika ni potrebna, torej so lahko sklenjeni tudi v elektronski obliki, med njimi kupoprodajna pogodba, posojilo itd. Za nekatere posle, kot npr. avtorske pogodbe, se zahteva pisno oblika, za kar bo zadostoval varen elektronski podpis. Za nekatere pravne posle, kot npr. prenos lastninske pravice na nepremičninah, oporočne posle itd. pa zakon ponavadi predpisuje notarsko obliko, kar pomeni, da taki posli sploh ne bodo mogli biti sklenjeni v elektronski obliki.

2.4. Implementacija direktive EU o elektronskem poslovanju v nekaterih državah EU

Države EU se da glede implementacije direktive EU primerjati med seboj na različne načine. V tem poglavju so primerjane glede na način, kako so vpeljale materijo elektronskega podpisa in elektronskega poslovanja v svoj pravni red. Za skoraj vse države velja, da so glede na direktivo sprejele poseben zakon o elektronskem poslovanju. Bolj ali manj pa se razlikujejo po načinu, kako so določile pravno veljavnost elektronske oblike in enakovrednost varnega elektronskega podpisa in pisne oblike. Države, ki so za to reformirale svoje civilne zakonike (in po potrebi tudi druge zakone) so: Nemčija, Francija, Nizozemska. Ostale, ki so to materijo na splošno uredile v zakonu o elektronskem podpisu so: Avstrija, Belgija, Danska,Finska,Grčija,Irska, Italija, Luksemburg, Portugalska, Španija, Švedska. Za podrobnejši pregled implementacije posameznih delov direktive po državah EU glej [9].

2.4.1 Nemčija

Nemčija je implementirala elektronski podpis in infrastrukturo overiteljev v posebnem zakonu [20]. Enakost elektronskega podpisa z lastnoročnim podpisom in enakost elektronske in pisne oblike je implementirala z zakonom o spremembah zakonov [17], ki se v nekaterih primerih izrecno sklicujejo na pisno obliko (obligacijski, procesni zakoni). Taka ureditev bi bila možna tudi za Slovenijo, zanjo bi bilo potrebno izločiti iz ZEPEPA dele, ki se nanašajo na elektronsko poslovanje (ki bi šli v Obligacijski zakonik in druge področne zakone), v smislu enakosti elektronskih in papirnih dokumentov pa bi bilo potrebno reformirati vse zakone, ki se sedaj izrecno sklicujejo samo na pisno obliko (glej v nadaljevanju). Nemški zakon vsebuje tudi določbe o varovanju podatkov, kar ZEPEPu manjka. Nemški Zakon o elektronskem podpisu tudi določa, da je nosilec elektronskega podpisa lahko samo *fizična* oseba, ne pa tudi pravna oseba (glede različnih uporab elektronskega podpisa glej del o politiki elektronskega podpisa).

2.4.2 Avstrija

Avstrija je sprejela poseben zakon o elektronskem podpisu. Ta zakon določa enakost elektronske in pisne oblike nasplošno (drugače kot v Nemčiji, enako kot pri nas). Zakon prav tako ne vsebuje določb o elektronskem poslovanju.

2.4.3 Belgija

Belgija je sprejela zakon o elektronskem podpisu, ki na sistemski način ureja vprašanja elektronskega podpisa in infrastrukture overiteljev. V njem ni določb o enakosti pisne in elektronske oblike, ker se v belgijskem pravnem redu na splošno ne zahteva posebne (npr. pisne) obličnosti za sklepanje pogodb.

2.4.4 Danska

Danska je, podobno kot Belgija, sprejela poseben zakon o elektronskem podpisu, izenačitev elektronske oblike s pisno pa je implicitna.

2.4.5 Finska

Finska je sprejela poseben zakon o elektronskem podpisu, v katerem so tudi določbe o enakosti elektronske in pisne oblike.

2.4.6 Francija

Francija ima podobna ureditev kot v Nemčiji. Zakon o elektronskem podpisu ureja infrastrukturo elektronskega podpisovanja, medtem ko so drugi členi direktive (npr. enakost elektronske in pisne oblike) urejeni v spremenjenem civilnem zakoniku (Code Civil). Francoski zakon ne razlikuje med pravno veljavnostjo elektronskih podpisov fizičnih in pravnih oseb.

2.4.7 Nizozemska

Nizozemska je ustrezno spremenila področne zakone (npr. civilni zakonik) za izenačitev elektronske oblike s pisno. Nizozemska še nima zakona, ki bi sistematično uredil infrastrukturo elektronskega podpisovanja.

2.4.8 Velika Britanija

Velika Britanija je sprejela poseben zakon o infrastrukturi overiteljev, splošno veljavnost elektronske oblike pa je predpisala v posebnem zakonu o elektronskih komunikacijah.

2.5. Slovenska zakonodajo s področja elektronskega podpisa in elektronskega poslovanja

2.5.1 Zakon o elektronskem poslovanju in elektronskem podpisu

Zakon o elektronskem poslovanju in elektronskem podpisu [28] je sprejel Državni zbor Republike Slovenije dne 23. junija 2000. Zakon povzema določbe direktive EU o elektronskem podpisu ter UNCITRALovega vzorčnega zakona o elektronskem poslovanju. ZEPEP opredeljuje pojme kot so: podatki v elektronski obliki, elektronsko sporočilo, navaden in varen elektronski podpis, časovni žig, pošiljatelj, naslovnik, prejemnik in posrednik elektronskega sporočila, podatki in sredstva za elektronsko podpisovanje, podatki in sredstva za preverjanje elektronskega podpisa, kvalificirano in navadno potrdilo itd. Značilno za zakon je, da vsebuje tako materijo elektronskega podpisa kot materijo elektronskega poslovanja. Podobni zakoni v državah EU opredeljujejo samo materijo elektronskega podpisa, medtem ko je elektronsko poslovanje delno opredeljeno bodisi v civilnih zakonikih oz. obligacijskih zakonih bodisi v posebnih zakonih namenjenih varstvu trga, konkurence in potrošnikov.

2.5.2 Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje [22] je sprejela vlada Republike Slovenije. Uredba podrobneje razčlenjuje določena vprašanja, ki jih zakon pušča odprte, npr. podrobnejšo vsebino notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila, podrobnejše tehnične pogoje za elektronsko podpisovanje in preverjanje

varnih elektronskih podpisov, časovno veljavnost kvalificiranih potrdil, uporabo varnih časovnih žigov, pogoje za elektronsko poslovanje v javni upravi itd. Kot taka je uredba bolj tehnična in bolj vezana na konkretno tehnologijo kot zakon, ki se trudi biti bolj abstrakten in tehnološko nevtralen. Glede na to se tudi pričakuje nadaljnje spreminjanje uredbe v prihodnosti, ki bo morala zaobseči nekatera nova vprašanja, kot so dolgoročno arhiviranje dokumentov ipd.

2.5.3 Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji

Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji [19] je sprejela vlada Republike Slovenije. Pravilnik podrobneje ureja postopke prijave overiteljev, njihov vpis v javni register overiteljev v Republiki Sloveniji in vodenje tega registra.

2.6. Nekateri praktični problemi z ZEPEPom in uredbo

ZEPEP je bil napisan po predlogi UNCITRALovih vzorčnih zakonov in direktiv EU in ima zato podobne pomanjkljivosti kot ti dokumenti. Predvsem glede na hitro napredovanje tehnologije ni vedno ažuren (kljub temu da je načelno tehnološko nevtralen, se pravi da ni vezan na konkretno tehnologijo), da pa tudi predlog po katerih je bil napisan niso dokončne se vidi iz dejstva, da se npr. direktive EU periodično revidirajo glede na spremembe v tehnološkem okolju. ZEPEP dovolj dobro ureja materijo elektronskega podpisa in infrastrukturo overiteljev, v praksi pa se pojavljajo problemi pri uresničevanju določenih njegovih določb, npr. pomanjkanje inšpekcijskega nadzorstvo nad izvajanjem zakona, neobstoj overiteljev časovnih žigov itd. Glede na hiter razvoj tehnologije in različnih vrst elektronskih storitev (npr. elektronski arhivi) lahko pričakujemo, da se bosta morala zakon, predvsem pa uredba, v prihodnosti ustrezno novelirati.

V nadaljevanju je podanih nekaj problemov v zvezi z ZEPEPom oz. uredbo, ki se pojavljajo pri praktičnem udejanjanju njunih določb. Za izčrpnejši pregled posameznih določb zakona in morebitnih pomanjkljivosti glej npr. [11].

2.6.1 Sistemski vidik

Na ZEPEP je mogoče očitek nasloviti s pravno sistemskega vidika, saj je v enem zakonskem besedilu urejena materija elektronskega podpisa in elektronskega poslovanja. Čeprav je res, da si pri današnjem stanju tehnike ne predstavljamo sodobnega elektronskega poslovanja brez elektronskega podpisa pa oba pojma nikakor nista identična. Elektronski podpis se poleg elektronskega poslovanja v smislu pravnih dejanj (dajanje in sprejemanje elektronskih ponudb in sklepanja elektronskih pogodb) uporablja tudi npr. pri arhiviranju elektronskih zapisov (ki niso nujno pravni dokumenti, npr. pri arhiviranju izvorne kode, ali pa različnih računalniških dokazov), podpisovanju računalniških komponent, avtentikaciji itd. Elektronsko poslovanje kot oddajanje in sprejemanje elektronskih ponudb pa je pravzaprav običajno poslovanje oz. sklepanje pogodb z razliko, da gre za elektronske dokumente, in kot tako tvori del civilnega prava (pri nas obligacije ureja Obligacijski zakonik). S sistemskega vidika bi bilo zato bolj smiselno določbe 5.-13.člena ZEPEPa uvrstiti v OZ.

2.6.2 Različne uporabe elektronskega podpisa

V 1.odstavku 28. člena je rahla nejasnost v zvezi s kvalificiranimi potrdili, katerih nosilci so lahko tudi strežniki oz. informacijski sistemi. Varen elektronski podpis, ki ga spremlja kvalificirano potrdilo je enakovreden lastnoročnemu podpisu. V zvezi z informacijskimi sistemi oz. strežniki seveda ne moremo govoriti o lastnoročnem podpisu. Na splošno so pravna dejanja računalniških programov (oz. agentov) v pravni teoriji še nejasno opredeljena, prevladuje pa mnenje, da gre za zastopanje, pri čemer je računalniški program zastopnik, zastopana oseba pa je njegov lastnik oz. tisti, ki je zanj odgovoren (glej npr. [10]). V tem primeru bi se lahko štelo, da gre za sklepanje pravnih poslov za lastnika programa. Ker pa bodo strežniki oz. informacijski sistemi elektronski podpis uporabljali veliko bolj pogosto za avtentikacijo kot za samo sklepanje pravnih poslov, se postavlja vprašanje, če ne bi veljalo že v ZEPEPu oz. uredbi opredeliti različne vrste uporabe elektronskega podpisa, od katerih je samo ena namenjena pravnemu zavezovanju (kar je sicer opredeljeno v politiki elektronskega podpisa). S tem bi se izognili tolmačenju, da je vsak elektronski podpis namenjen pravnemu zavezovanju. Druge vrste uporabe elektronskega podpisa, poleg izražanja izjav volje, so npr. še (glej [4]):

- avtentikacija,
- potrditev sprejema dokumenta,
- avtorstvo oz. odgovornost za vsebino dokumenta
- avtorizacija dokumenta,
- pregled dokumenta,
- notarski zapis itd.

2.6.3 Ohranjanje veljavnosti elektronsko podpisanih dokumentov

Težavo predstavlja tudi 33. člen uredbe, ki zahteva da mora, *»kdor hrani elektronsko podpisane podatke, najkasneje en mesec pred iztekom roka, ki ga je za veljavnost podatkov za elektronski podpis določil overitelj v javnem delu notranjih pravil, če tega roka ni, pa z dnem konca veljavnosti kvalificiranega potrdila, zagotoviti ponoven elektronski podpis teh podatkov s strani vseh oseb, ki so podatke elektronsko podpisale prvič, ali s strani notarja ali potrditev teh podatkov z varnim časovnim žigom overitelja.*« Prva izbira, ponoven podpis s strani vseh oseb, ki so dokument podpisale je nepraktična, saj ni nujno, da bodo te osebe kasneje hotele dokument še enkrat podpisati. Tudi podpis s strani notarja zaenkrat ni urejen, saj je Zakon o notariatu še iz leta 1994 in ni bil ažuriran v smislu elektronskega poslovanja. Pri notarju je sicer možno potrditi čas, ko mu je bila predložena kakšna listina, vendar to po zakonu velja le za pisne dokumente (oz. listine). Tako naposled ostane le možnost (varnega) časovnega žigosanja, ki ga opredeljuje novela ZEPEPa [29] in ki je postala možna z vzpostavitvijo agencije za izdajanje varnih časovnih žigov SI-TSA dne 10.11.2003. Pred vzpostavitvijo omenjene agencije je bila možnost ohranjanja veljavnosti elektronsko podpisanih dokumentov precej nepraktična, z vzpostavitvijo agencije pa je odpravljena največja ovira pri vzpostavljanju elektronskih arhivov. Tako kot v preteklosti pa je še vedno možno uporabljati tudi časovno žigosanje pri overiteljih časovnih žigov v državah EU.

2.6.4 Hranjenje podatkov o kvalificiranih potrdilih

S tem je povezan tudi 35. člen zakona, ki nalaga overiteljem dolžnost, da hranijo *»vse pomembne podatke o kvalificiranih potrdilih, …, vsaj toliko časa, kot bodo hranjeni podatki, podpisani z elektronskim podpisom, na katerega se nanaša kvalificirano potrdilo, najmanj pa pet let od izdaje potrdila«.* Pri tem gre za podatke kot npr. identiteta imetnika potrdila ipd. ki enolično določajo imetnika potrdila, kar je možno uporabiti v potencialnih sodnih, upravnih in drugih postopkih (samo potrdilo teh podatkov ponavadi ne vsebuje, pač pa samo ime, včasih tudi samo psevdonim). Najdaljši rok trajanja kvalificiranega potrdila je po 32. členu uredbe 5 let. Po tem času imetnik potrdila to zamenja. Ker mora v istem času po 33. členu uredbe še enkrat podpisati podatke in ker overitelj sedaj hrani novo potrdilo je določba navidezno smiselna. Problematično pa je, če podpisnik elektronske podatke časovno žigosa oz. jih da podpisati pri notarju. Po poteku petih let, ko overitelj ne bo več hranil originalnih potrdil, je zato izključno odgovornost podpisnika, da poleg časovnega žiga na dokumentu hrani tudi originalno potrdilo (ne samo referenco nanj, kajti originalno potrdilo po določenem času ni več dostopno), s katerim bo dokazoval, da je bilo to potrdilo uporabljeno v času podpisovanja dokumenta (hranjenje komplementarnih podatkov in sredstev za preverjanje elektronskega podpisa med drugim zapoveduje 16. člen ZEPEPa). Problem je seveda v tem, da kljub hranjenju teh potrdil, zainteresirana oseba po roku, ko overitelj ne bo več hranil podatkov o potrdilih (in overitelj ne bo mogel vedeti, kot mu to sicer veleva zakon, koliko časa bodo hranjeni kateri od podatkov, ki so bili overjeni z njegovim potrdilom) ne bo več mogel v sodnih in drugih postopkih ugotavljati identitete podpisnika. Zato bi bilo tu bolj smiselno zahtevati permanentno evidenco o teh podatkih.

2.6.5 Register preklicanih potrdil

Glede preklicanih potrdil zakon zahteva obstoj registra preklicanih potrdil za kvalificirana potrdila. Zakon v tem sledi direktivi in ne zahteva takega registra za vsa potrdila (3. odstavke 20. člena). Več avtorjev (glej npr. [11]) upravičeno meni, da bi taka zahteva najbrž morala veljati za vsa potrdila. Postopki preverjanja podpisa namreč potekajo on-line pri čemer je vpogled v register preklicanih potrdil (CRL) ali informacija o veljavnosti določenega potrdila (OCSP) nujen del verifikacije vsakega podpisa. Podobno ti avtorji opozarjajo na nejasnost 30. člena ZEPEPa, ki določa dolžnost vodenja registra preklicanih potrdil za overitelje, ki izdajajo kvalificirana potrdila. Zakon namreč določa, da je potrebno v primeru prenehanja delovanja določenega overitelja zagotoviti nadaljevanje dejavnosti preklica. Če overitelj tega ne stori sam, stori to na njegove stroške ministrstvo. Pri tem se pojavi več vprašanj, kot npr. kaj takrat ko je overitelj v stečaju in ne more več sam kriti stroškov, kaj se zgodi z dolgoročnim vzdrževanjem registra preklicanih potrdil, kar je pomembno pri dokumentih, ki se hranijo na dolgi rok itd.

2.7. Nekateri drugi zakoni z vidika elektronskega poslovanja

V nadaljevanju je podan selektiven pregled druge domače zakonodaje z vidika materije elektronskega poslovanja. Ugotavlja se predvsem, do katere mere je določen zakon ali predpis že skladen z določbami Zakona o elektronskem podpisu in elektronskem poslovanju oz. direktivami EU oz. kako ga bo v prihodnosti verjetno potrebno spremeniti. Glede na število zakonov, podzakonskih aktov in drugih predpisov je podana samo analiza nekaterih najpomembnejših aktov.

2.7.1 Obligacijski zakonik

Če bi sledili tujim zgledom z umestitvijo materije elektronskega poslovanja, bi jo morali zapisati v Obligacijski zakonik [18] Vanj bi bilo potrebno uvrstiti določbe o elektronskem poslovanju, ki se tičejo temeljnih obligacijskih pojmov (elektronska ponudba in sprejem ponudbe, določitvi časa in kraja sklenitev pogodbe, potrebne obličnosti – navaden, varen elektronski podpis).

2.7.2 Zakon o varstvu osebnih podatkov

Zakon o varstvu osebnih podatkov [36] je bil sprejet pred ZEPEPom, tako da se postavlja vprašanje, ali ga je potrebno v kakršnemkoli smislu uskladiti z njim in direktivo EU o elektronskem podpisu. Zakon določa zbiranje, hrambo in posredovanje osebnih podatkov. Glede na občutljivost le teh, bo potrebno v zakonu predpisati stroge oblike ravnanja z osebnimi podatki (hramba v šifrirani obliki, posredovanje v elektronski obliki z obojestransko varno identifikacijo itd.). Zaenkrat komunikacija med upravljalci zbirk osebnih podatkov in njihovimi uporabniki poteka v pisni ali fizični obliki, posredovanje osebnih podatkov in drugih informacij (npr. komu so bile take informacije posredovane) v elektronski obliki pa predstavlja pomembno novost, ki jo bo potrebno zakonsko opredeliti.

2.7.3 Računovodski standardi

Računovodski standardi [21] so bili pred kratkim revidirani in po novem štejejo za veljavne elektronske listine in drugo elektronsko poslovanje. V zvezi z hranjenjem takih elektronskih listin pa se pojavljajo ista vprašanja kot pri dolgotrajnem hranjenju (arhiviranju) kakršnihkoli elektronskih zapisov.

2.7.4 Zakon o dostopu do informacij javnega značaja

Zakon o dostopu do informacij javnega značaja [27] je novejšega datuma in zato vsebuje določbe o elektronskem poslovanju in elektronskem podpisu. Za vložitev zahteve za dostop do informacij javnega značaja v elektronski obliki se zakon sklicuje na ZEPEP, sicer pa je postopek pridobivanja informacij javnega značaja na splošno urejen tudi z določbami Zakona o splošnem upravnem postopku, ki dovoljuje izdajo elektronsko podpisane elektronske odločbe.

2.7.5 Zakon o gospodarskih družbah

Zakon o gospodarskih družbah [30] bo potrebno v prihodnosti reformirati zaradi množice razlogov, taka revizija pa bo prilika tudi za uvajanje določb o elektronskem poslovanju in elektronskem arhiviranju dokumentacije. Zadnja novela zakona sicer uvaja oddajanje letnih izkazov v elektronski obliki, medtem ko se druge oblike elektronskega poslovanja ne obravnavajo. V zvezi s tematiko ZGDja je zanimiva tudi izvedba elektronske knjige sklepov pri enoosebnih družbah z omejeno odgovornostjo. V ostalem pa bodo nadaljnje novele, kjerkoli se zakon sedaj sklicuje na pisne listine (letna poročila, izkaze stanja) morale dodati, kateri od omenjenih dokumentov se lahko izdelajo tudi v elektronski obliki.

2.7.6 Zakon o arhivskem gradivu in arhivih

Zakon o arhivih [26] se na nekaj mestih sklicuje na podatke v elektronski obliki (4.člen, ki določa, da je dokumentarno gradivo, med drugim, digitalne ali analogne oblike zapisov računalniških obdelav skupaj s programsko opremo ter 24. člen, ki določa da se oblika izročitve informacij, ki so shranjene v strojno berljivi obliki, določi na podlagi dogovora med

arhivom in javnopravno osebo), vendar ne predpisuje bolj natančnega ravnanja (sprejemanja, arhiviranja) z njimi. V zvezi z elektronskim gradivom bo potrebno zakon dopolniti z ustreznimi določbami glede elektronskega podpisovanja in časovnega žigosanja dokumentarnega gradiva. To bo uredil novi Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), ki je v trenutku pisanja tega dokumenta v nastajanju.

2.7.7 Kazenski zakonik RS in Zakon o kazenskem postopku

Kazenski zakonik bo potrebno posodobiti v skladu z konvencijo Sveta Evrope o računalniškem kriminalu [14], ki opredeljuje posebna kazniva dejanja v zvezi z računalniki in postopke za njihovo odkrivanje. Med kaznivimi dejanji so tudi dejanja, ki se nanašajo na elektronsko poslovanje, denimo računalniška goljufija (goljufija s pomočjo računalniških sredstev, denimo ukradenih elektronskih podpisov), računalniško ponarejanje (ponarejanje računalniških zapisov).

2.7.8 Zakon o pravdnem postopku, Zakon o izvršilnem postopku, Zakon o nepravdnem postopku, Zakon o upravnem postopku,

Procesne zakone bo potrebno posodobiti v smislu, da bodo omogočali vlaganje in izdajanje vlog in odločb tudi v elektronski obliki. Zakon o pravdnem postopku tega zaenkrat ne predvideva, podobno je z nepravdnim in izvršilnim postopkom. Še najdlje je šel upravni postopek, ki e-poslovanje z državo ureja z Zakonom o splošnem upravnem postopku [35] iz leta 1999, ki sicer dovoljuje, da stranke z državo komunicirajo v elektronski obliki, *»v kolikor obstajajo pri organu tehnične možnosti sprejema takšne vloge«* (63. člen), ne obvezuje pa državnih organov, da morajo zagotoviti e-poslovanje z občani. Zakon v 216. členu določa, da se odločbo, kadar se izda v elektronski obliki, podpiše z elektronskim podpisom. Zakon dovoljuje tudi vročanje po elektronski pošti, pri tem pa se sklicuje na uredbo vlade [23].

3. ARHIVIRANJE ELEKTRONSKIH DOKUMENTOV

3.1. Uvod

Elektronski podpis zagotavlja avtentikacijo podpisnika elektronskega sporočila ter nespremenljivost podpisane vsebine. Kot tak je (varen) elektronski podpis izenačen z lastnoročnim podpisom. Vendar elektronski podpis zaradi svoje tehnološke vsebine (ključi oz. podatki za elektronsko podpisovanje, kot jih imenuje zakon ter programska oprema oz. algoritmi za šifriranje – sredstva za elektronsko podpisovanje) ni tako trajen kot lastnoročni podpis. Elektronski podpis namreč temelji na kriptografskih metodah, ki v določenem časovnem trenutku, glede na stanje tehnike (hitrost računalnikov) zagotavljajo, da v razumnem času z izčrpnim iskanjem ni možno iz šifriranega oz. podpisanega sporočila povrniti izvirnega sporočila. Ta predpostavka je povezana z bitno dolžino ključev in vedno velja glede na obstoječe stanje tehnike, predvsem glede na trenutno hitrost računalnikov ter znane algoritme. Z razvojem hitrejših računalnikov in odkritjem novih algoritmov postaja vedno bolj verjetno oz. gotovo, da se da na določeni točki proces obrniti in pridobiti iz šifriranega sporočila izvirno sporočilo s tem pa tudi ključ za šifriranje oz. podpisovanje. Elektronski podpis tako na določeni točki preneha biti varno sredstvo za podpisovanje. Ta okoliščina je pomembna predvsem pri trajnem shranjevanju – arhiviranju elektronskih sporočil. Medtem ko pri lastnoročnem podpisu ni razlike med delovanjem na kratek in dolgi rok, je pri elektronskem podpisu potrebno stalno skrbeti za to, da je podpis še vedno varen oz. podpisano sporočilo ponovno podpis(ov)ati v primeru, ko poteče doba, ko je še varen. Zagotavljanje veljavnosti elektronskega podpisa na dolgi rok, kar je pomembno predvsem za arhiviranje elektronskih dokumentov, postaja zelo pomembno vprašanje elektronskega podpisa. Kot elektronsko poslovanje temelji tudi elektronsko arhiviranje na tehnologiji e-podpisa, glede na princip trajnosti pa predstavlja za (obstoječo) tehnologijo e-podpisa bistveno večji izziv kot običajno e-poslovanje.

3.2. Razlogi za arhiviranje dokumentov

Med razlogi za arhiviranje dokumentov najdemo predvsem arhiviranje za potrebe kontrole in revidiranja, arhiviranje za potrebe kasnejšega dokazovanja dejstev na katera kažejo shranjeni dokumenti ter arhiviranje zaradi zaščite interesov tretjih oseb, na katere se nanašajo arhivirane listine. Arhiviranje za potrebe kontrole in revidiranje npr. nastopi pri arhiviranju poslovnih listin, računov, obračunov davka itd. Arhiviranje za potrebe kasnejšega dokazovanja nastopi predvsem pri pogodbenih odnosih, ko obe stranki shranjujeta dokumente iz svojega pravnega razmerja, kot so pogodbe, računi, dobavnice itd. za primere kasnejšega dokazovanja na sodišču. Arhiviranje zaradi zaščite tretjih oseb pa npr. nastopi pri arhiviranju oporoke, kjer je potrebno zaščititi interese dedičev oz. volilojemalcev. Velikokrat se vsi trije razlogi tudi prekrivajo: stranke npr. hranijo prejete in izdane račune najprej zaradi možnosti revidiranje davčnih obveznosti s strani države, potem zato, da se lahko v medsebojnih razmerjih sklicujejo nanje (npr. po izdaji računa, ki ga druga stran ne plača lahko prva stran zaračuna še zamudne obresti), potem pa seveda tudi zaradi zaščite interesov tretjih oseb (npr. lastnikov podjetja, ki želijo imeti uvid v poslovanje podjetja ali države, ki želi pobrati davčne obveznosti).

3.3. Primerjava lastnosti lastnoročnega in elektronskega podpisa

Za lastnoročni podpis, skupaj z določenimi dodatnimi elementi na podpisanem dokumentu velja, da zagotavlja:

- enoznačno ugotavljanje identitete podpisnika (podpisa se ne da stoodstotno ponarediti, nobeni dve osebi nimata istega podpisa),
- nespremenljivost podpisanega dokumenta (ob parafiranju ter oštevilčenju strani ter zapolnitvi praznih prostorov na dokumentu) ter
- dolgoročno možnost preverjanja (vse dokler podpisnik živi, kar je ponavadi dlje od življenjske dobe dokumenta)

Podobno velja za elektronski podpis. Ta zagotavlja enoznačno ugotavljanje identitete podpisnika (kdo je podpisal) ter daje jamstvo za nespremenljivost vsebine podpisanega dokumenta. V tretjem elementu pa se podpisa razlikujeta; medtem ko je trajnost navadnega podpisa neomejena (oz. omejena na čas življenja podpisnika) pa e-podpis ni trajen. Zaradi razvoja vse hitrejših računalnikov in boljših algoritmov za odkrivanje šifrirnih ključev je življenjska doba takega ključa (oz. e-podpisa) omejena. Zaradi tega je potrebno ključe menjati oz. osveževati podpis na elektronskih dokumentih, da se ta šteje za varnega. Vzdrževanje veljavnosti e-podpisa oz. elektronskih dokumentov je posebna tehnična dejavnost, ki jo zahteva e-podpis in ki nima ekvivalenta pri običajnem podpisu.

3.4. Primerjava lastnosti navadnih in elektronskih dokumentov

Za papirne dokumente se včasih zahtevajo posebni formati (žigi, štampiljke, logo) za njihovo veljavnost. Postavlja se vprašanje, kako je tem zahtevam zadoščeno v elektronskem svetu oz. katere od teh so v elektronskem svetu sploh smiselne. Pri tem posebni formati služijo več namenom, med drugim ugotovitvi identitete avtorja, opozorilu na pomembnost samega dokumenta, zagotovitvi integritete vsebine dokumenta itd.

Za ugotovitev identitete avtorja se v neelektronskih dokumentih, poleg lastnoročnega podpisa, včasih uporabljajo še žig, pečat, vodna štampiljka itd. Te dodatne obličnosti naj bi utrdile vero nasprotne stranke v identiteto podpisnika in preprečile oz. otežile možnost zatrjevanja lažne identitete. V elektronskem svetu tem zahtevam zadošča varen elektronski podpis, saj je ta sam v resnici pravzaprav bolj podoben žigu oz. pečatu kot navadnemu podpisu. Zaradi njegovih lastnosti (unikatnost zasebnega ključa) je, skupaj z digitalnim potrdilom, jamstvo za to, da je vsebino lahko podpisal samo njegov zakoniti imetnik (če mu zasebni ključ seveda ni bil odtujen, kar pa predstavlja enako nevarnost z žigi in pečati).

V opozorilo podpisnikom, da podpisujejo posebno pomemben dokument (ali da je eden od subjektov posebno pomemben) se včasih zahteva prisotnost posebnih logotipov, reliefov, barv in dimenzij papirja. V elektronskem svetu je omenjeno sicer možno zagotoviti (npr. aplikacija za podpisovanje podpiše posebej formatirano različico dokumenta), vprašanje pa je, če je še potrebno, saj je možno opozorilo o pomembnosti vgraditi v sam postopek kreiranja elektronskega podpisa. S posebnim formatom, če bo zahtevan, se bo morala ukvarjati aplikacija za elektronsko podpisovanje, ki bo morala podpisniku prikazati ustrezen format in potem podpisati dokument v tem formatu.

Še najbolj pomembni pa so ukrepi, ki naj zagotovijo integriteto (nespremenljivost) vsebine dokumentov. V papirnem svetu se za to včasih uporablja parafiranje strani (da se prepreči kasnejše uvrščanje novih strani v podpisan dokument), številčenje strani (da se kakšna stran kasneje ne zataji) oz. notarski zapis s črticami (ki onemogoča dopis dodatnega teksta). V elektronskem svetu vsem omenjenim zahtevam ustreza varen elektronski podpis, saj ta jamči za nespremenljivost vsebine podpisanega dokumenta.

3.5. Subjekti hranjenja navadnih in elektronskih dokumentov

Pri papirnih dokumentih je možnih več kombinacij arhiviranja dokumentov z vidika subjekta, ki dokumente hrani. Najbolj običajna rešitev je, da vsaka stranka (npr. pri pogodbi) hrani svoj *originalni* izvod pogodbe, torej stranki izdelata dvojni (ali večkratni) original. Druga možnost je, da originalni dokument hrani tretja oseba, ki ji obe stranki zaupata (notar, stranki pa dobita odpravke) ali tretja oseba, ki jo za to postavi zakon (npr. javni register), tretja možnost pa je, da original obdrži ena stranka, druga pa pridobi (notarsko) overjeno kopijo oz. prepis dokumenta.

V primerjavi s temi metodami arhiviranja papirnih dokumentov je elektronsko arhiviranje dokumentov v določenih elementih lažje, v določenih pa težje kot pri papirnih dokumentih. Predvsem gre pri elektronskem podpisovanju za celo tehnično infrastrukturo podpisovanja in verificiranja ter verigo vpletenih tretjih oseb (overiteljev digitalnih certifikatov), tako da je nemogoče govoriti o podpisovanju, verificiranju ter arhiviranju elektronskih dokumentov brez vpletenosti tretjih oseb.Tretje osebe so *vedno* navzoče vsaj pri overjanju digitalnih podpisov in izdajanju digitalnih certifikatov, največkrat pa tudi pri izdajanju elektronskih podpisov ter shranjevanju elektronskih dokumentov. Izdelava dvojnika (ali večkratnika) nepodpisanega dokumenta v elektronski obliki nima smisla, saj se da elektronske dokumente kopirati v poljubnem številu izvodov brez problema. Še bolj pomenljivo je dejstvo, da se elektronska kopija ne razlikuje od originala. Zato pri elektronskih dokumentih tudi odpade opcija izdelave overjenih kopij po tretji osebi. Ostane torej hranjenje elektronskih kopij dokumentov pri strankah *skupaj* s hranjenjem elektronskega podpisa nasprotne stranke (ali še bolje obeh strank), pri čemer dokument sam služi dokazovanju vsebine e-pogodbe, e-podpis pa identifikaciji nasprotne stranke in verifikaciji nespremenljivosti podpisane vsebine. V takem primeru morata stranki sami skrbeti za dolgoročno veljavnost e-podpisa nasprotne stranke. Pri elektronskem arhiviranju pa je bolj običajna možnost, da stranki elektronski dokument s podpisi (ali pa samo podpise) shranita pri tretji osebi – elektronskem arhivu , ki skrbi za vzdrževanje veljavnosti e-podpisov. Glede na določeno tehnično znanje, ki ga to zahteva, bo ta rešitev v praksi verjetno najpogostejša.

3.6. Arhiviranje večkratnih in vgnezdenih podpisov

Posebno vprašanje se postavi pri arhiviranju elektronskih dokumentov, ki so podpisani večkrat. Pri tem gre lahko za dve različni situaciji: pri prvi dokument *vzporedno* podpiše več podpisnikov (npr. podpis elektronske pogodbe s strani vseh vpletenih), pri čemer vsi podpišejo izvorni dokument. Druga možnost je, da so podpisi vgnezdeni oz. zaporedni: najprej izvorni dokument podpiše prvi podpisnik, nato pa že podpisani dokument elektronsko podpiše naslednji podpisnik. Pravna razlika je v tem, da gre pri vzporednem podpisu za zavezo večih strank za isto vsebino (npr. vsebino neke pogodbe), pri zaporednem podpisu pa navadno drugi podpis na nek način avtorizira (npr. vodja oddelka v organizaciji avtorizira pravni posel, ki ga je sklenil zastopnik organizacije), jamči (npr. porok jamči za zavezo originalnega zavezanca) oz. priča o verodostojnosti prvega podpisa (npr. priča potrdi, da je nek posebno pomemben dokument resnično elektronsko podpisal njegov prvi podpisnik). Kakšen namen bo imel posamezen elektronski podpis in v kakšnem zaporedju se bo uporabil bodo seveda določili posebni dogovori med strankama oz. politike elektronskih podpisov, ki jih bosta stranki uporabljali kot svoje splošne pogoje poslovanja. Pri arhiviranju večkratnih in vgnezdenih podpisov pa je ravno tako tehnična razlika med njimi, saj je pri vzporednih podpisih možno skrbeti za dolgotrajno veljavnost vsakega elektronskega podpisa posamezno, pri vgnezdenih podpisih pa bo praktično moral vsak kasnejši podpisnik sam skrbeti za verifikacijo in tudi arhiviranje vseh varnostnih atributov prejšnjega elektronskega podpisa. ZEPEP v 16. členu namreč določa, da morajo osebe, ki hranijo dokumente, ki so elektronsko podpisani, same hraniti tudi komplementarne podatke in sredstva za preverjanje takega podpisa. Kot rečeno bo to praktično pomenilo, da bo moral kasnejši podpisnik za potrebe dolgoročnega arhiviranja pridobiti in hraniti vso verigo potrdil za elektronski podpis pred njim, skupaj z vsemi CRLji oz. OCSPji v trenutku verifikacije, jih časovno žigosati in na teh podatkih periodično obnavljati časovne žige.

3.7. Rok hranjenja elektronskih dokumentov

Rok hranjenja dokumentov je lahko različen. Nekatere roke predpisujejo kogentni predpisi (npr. rok hranjenja poslovnih listin, računov, itd), nekateri roki so določeni s postopki v katerih se dokumenti uporabljajo kot dokazno sredstvo (pri čemer so dokumenti relevantni dokler postopki ne zastarajo), nekateri roki pa so odvisni od razpolaganja strank v zasebnih pogodbenih odnosih (npr. pogodba o najemu zemljišča in nepremičnine lahko traja poljubno vrsto let, tudi 50 ali 100). Na splošno zato velja, da ni zgornje meje hranjenja elektronskih dokumentov, za stranke, ki hranijo posamezne elektronske dokumente pa je priporočljivo, da poznajo, koliko časa so taki dokumenti relevantni, da bodo lahko sprejele ustrezne ukrepe za shranjevanje v času njihove relevantnosti.

3.8. Opredelitev kratkega, srednjega in dolgega roka arhiviranja

Z vidika elektronskih arhivov delimo rok shranjevanja elektronskih dokumentov na kratek, srednji in dolgi rok, v odvisnosti od dostopnosti podatkov za elektronsko podpisovanje, podatkov za preverjanje elektronskega podpisa in glede na njihovo varnost, ki se s tekom časa zmanjšuje. S podatki za elektronsko podpisovanje tu mislimo, skladno z dikcijo ZEPEPa, na zasebne ključe, s podatki za preverjanje elektronskega podpisa na potrdila, z varnostjo pa na neogroženost oz. nekompromitiranost sredstev in podatkov za elektronsko podpisovanje in preverjanje elektronskih podpisov. Opredelitev kratkega, srednjega in dolgega roka je povzeta iz [8].

Kratek rok je opredeljen kot tisti rok, ko so vsi podatki za preverjanje elektronskih podpisov še na voljo (v obliki veljavnih potrdil overiteljev, to se pravi pred njihovim potekom) in ko so hkrati že na voljo podatki o morebitni neveljavnosti takih potrdil (registri CRL oz. odgovori OCSP). Za preverjanje veljavnosti elektronskih dokumentov na kratek rok je potrebno elektronsko podpisati prstni odtis izvornega sporočila ter ime overitelja in serijsko številko potrdila za uporabljeni elektronski podpis. Za kasnejšo uporabo pa bo potrebno elektronski podpis se časovno žigosati in mu priložiti sklicevanja (ne vrednosti) na potrdila v certifikacijski verigi oz. reference na statuse teh potrdil (CRL, OCSP). Časovni žig ne bo potreben za to, da bi se dokazovalo, da je zapis nastal pred časom, ko bi se dalo z vzvratnim inženiringom iz javnega ključa dobiti zasebni ključ (ker gre za kratek rok), pač pa zato, da se dokaže, da je elektronski podpis oz. podpisan dokument nastal pred dnem, ko je bil razglašen za neveljavnega (CRL).

Srednji rok je opredeljen kot rok ko so nekatera potrdila v verigi potrdil lahko že neveljavna oz. ko nekatere informacije kot so seznam preklicanih potrdil (CRL) niso več na voljo. V tem primeru je potrebno, v času ko so potrdila še veljavna,

oz. ko so seznami preklicanih potrdil še na voljo, shraniti ta potrdila in njihove statuse (shraniti vrednosti, ne samo reference) in jih časovno žigosati. Časovni žig na potrdilih in njihovih statusih bo kasneje pričal o tem, da so ta potrdila v določenem času obstajala in da niso bila neveljavna, da je torej s temi potrdili opremljeni elektronski dokument bil veljavno podpisan preden bi podatki za podpisovanje postali neveljavni. Ta način verificiranja elektronskih dokumentov je primeren tudi kadar nadaljnji verifikatorji ne bodo imeli dostopa do vseh potrdil in njihovih statusov in morajo biti ti zato priloženi (in časovno žigosani) elektronskemu podpisu izvornega dokumenta.

Dolgi rok je opredeljen kot rok v katerem je možno kriptografske metode, ki se uporabljajo za časovno žigosanje razbiti in iz javnih ključev overiteljev časovnih žigov dobiti zasebne. V takih primerih bo potrebno vsakokrat pred potekom tega roka ponovno časovno žigosati celoten dokument oz. varnostne atribute na njem (elektronski podpis na izvornem dokumentu hkrati z časovnim žigom na njem, verigo potrdil in statuse potrdil ter časovni žig na njih), kar bo dokazovalo, da je njena vsebina nastala pred časom, ko so postali prejšnji časovni žigi ogroženi (kompromitirani).

V zvezi z omenjenimi tehničnimi zahtevami za arhiviranje elektronskih dokumentov se postavlja vprašanje, kako pravno zagotoviti, da se bodo omenjeni ukrepi izvajali. Zakon oz. uredba sta presplošna, da bi vsebovala konkretne napotke, zato bodo morale zaenkrat stranke s politikami elektronskih podpisov (glej v nadaljevanju) določiti, kako bo potrebno arhivirati take dokumente, da se bodo šteli za veljavne. Politike elektronskih podpisov vsebujejo določbe o verifikaciji elektronsko podpisanih dokumentov, za dolgoročno veljavnost elektronskih dokumentov pa bo potrebno te določbe razširiti s smiselno vključitvijo zahtev za dolgoročno arhiviranje takih dokumentov.

3.9. Kakšne možnosti elektronskega arhiviranja ponuja obstoječa slovenska zakonodaja ?

ZEPEP v 12. členu ureja hranjenje podatkov v elektronski obliki. ZEPEP na splošno določa, da se lahko določeni dokumenti, zapisi ali podatki, za katere zakon (ali drug predpis) določa, da se morajo hraniti, hranijo tudi v elektronski obliki. Pri tem pa morajo biti taki podatki:

- dosegljivi in primerni za kasnejšo uporabo,
- shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti, ali kakšni drugi obliki, ki verodostojno predstavlja oblikovane, poslane ali prejete podatke,
- če gre za elektronsko sporočilo mora biti mogoče ugotoviti od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema,
- uporabljena tehnologija in postopki morajo v zadostni meri onemogočati spremembo ali izbris podatkov, ki ju ne bi bilo mogoče enostavno ugotoviti, oziroma obstajati mora zanesljivo jamstvo glede nespremenljivosti sporočila.

Zakon v 3. odstavku 12. člena izrecno izenači pisno in elektronsko obliko tudi glede hranjenja dokumentov (sicer zakon v 15.členu izenačuje lastnoročni in varen elektronski podpis). Pri tem šteje, da je elektronska oblika hranjenja ustrezna, če ustreza zgoraj navedenim pogojem in če zakon za posamezne podatke (4.odstavek 15. člena) ne zahteva strožjih pogojev hrambe ali posebne hrambe.

Prvi dve alineji se nanašata na podatke, ki se shranjujejo. Ti se lahko shranijo v izvirni obliki ali pa v kakšni drugi obliki, ki verodostojno predstavlja izvirne podatke..Zaradi hitrega napredka tehnologije namreč pri dolgoročnem shranjevanju nima smisla (ni mogoče) vztrajati pri izvirni obliko podatkov, saj bi bilo za to potrebno zagotoviti izvirno strojno platformo (strojno opremo), sistemsko programsko opremo (operacijski sistem) ter aplikativno programsko opremo. Ker to največkrat ne bo realistično, bo mogoče zagotoviti bodisi emulacijsko okolje, ki bo simuliralo izvorno strojno in programsko opremo, ali pa periodično spreminjati format zapisa podatkov (migracija), tako da bo ustrezal trenutnim tehnološkim zahtevam.

Tretja alineja postavlja pogoje za shranjevanje elektronskih sporočil, se pravi elektronskih podatkov, ki so bili po neki komunikacijski mreži odposlani prejemniku. Pri shranjevanju takih sporočil je potrebno zagotoviti, da se shranijo podatki o izvoru sporočila, naslovniku sporočila, času in kraju njegove oddaje ter času in kraju njegovega sprejema. Zakon pri tem ne specificira, ali gre za dejanski, dokazljiv čas in kraj oddaje in sprejema ali zatrjevan. Glede na neobstoj določenih storitev elektronskega certificiranja v preteklosti (npr. overiteljev časovnih žigov) so bili taki podatki v preteklosti lahko samo zatrjevani.

Četrta alineja pa na splošno določa pogoje, ki jim mora zadostiti vsako shranjevanje elektronskih podatkov, če naj se to šteje za skladno z zakonom. Glede na dikcijo, ki pravi, da morajo postopki za elektronsko arhiviranje v zadostni meri onemogočati spremembo ali izbris podatkov oz. zahtevo po jamstvu glede nespremenljivosti sporočila (integriteta podatkov) ter skupaj z zahtevami prejšnje alineje (neizpodbitna ugotovitev izvora, naslovnika, kraja in časa oddaje in prejema) bi lahko sklepali, da gre za podobne zahteve kot pri varnem elektronskem podpisu, torej da postopki, ki jih zakon tu omenja merijo na varno elektronsko podpisovanje (4. odstavek 2.člena ZEPEP):

- podpis mora biti povezan izključno s podpisnikom,
- iz njega je mogoče zanesljivo ugotoviti podpisnika,
- ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom,
- podpis je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

Glede na povedano in v izogib dvoumnostim bi bilo verjetno bolje, da bi se zakon v 12. členu direktno skliceval na uporabo varnega elektronskega podpisa pri shranjevanju elektronskih podatkov.

Drug formalni pravni vir za arhiviranje elektronskih dokumentov je uredba.

Uredba tako npr. določa (32. člen), da časovna veljavnost kvalificiranih potrdil (razen lastnih kvalificiranih potrdil overitelja) znaša največ pet let od dneva njegove izdaje.

33. člen uredbe pa določa, da mora tisti, ki hrani elektronsko podpisane podatke, če hoče ohraniti veljavnost elektronskega podpisa, najkasneje en mesec pred iztekom roka veljavnosti kvalificiranega potrdila, zagotoviti ponoven elektronski podpis podatkov s strani vseh oseb, ki so podatke elektronsko podpisale ali pa s strani notarja ali pa potrditev teh podatkov z varnim časovnim žigom overitelja.

Od omenjenih možnosti je z vzpostavitvijo agencije za izdajanje varnih časovnih žigov SI-TSA najbolj praktično časovno žigosanje. Ostale možnosti namreč niso posebej praktične, nekatere pa tudi (še) niso izvedljive.

Možnost ponovnega podpisa pred iztekom veljavnosti le tega s strani vseh prvotno podpisanih strani je ponavadi izven sfere vplivanja ene pogodbene stranke (če gre za pogodbo bodo druge pogodbene stranke včasih imele neposredno korist od zanikanja svojega podpisa), zato ta možnost največkrat ne bo prišla v poštev.

Zakon o notariatu [32] sicer dovoljuje, da notar potrdi čas, ko mu je bila na vpogled predložena kakšna listina (66. člen), vendar zakon govori samo o listinah, ne pa tudi o elektronskih dokumentih, zato je vprašljivo, če se da določbe omenjenega člena brez nadaljnjih sprememb zakona interpretirati v smislu elektronskih dokumentov. Poleg tega se uporaba elektronskega podpisa pri notarjih šele uveljavlja (npr. elektronska knjiga sklepov pri enoosebnih družbah z omejeno odgovornostjo), tako da še ni v celoti jasno, kako bodo taki postopki potekali.

V zvezi s časovnim žigosanjem pa se postavlja tudi vprašanje, ali je po slovenski zakonodaji dopustno časovno žigosati elektronske dokumente izven RS oz. kakšno pravno veljavo ima tako žigosanje. 46. člen ZEPEPa določa, da so kvalificirana potrdila overitelja s sedežem v Evropski Uniji enakovredna domačim kvalificiranim potrdilom. Zakon podrobneje določa tudi, kako je z veljavnostjo potrdil overiteljev, ki imajo sedež v tretjih državah. Ker gre pri časovnem žigu samo za posebno vrsto potrdila, ki potrjuje vsebino podatkov na katere se nanaša, v navedenem času, lahko sklenemo, da je v RS, kljub odsotnosti domačih overiteljev časovnih žigov, možno veljavno časovno žigosati elektronske dokumente z uporabo teh storitev najmanj pri overiteljih, ki imajo sedež v EU.

Postavlja se vprašanje, ali so omenjene določbe zakona in uredbe dovolj jasne oziroma interpretativne za konkretno implementacijo arhiviranja elektronskih dokumentov ali bi bilo potrebno zakon (ali še bolje uredbo) spremeniti oz. dopolniti z bolj natančnimi zahtevami za varno elektronsko arhiviranje dokumentov oz. sklicevanjem na tehnične standarde, ki urejajo to materijo. Odgovor na to vprašanje je deloma ponudila že novela ZEPEPa [29] , ki nekoliko podrobneje ureja materijo, ki prej ni bila ali pa ne dovolj dobro urejena (npr. varno časovno žigosanje), še več pa glede ureditve elektronskih arhivov pričakujemo od nastajajočega Zakona o varstvu dokumentarnega in arhivskega gradiva ter

arhivih.

4. ELEKTRONSKI ARHIVI KOT PONUDNIKI ELEKTRONSKIH STORITEV

4.1. Uvod

Dejanja potrebna za pravno veljavno arhiviranje elektronskih dokumentov so dovolj zapletena, da jih bodo včasih stranke hotele poveriti za to specializiranim tretjim osebam – elektronskim arhivom. Elektronski arhivi bodo odgovorni za shranjevanje elektronskih dokumentov in vseh potrebnih podpisov, potrdil in časovnih žigov na teh dokumentih, ki bodo dokazovali njihov izvor, čas nastanka ter integriteto njihove vsebine. Elektronski arhivi bodo tako odgovorni za vse procese v zvezi z verifikacijo, shranjevanjem, časovnim žigosanjem in ponovnim časovnim žigosanjem originalnih dokumentov in vseh varnostnih atributov na njih. Ko taki bodo elektronski arhivi ponudniki elektronskih storitev, za katere bodo veljale direktive EU o elektronskem poslovanju (v zvezi z ustanavljanjem in poslovanjem ponudnikov storitev informacijske družbe ter trženjem njihovih storitev). Glede na naravo njihovega dela pa bo potrebno, verjetno na sistemski ravni z zakonom, urediti se njihovo odgovornost za pravilno shranjevanje in verificiranje dokumentov, njihove obveznosti glede varovanja osebnih in zaupnih podatkov itd. Nekatera od teh vprašanj so predstavljena v nadaljevanju.

4.2. Centralizirani/decentralizirani model storitev elektronskega arhiviranja

Teoretično sta možna dva pristopa k izvedbi elektronskih arhivov: centralizirani in decentralizirani. Centralizirani arhiv je zadolžen tako za hrambo elektronskih podpisov, časovnih žigov in drugih podatkov za dolgoročno vzdrževanje veljavnosti elektronskih dokumentov kot tudi hrambo samih podatkov, ki so podpisani. To seveda pomeni, da ima arhiv vpogled v vsebino podpisanih elektronskih zapisov in da je potrebno na nek način določiti, kaj s to vsebino lahko počne (pogodbena zaveza k varovanju zaupnih podatkov, splošna zakonska zapoved za zaupnost arhiviranih zapisov). Decentralizirana izvedba arhiva pa skrbi samo za arhiviranje elektronskih podpisov, časovnih žigov in drugih podatkov za dolgoročno vzdrževanje veljavnosti elektronskih dokumentov, ne pa tudi za shranjevanje samih dokumentov. Te morajo, če bodo hoteli dokazovati njihovo veljavo, shranjevati stranke same, decentralizirani arhiv pa skrbi samo za neovrgljivo potrjevanje, da so bili ti zapisi, ustvarjeni oz. podpisani in predloženi s strani določene osebe v določenem času. S tem postane odvečno tudi vprašanje zaupnosti shranjenih podatkov, saj morata za to skrbeti stranki.

4.3. Zaupnost arhiviranih podatkov

Elektronski arhivi včasih vsebujejo zaupne in osebne podatke. Če gre za centralizirane arhive, ki poleg elektronskih podpisov in časovnih žigov shranjujejo še vsebino podpisanih elektronskih dokumentov, imajo ti nujno vpogled v vso njihovo vsebino. S pravnega vidika je dolžnost elektronskih arhivov za spoštovanje zaupnosti shranjenih dokumentov lahko predpisana na več različnih načinov. Dolžnost spoštovanja zaupnosti shranjenih dokumentov lahko predpiše zakon (kot jo npr. predpisuje za posebne poklice kot so zdravniki, odvetniki itd), lahko pa se uredi pogodbeno med shranjevalcem elektronskih zapisov in elektronskim arhivom. V primeru, da gre za decentralizirano različico arhiva, ko arhiv ne vidi vsebine podpisanih dokumentov, pa težave z zaupnostjo podatkov odpadejo.

4.4. Varstvo osebnih podatkov in elektronski arhivi

Ne glede na izvedbo elektronskega arhiva (centralizirana/decentralizirana) bo potrebno posebej urediti vprašanja varstva osebnih podatkov. Taka vprašanja se pojavljajo v zvezi z različnimi potrdili, ki jih bodo arhivi hranili kot varnostne atribute shranjenih dokumentov in ki lahko vsebujejo osebne podatke (ime, psevdonim, elektronska pošta) strank, še bolj pa v zvezi z morebitnimi osebnimi podatki, ki bi se nahajali v shranjenih dokumentih. Pri tem bo veljal podoben premislek kot glede varstva zaupnih podatkov v centraliziranih/decentraliziranih arhivih.

4.5. Ustanavljanje elektronskega arhiva

Ustanavljanje elektronskih arhivov v državah članicah EU mora biti po direktivah o elektronskem podpisu in elektronskem poslovanju stvar svobodnega trga in ne sme biti pogojena s posebnimi administrativnimi odobritve s strani državnih organov.

4.6. Uporaba elektronskega arhiva za dokazovanje obstoja odposlanih sporočil

Poleg shranjevanja elektronskih zapisov je elektronski arhiv pomemben tudi zaradi dokazovanja, da je bilo določeno elektronsko sporočilo poslano ob določenem času oz. da je bilo ob določenem času na voljo. Pošiljatelj in prejemnik lahko v tripartitni pogodbi pooblastita elektronski arhiv, ki bo deloval kot neke vrste poštni nabiralnik, kamor bo pošiljatelj odlagal sporočila, ki se bodo časovno evidentirala in od kjer jih bo prejemnik lahko sprejemal. Na ta način bo pošiljatelj lahko dokazal, da je določeno sporočilo poslal oz. dal na voljo prejemniku, saj bi sicer ta lahko zanikal, da je tako sporočilo dobil.

4.7. Pogodbeni odnos med elektronskim arhivom in uporabniki storitev elektronskega arhiviranja

Odnos med elektronskim arhivom in uporabniki storitev elektronskega arhiviranja bo pravno urejen s pogodbo med arhivom in uporabnikom storitev. Poleg pogodbe bo temelj njunega medsebojnega pravnega odnosa lahko zakon, ki bo posebej opredeljeval, podobno kot pri overiteljih potrdil, pravice in dolžnosti elektronskih arhivov. Pogodba bo morala vsebovati vsaj rok hranjenja dokumentov, krog subjektov, ki bodo imeli dostop do shranjene vsebine (poleg samega shranjevalca), opredelitev narave shranjenih podatkov (tajni, zaupni, osebni) in posebnega ravnanja z njimi, odgovornost elektronskega arhiva za pravilno shranjevanje zapisov in njihovo dostopnost, dolžnost arhiva, da podatke po prenehanju veljavnosti pogodbenega odnosa izbrišejo itd.

4.8. Odgovornost elektronskih arhivov

Najbolj pomembne naloge elektronskih arhivov so shranjevanje elektronskih zapisov in ohranjanje njihove veljavnosti (z vključevanjem podatkov o potrdilih, statusnih potrdil in njihovim časovnim žigosanjem). Uporabniki elektronskih arhivov bodo z elektronskim arhivom sklenili pogodbe o shranjevanju svojih elektronskih dokumentov. Od določb takih pogodb oz. splošnih zakonskih določb za elektronske arhive bo odvisno, kakšno odgovornost bodo nosili elektronski arhivi oz. za kaj bodo jamčili. V primeru centraliziranih elektronskih arhivov bodo ti poleg hrambe elektronskih podpisov odgovorni tudi za hrambo samih elektronskih dokumentov. Če bi se v tej hrambi pojavila kakršnakoli napaka (uničenje elektronskih zapisov, njihovo predrugačenje, nedostopnost) bi elektronski arhiv pogodbeno in zakonsko odgovarjal za škodo, ki bi s tem nastala. Podobno bi elektronski arhiv (kakršnegakoli tipa) odgovarjal, če ob zahtevi za predložitev verige časovnih žigov in potrdil, ki bi potrjevali veljavnost elektronskih zapisov, tega ne bi zmogel storiti (npr. ker določenih potrdil oz. statusov ni shranil, pa niso več dosegljivi, ker ni pravočasno, pred koncem veljavnosti, časovno žigosal zapisov, itd). Tu se postavlja vprašanje, kako tako odgovornost urediti, pogodbeno ali zakonsko. Zaradi poenotenja prakse bo verjetno potrebno, tako kot pri odgovornosti overiteljev potrdil, zakonsko določiti minimalne zahteve, ki jih bo moral elektronski arhiv izpolnjevati oz. jamstva, ki jih bodo imeli njegovi uporabniki po samem zakonu. Izven tega pa bodo pogodbe med elektronskim arhivom in njegovimi uporabniki lahko določale višjo stopnjo pravne varnosti za uporabnike v smislu višjih zahtev, pogodbenih kazni itd., če elektronski arhiv ne bi izpolnil svoje osnovne dolžnosti shranjevanja in verificiranja elektronskih zapisov. Zakonodaja EU predpisuje splošno odgovornost ponudnikov elektronskih storitev (npr. [16] in druge direktive), slovenska zakonodaja pa je del teh določb že implementirala v Zakonu o varstvu potrošnikov [37], del pa v noveli Zakona o elektronskem poslovanju in elektronskem podpisu [29].

5. SPORAZUM O ELEKTRONSKEM POSLOVANJU

Sporazum o elektronskem poslovanju je pogodba med strankami, ki želijo poslovati v elektronski obliki, ki vsebuje določitev načinov elektronskega komuniciranja med strankama ter pogojev za pravno veljavnost take komunikacije. Sporazum o elektronskem poslovanju za samo elektronsko poslovanje ni nujen, saj zakon določa splošni okvir, znotraj katerega se odvijajo dejanja elektronske komunikacije. Določbe zakona pri tem veljajo za odprte sisteme, se pravi za sisteme ki niso določeni v posebnih sporazumih med strankami, ki elektronsko komunicirajo (npr. EDI). Kot take imajo določbe zakona naravo dispozitivnih določb ki so privzeta, če ni drugače določeno med strankama. Določbe zakona so tako splošne, da poslovni partnerji velikokrat vidijo potrebo skleniti poseben sporazum o elektronskem poslovanju s katerim podrobneje uredijo načine medsebojne komunikacije. Tak sporazum ponavadi podrobneje kot zakon specificira določene načine elektronske komunikacije in s tem nadomesti določene dispozitivne dele zakona, po drugi strani pa se, kjer zakon določeno materijo opredeljuje dovolj podrobno, nanj sklicuje. V tem smislu ni natančne meje med zaprtimi in odprtimi sistemi. Odprti sistemi so tisti, za katere v celoti velja zakon in ki niso podrobneje specificirani z dodatnimi sporazumi med strankami. Zaprti sistemi so tisti, ki so *»v celoti urejeni s pogodbami med znanim številom pogodbenih strank«* (2.odstavek 1.člena ZEPEP). Večina sistemov pa bo nekje vmes: med strankami bodo sprejeti dodatni, vsaj okvirni, sporazumi o elektronskem poslovanju (ter politike elektronskih podpisov, politike potrdil itd.), ki bodo specificirali določene zakonske določbe, druge določbe zakona pa bodo za te primere normalno veljale naprej.

5.1. Povezanost med sporazumom o elektronskem poslovanju, politikami elektronskih podpisov in konkretnimi pravnimi posli

Predmet sporazuma o elektronskem poslovanju je podrobnejša določitev določenih zakonskih določb. Vsebina sporazuma o elektronskem poslovanju se včasih pokriva z vsebino politik(e) elektronskega podpisa, predvsem v njenem pravnem delu. Sporazum o elektronskem poslovanju se sklene zaradi določitve splošnih načinov elektronskega poslovanja, politika elektronskega podpisa, ki lahko spremlja posamezen elektronski podpis (oziroma podpisan dokument) pa določa splošne pogoje pod katerimi veljajo oz. se presojajo dokumenti, ki se sklicujejo na to politiko. Kot tak ima sporazum o elektronskem poslovanju naravo generalnega pravnega akta, politika elektronskega podpisa pa v odnosu do sporazum naravo specialnega pravnega akta (kar tudi pomeni, da v primeru nesoglasja veljajo določbe specialnejšega pravnega akta). V idealnem primeru bo sporazum o elektronskem poslovanju določil splošne pogoje elektronskega komuniciranja, pri tem pa se bo za posamezen tip elektronskega sporočila skliceval na uporabo posebne politik(e) elektronskega podpisa. Če stranki za posamezne posle ne bosta uporabljali posebnih politik elektronskega podpisa pa bosta ustrezno materijo tipično uredile kar v sporazumu o elektronskem poslovanju.

Po drugi strani je sporazum o elektronskem poslovanju povezan tudi s konkretnimi elektronskimi posli. Kot rečeno je običajno da so načini komuniciranja urejeni v sporazumu o elektronskem poslovanju. Če takega sporazuma ni, pa lahko vsak elektronski posel (pogodba, izjava volje) posebej določi pogoje za svojo veljavnost oziroma presojanje svoje vsebine. Pravna pravila, ki urejajo posamezen elektronski posel, bodo tako lahko vsebovana v štirih pravnih virih: prvi vir bo zakon s svojimi splošnimi določbami za elektronsko poslovanje, drug vir bo sporazum o elektronskem poslovanju, ki velja med strankami podpisnicami sporazuma in podrobneje razčlenjuje določene načine komuniciranja, tretji vir bodo politike elektronskega podpisa za posamezna poslovanja dejanja oz. za posamezne poslovne vloge, četrti vir pa bo konkreten elektronski pravni posel (pogodbe, ponudbe itd).

5.2. Primer sporazuma o elektronskem poslovanju

Sporazum o elektronskem poslovanju ponavadi podrobneje določa načine elektronske komunikacije. Pri tem so pomembni tako tehnični načini (elektronska pošta, uporaba elektronskih podpisov, potrdila kvalificiranih overiteljev) kot njihova pravna vsebina (ponudba, sprejem ponudbe, potrditev prejema itd). Sporazum o elektronskem poslovanju nadalje določa, kaj se šteje za kraj in čas oddaje elektronskega sporočila, kraj in čas prejema elektronskega sporočila, kdaj nastopijo pravni učinki elektronskega sporočila, kakšne konkretne obveznosti imata stranki glede verifikacije in shranjevanja elektronskih sporočil itn. Podobno taki sporazumi ponavadi vsebuje izbiro prava in jurisdikcije, načine prekinitve pogodbe, načine razreševanje sporov itd.

V nadaljevanju je komentirana vsebina posameznih členov vzorčnega sporazuma o elektronskem poslovanju, ki je podan

v prilogi.

5.2.1 Način komuniciranja

Način komuniciranja opredeljuje tehnične (elektronska pošta, splet, EDI, itd) ter pravne (ponudba, sprejem ponudbe, protipredlog itd). Tehnično komunikacija lahko poteka preko elektronske pošte (najbolj običajno), lahko pa se stranki domenita tudi za komuniciranje preko oglasnih desk oz. forumov (npr. pri dražbah), za interaktivno komuniciranje (npr. s tehnologijo on-line klepetalnic) itd.

Z vidika različnih pravnih izjav volje lahko dejanja komunikacije delimo na ponudbo, sprejem ponudbe, protiponudbo ali nasprotni predlog, obvestilo, potrdilo o prejemu itd. Z vidika poslovnih procesov pa posamezna (komunikacijska) dejanja stranka delimo tudi na predračune, naročilnice, dobavnice, račune itd. (pri tem ima predračun pravno naravo ponudbe, naročilnica pravno naravo sprejema ponudbe, dobavnica pravno naravo obvestila o izpolnitvi obveznosti, račun pa pravno naravo poziva k plačilu in ugotovitve o višini davčne obveznosti).

5.2.2 Kraj in čas oddaje elektronskega sporočila

Zanimiva je določitev kraja in časa oddaje elektronskega sporočila. Za kraj oddaje se ponavadi šteje stalno bivališče fizične osebe oz. sedež pravne osebe, ne glede na dejanski kraj, od koder je bilo elektronsko sporočilo poslano. Navezna okoliščina bivališča oz. sedeža zaradi svoje stalnosti in iz tega izhajajoče pravne varnosti ponavadi prevlada nad dejanskim krajem oddaje (tako tudi 21. člen OZ). Za čas oddaje elektronskega sporočila ZEPEP določa čas, ko elektronsko sporočilo vstopi v informacijski sistem izven nadzora pošiljatelja. Taka določba je bila povzeta tudi v vzorčnem sporazumu o elektronskem poslovanju. Kljub temu, da sporočilo pravne učinke ponavadi dobi, ko ga prejemnik dobi oz. ko vstopi v informacijski sistem prejemnika, je čas oddaje sporočila pomemben, ker v določenih primerih od tega časa naprej tečejo roki (npr. če ni navedeno, kdaj rok začne teči, 2. odstavek 26. člena OZ za pisno komuniciranje določa za čas oddaje datum, ki je v pismu oz. na pisemski ovojnici). V elektronskem svetu je sicer razlika med časom oddaje in sprejema elektronskega sporočila manjša kot pri pisnih pošiljkah, zato ta čas ne igra tako velike vloge.

5.2.3 Kraj in čas prejema elektronskega sporočila

Podobno se za kraj prejema elektronskega sporočila šteje kraj, kjer ima prejemnik sedež oziroma stalno prebivališče v času prejema. Za čas prejema elektronskega sporočila pa se šteje čas, ko je elektronsko poročilo vstopilo v prejemnikov informacijski sistem. Pri tem ni bistveno, če se je prejemnik s sporočilom dejansko seznanil, bistveno je, da je imel to možnost. Čas sprejema elektronskega sporočila je posebej pomemben, ker je to ponavadi čas, ko nastanejo pravni učinki sporočila (sprejemna teorija, ki velja tudi v našem pravu).

5.2.4 Potrditev prejema elektronskega sporočila

Potrditev prejema elektronskega sporočila je opcionalna. Tako določa tudi ZEPEP v 7. členu. Vzorec sporazuma o elektronskem poslovanju upošteva obe možnosti. Po eni strani je prejem vedno možno potrjevati, po drugi strani pa so pravni učinki delovanja elektronskega sporočila premaknjeni na čas, ko pošiljatelj od naslovnika prejme potrditev prejema, samo v primeru, ko je potrditev prejema nujna. V nasprotnem primeru začne sporočilo pošiljatelja vezati, ko ga naslovnik prejme.

5.2.5 Razveljavitev sporočila

Razveljavitev sporočila ima v elektronskem svetu smisel samo, če je prejemnik zahteval potrdilo o prejemu z nasprotne strani. V tem primeru ima pošiljatelj možnost, da sporočilo prekliče, dokler ne dobi od nasprotne strani takega potrdila. Možnost, ki sicer velja za razveljavitev sporočila, da je to namreč brez veljave, če prejemnik hkrati s sporočilom (ali prej) dobi tudi njegovo razveljavitev (2. odstavek 25. člena OZ), v elektronskem svetu nima velikega smisla, saj bo sporočilo ponavadi oddano in sprejeto v teku nekaj sekund.

5.2.6 Nastop pravnih učinkov

Čas sprejema elektronskega sporočila je posebej pomemben, ker je to ponavadi čas, ko nastanejo pravni učinki sporočila. S pravnega vidika je nastop pravnih učinkov mogoče vezati na čas oddaje sporočila (oddajna teorija), čas sprejema sporočila (sprejemna teorija) ter čas, ko se naslovnik dejansko seznani z vsebino sporočila (informacijska teorija), glej npr.[2], str 136-137. V našem pravu velja sprejemna teorija (21. člen OZ). To upošteva tudi ZEPEP, ki isto določa za elektronska sporočila, to pa upošteva tudi pričujoči vzorčni sporazum o elektronskem poslovanju. Kot rečeno je razlika med časom oddaje in prejema pomembna v svetu pisnih sporočil, saj je možno pravne učinke, ki so vezani na čas sprejema sporočila preprečiti, če pošiljatelj naslovniku pred tem časom sporoči, da od sporočila odstopa. Ta ureditev bo imela manjšo težo v elektronskem svetu, ko je razlika med časom oddaje in časom prejema ponavadi neznatna.

5.2.7 Obdobje za sprejetje

Člen določa privzeto pravilo, da ponudba ali protipredlog (lahko pa bi veljalo tudi za druga sporočila, npr. predračun, naročilnico, itd.) veljata 15 dni, če ni v samem elektronskem sporočilu drugače določeno. V primeru kasnejšega sprejetja s strani nasprotne stranke, se tako sprejetje šteje kot nova ponudba nasprotne strani.

5.2.8 Obdobje za potrditev

Podobno je določeno privzeto pravilo, da je prejem sporočil potrebno potrditi v roku 24 ur od njegovega prejema, sicer velja za neobstoječe.

5.2.9 Omejitev odgovornosti za elektronske pravne posle

Omejitev odgovornosti je sicer značilna za politike elektronskega podpisa, ki omejujejo odgovornost za določene vrst posla na določeno vsoto. Podobno se da na splošno določiti v sporazumu o elektronskem poslovanju za vse vrste izjav volje. Ta člen je opcionalen.

5.2.10 Politike elektronskih podpisov

Politike elektronskih podpisov ponavadi določajo splošne pogoje za posamezne vrste poslov. Sporazum o elektronskem poslovanju se lahko eksplicitno sklicuje na politik, ki se bodo uporabljale.

5.2.11 Kvalificirana digitalna potrdila

Sporazum o elektronskem poslovanju lahko vsebuje opis oziroma seznam overiteljev kvalificiranih digitalnih potrdil, ki jih bosta stranki uporabljali pri svojem poslovanju. Stranki se pri tem zavezujeta, da bosta kot veljavne upoštevali vsa elektronska sporočila, ki bodo varno elektronsko podpisana in opremljena s kvalificiranim potrdilom, za katerega bo jamčil zaupanja vreden overitelj ter overitelji za katere ta jamči posredno ali neposredno.

5.2.12 Verifikacija elektronskih sporočil

Določbe, ki opredeljujejo tehnične korake, ki so potrebni pri verifikaciji elektronskih sporočil. Ponavadi se te določbe nahajajo v politiki elektronskega podpisa.

5.2.13 Arhiviranje elektronskih sporočil

Določbe, ki opredeljujejo tehnične korake, ki so potrebni pri dolgoročnem shranjevanju elektronskih sporočil .Te določbe se lahko nahajajo tudi v politiki elektronskega podpisa.

5.2.14 Izbira prava

Če gre za mednarodni element, je potrebno določiti pravo, ki se bo uporabljalo za presojo pravnih razmerij, ki nastanejo s tem sporazumom.

5.2.15 Prekinitev pogodbe

S prekinitvijo pogodbe stranki prenehata elektronsko poslovati v prihodnosti (oz. lahko poslujeta v skladu z zakonskimi določili, ki urejajo elektronsko poslovanje ali pa sprejmeta nov sporazum). Pomembno je, da sporazum določa, da pretekla elektronska komunikacija med strankama ohrani pravno veljavo ter da za tako komunikacijo kljub prekinitvi pogodbe nadalje veljajo določbe o shranjevanju in dolgoročnem arhiviranju takih elektronskih dokumentov.

5.2.16 Razreševanje sporov

Ponavadi se zahteva mirno razreševanje sporov pri čemer se določi sodišče, ki naj bo krajevno pristojno za morebitne spore, ki bi nastali iz tega sporazuma. Alternativno se lahko določi arbitražno reševanje sporov.

6. POLITIKE ELEKTRONSKEGA PODPISA

6.1. Uvod

Sporazum o elektronskem poslovanju podrobneje določa pravne in tehnične načine elektronskega poslovanja med pogodbenimi strankami. Pri tem je sporazum o elektronskem poslovanju lahko zelo podroben in določa pogoje za veljavnost vsakega elektronskega dejanja oz. sporočila posebej, lahko pa je bol splošen. Včasih bodo stranke želele posebej podrobno opredeliti določena poslovna dejanja (npr. elektronsko ponudbo, izstavitev elektronskega računa itd) ali pa bodo želela natančneje specificirati pooblastila, ki jih ima določena poslovna vloga (npr. direktor, računovodja) pri elektronskem poslovanju oz. uporabi elektronskega podpisa (npr. vodja oddelka se lahko z elektronskim podpisom pravno zaveže samo do določene višine, ali pa: elektronske račune lahko izstavlja samo vodja računovodstva). V takih primerih bosta stranki želeli sprejeti dodatne pravne (in tehnične) predpise, ki bodo natančneje opredeljevali posamezna pravna dejanja oz. pooblastila posameznih poslovnih vlog. Za dosego omenjenih ciljev bosta stranki uporabili politike elektronskega podpisa.

Kot pove ime samo, je politika elektronskega podpisa dokument, ki se nanaša na elektronski podpis. Natančneje, politika elektronskega podpisa se nanaša na elektronsko podpisan dokument, ki vsebuje ali se sklicuje na tako politiko. Npr. elektronsko podpisan dokument lahko kot neke vrste splošne pogoje poslovanja (glej spodaj) oz. drobni tisk vsebuje napotilo na določeno politiko elektronskega podpisa, ki podrobneje opredeljuje način in pogoje poslovanja podpisnika in ki *dopolnjuje* v elektronskem dokumentu navedeno besedilo (pravno zavezo). Nasprotna stran npr. lahko iz take politike izve, da elektronska ponudba, ki se sklicuje na to politiko, velja 8 dni. Politiko elektronskega podpisa pa je mogoče razumeti tudi drugače in v povezavi s politiko potrdil (certifikatov). Možno je npr. izdati elektronsko potrdilo za določeno poslovno funkcijo (npr. računovodja), ki se sklicuje na politiko elektronskega podpisa. To bo pomenilo, da bo za to potrdilo oz. za vse dokumente, podpisane z zasebnim ključem katerega javni par se bo nahajal v tem potrdilu, veljalo, da veljajo samo v povezavi s takšno politiko elektronskega podpisa. Na ta način se bo dalo vezati pooblastila določene poslovne vloge na njen elektronski podpis (nekaj kar sicer na primer ne velja za lastnoročne podpise, da bi lahko oseba kateri je podpis namenjen iz samega podpisa ugotovila pooblastila nasprotne strani). Tako bo npr. v taki elektronski politiki lahko pisalo, da lahko trgovski potnik sklene pravni posel brez avtorizacije svojega nadrejenega samo do določene višine, iz česar bo nasprotna stranka lahko ugotovila njegova pooblastila (in potencialno neveljavnost njegovih ponudb).

Politika elektronskega podpisa je tako množica pravil za ustvarjanje in preverjanje elektronskega podpisa, ki opredeljujejo veljavnost elektronskega podpisa. Politika določa tako pravne kot tehnične pogoje za veljavnost elektronskega podpisa in določa področje njegove uporabe.

Vsebino politike elektronskega podpisa lahko delimo na pravno in tehnično. Tehnična vsebuje tehnične pogoje za kreiranje in preverjanje elektronskega podpisa, pravna pa opredeljuje pogoje pod katerimi je pravno veljavna vsebina elektronskega zapisa in pravne omejitve (npr. tip zaveze, ki izhaja iz določenega dokumenta, pooblastila in omejitve podpisnika, itd).

Politika elektronskega podpisa mora vsebovati vsaj naslednje splošne informacije (glej npr. [3]):

- naziv izdajatelja politike,
- enolični identifikator politike,
- čas veljavnosti elektronske politike,
- datum izdaje politike,
- področje uporabe politike

Poleg tega ponavadi vsebuje še vrsto pravil, ki se delijo na splošna in posebna. Splošna pravila veljajo na splošno za vse transakcije oz. področje uporabe, na katerem se politika elektronskega podpisa uporablja. Posebna pravila pa so podvrsta splošnih, ki veljajo za posamezna ožja področja (npr. elektronski računi v zvezi z nepremičninami so posebna vrsta elektronskih računov, za katere veljajo posebna pravila).

Splošna in posebna pravila se delijo na pravila, ki se tičejo podpisnika in tista v zvezi z nasprotno stranko. Poleg tega vsebujejo varnostne zahteve, ki jim mora ustrezati podpis ter njegova kasnejša verifikacija. Varnostne zahteve obsegajo

zahteve v zvezi z izdajatelji certifikatov, časovnim žigosanjem itd.

Politike elektronskih podpisov delimo na unilateralne in multilateralne. Unilateralne opredeljujejo pogoje za veljavnost enega elektronskega podpisa (npr. izjava volje, podpis), multilateralne pa kadar gre za (hkratni ali zaporedni) elektronski podpis več podpisnikov (npr. pogodba, notarsko overjena listina, zaporedje avtorizacij na nekem dokumentu itd).

Izdajatelji politik elektronskega podpisa so lahko sami imetniki elektronskih potrdil (unilateralno ali multilateralno), lahko pa tipske politike izdelajo tudi različne interesne skupine (zveze potrošnikov, predstavniki gospodarskih skupin itd).

Podpisnik lahko elektronsko podpisuje kot posameznik s svojim osebnim zasebnim ključem, lahko pa v določeni vlogi (direktor, računovodja, skladiščnik, itd), ki je lahko dokazana ali zatrjevana.

Nasprotna stran mora elektronski podpis preveriti v skladu z politiko elektronskega podpisa (in politiko potrdil). Šele s tem ugotovi veljavnost oz. neveljavnost vsebine določenega elektronskega zapisa. Če posebna politika elektronskega podpisa ne obstaja, potem je potrebno podpis preveriti v skladu s tehničnimi standardi, ki veljajo za tisti tip podpisa[1] in splošnimi zahtevami zakonodaje. Tako bo tisti, ki preverja podpis vedno moral izdelati elektronski prstni odtis prejetega sporočila in ga primerjati z podpisanim prstnim odtisom, ki ga je prejel od nasprotne stranke. Politika elektronskega podpisa pa lahko postavi še druge pogoje za verifikacijo oz. veljavnost podpisa, npr. da je ta veljaven šele po preteku nekega prehodnega obdobja (cautionary period), v katerem se dokončno ugotovi, da potrdilo v času podpisa še ni bilo preklicano, pogoje za dolgoročno shranjevanje elektronskega zapisa, med katerimi je minimalen vsaj časovni žig (glej poglavje o arhiviranju) itd.

6.2. Pravni vidiki politike elektronskega podpisa

Direktiva EU (1999/93/EC) nikjer ne omenja politike elektronskega podpisa izrecno. Na več mestih pa se zavzema za promocijo sredstev in tehnologij za podporo varnemu elektronskemu poslovanju. Glede na prispevek politike elektronskega podpisa k varnejšemu (predvsem z vidika večje reguliranosti, torej večje pravne varnosti) poslovanju, politiko lahko štejemo kot eno izmed teh sredstev. Podobno ravna tudi ZEPEP, ki politike elektronskega podpisa ne omenja direktno. Seveda je nujno, da obstaja vsaj tehnični del politike, sicer ne bi bilo mogoče ne elektronsko podpisovati ne preverjati podpisov (npr. politika določa kateri algoritmi se uporabljajo za podpisovanje ter zgoščevanje itd.). Za kakršnokoli resnejše elektronsko poslovanje pa bo uporaba politike elektronskega podpisa nujna.

Zakon za elektronsko poslovanje strank politike elektronskega podpisa ne zahteva, torej je njena vsebina (in obstoj) prepuščena volji strank. Pri navadni uporabi elektronskega podpisa (brez politike elektronskega podpisa) zakonodaja in tehnološka infrastruktura (PKI) sicer zagotavljata veljavnost takega podpisa (izvor, nespremenljivost, nezavrnljivost), mnogokrat pa v praksi samo iz tega ni pravno jasno, za kaj (če sploh za kaj) se je hotel podpisnik zavezati. Ni nujno, da bi stranki radi šteli, da je elektronsko podpisana vsebina pravno veljavna, pravzaprav se stranki lahko samo pogovarjata, izmenjujeta mnenja itd. Elektronski podpis se npr. lahko v elektronskem svetu uporablja samo za identifikacijo, da fizično ločeni stranki ugotovita identiteto nasprotne strani in vzpostavita zaupanja vredno (trusted) povezavo. Uporaba elektronskega podpisa tu zato nima zveze z elektronskim poslovanjem v pravnem smislu, se pravi elektronskem sklepanju pogodb. Tudi če bi kakšna od strank v tem primeru sporočila kaj drugi stranki (poleg avtentikacije), se ne bi moglo šteti, da se je hotela kakorkoli pravno zavezati za to (primer, ki se velikokrat navaja je podtaknitev kakšnega sporočila oddaljenemu strežniku, ki se mora identificirati s svojim elektronskim podpisom. Ta elektronsko sporočilo podpiše v dokaz svoje identitete, ne pa seveda, ker bi se hotel kakorkoli zavezati. Slaboverna stranka bi se v takem primeru sicer lahko sklicevala, da gre za pravno veljavno ponudbo). Podobno je, kadar hoče ena stranka drugi poslati samo predlog oz. vzorec nekega dokumenta brez namena, da jo pravno zavezuje. Dokument bo morala v dokaz svoje identitete podpisati, to pa še ne pomeni, da gre za pravno veljavno ponudbo. Po drugi strani pa se seveda elektronski podpis uporablja tudi za pravne posle: elektronske ponudbe, pogodbe itd. Politika elektronskega podpisa se lahko npr. uporablja tudi za označitev pooblastila nosilca elektronskega podpisa (za kakšne posle se lahko zavezuje, do katere višine je veljaven njegov podpis itd.). Zato bo za stranke, ki bodo elektronsko poslovale, priporočljivo, da bodo izdelale ustrezne politike elektronskih podpisov s katerimi bodo jasno določile vsebino in pravno naravo posameznih elektronskih

[1] Če seveda ne štejemo, da takšni standardi že sami po sebi sestavljajo politiko, ki torej obstaja. Politika elektronskega podpisa je ponavadi sestavljena iz pravnega in tehničnega dela.

dejanj oz. sporočil in jih vključile v svoje elektronsko poslovanje.

V odprtih okoljih politike običajno izdelajo imetniki elektronskih podpisov, prejemniki elektronsko podpisanih dokumentov pa jih sprejmejo. V tem primeru je politika elektronskega podpisa ustvarjena samo s strani imetnika elektronskega podpisa in ima naravo splošnih pogojev pogodbe. V zaprtih okoljih pa se stranke vnaprej medsebojno dogovorijo, kakšne politike elektronskega podpisa glede njegovega ustvarjanja in preverjanja bodo sprejele.

Politika elektronskega podpisa je lahko vsebovana v podpisanem dokumentu eksplicitno, lahko pa ta vsebuje samo sklicevanje na politiko, ki je objavljena nekje drugje. V vsakem primeru bo politika določala splošne pogoje veljavnosti elektronskega podpisa in bo imela pravno naravo splošnih pogojev pogodbe, ki jih pri nas ureja 120. člen OZ. Ta med drugim določa, da »*splošni pogoji, ki jih določi en pogodbenik, bodisi da so vsebovani v formularni pogodbi bodisi da se pogodba nanje sklicuje, dopolnjujejo posebne dogovore med pogodbenikoma v isti pogodbi in praviloma zavezujejo tako kot ti».* V kolikor politika oz. splošni pogoji pogodbe niso del podpisanega dokumenta, *»morajo biti objavljeni na običajen način«,*za stranko pa veljajo*,« če so ji bili ob sklenitvi pogodbe znani ali bi ji morali biti znani.«*

Pravno bo zato najvarneje, če bo politika elektronskega podpisa kar del podpisanega dokumenta. Zaradi obsežnosti takih politik pa to tehnično velikokrat ne bo najboljša rešitev, zato bo podpisan dokument vseboval samo sklic na politiko, ki bo ponavadi objavljena na neki spletni strani, se pravi dosegljiva on-line (možna pa je tudi opcija, ko bo npr. politika distribuirana na CD-romih itd.). Vendar bo taka rešitev hkrati nevarnejša za podpisnika, ki jo bo uporabljal, saj bo od njene dejanske dosegljivosti v času verifikacije podpisa odvisno, koliko bo veljala. Zakon namreč govori, da splošni pogoji zavezujejo pogodbeno stranko samo, »če so ji bili ob sklenitvi pogodbe znani ali bi ji morali biti znani«. V primeru nedosegljivost se bo namreč nasprotna stranka lahko upravičeno sklicevala na to, da ji niso mogli biti znani.

6.3. Primer politike elektronskega podpisa za elektronski račun

V nadaljevanju je podan komentar tipična vsebina politike elektronskega podpisa na primeru, ki je trenutno zelo aktualen za slovensko gospodarstvo: izdaje elektronskih računov. Vzorčna politika za izdajo elektronskega računa je podana v prilogi.

V prvem delu politike so podani obvezni elementi politike (enolični identifikator politike, naziv izdajatelja politike, datum izdaje politike, področje uporabe politike ter ožji poslovni kontekst).

V nadaljevanju so podana splošna pravila, ki veljajo za izdajanje elektronskih računov na splošno ter posebna pravila, ki veljajo v specifičnem poslovnem kontekstu izdajanja računov v zvezi z nepremičninami.

6.3.1 Pravna opredelitev izdajanja elektronskih računov

Račun morajo podjetja izdajati po Zakonu o DDV (1. odstavek 33. člena ZDDV, ki pravi »*davčni zavezanec mora za vsak promet blaga oziroma storitev izdati račun ali drug dokument, ki služi kot račun (v nadaljnjem besedilu: račun) ter obdržati kopijo računa*«). Hramba računov je po 57. členu nujna vsaj v obdobju 10 let (za račune v zvezi z nepremičninami 20 let). Pomemben je 5.odstavek 33. člena, ki govori o računih v nematerializirani obliki, kamor sodi tudi elektronska, ki so lahko *»izdani tudi v nematerializirani obliki, če ima davčni zavezanec dovoljenje davčnega organa za takšno obliko izdaje«*.Podobno velja za stran, ki prejme tak račun:*«Davčni zavezanec, ki prejme račun v nematerializirani obliki, mora prav tako imeti dovoljenje davčnega organa, sicer se šteje, da račun ni izdan za namene odbitka vstopnega DDV*«. Zakon v zvezi z nematerializiranimi računi določa v 4. odstavku 57. členu, ki sicer govori o hrambi, še: *"Davčni zavezanec lahko dokumentacijo iz tega člena hrani tudi v elektronski obliki, če je v obdobju iz prvega oziroma drugega odstavka tega člena davčnemu organu zagotovljen dostop do tako shranjenih podatkov brez povzročanja neupravičenih dodatnih stroškov in če so izpolnjeni naslednji pogoji:*
- podatki, vsebovani v elektronskem dokumentu ali zapisu, so dosegljivi in primerni za kasnejšo uporabo, in
-podatki so shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti, in
- iz shranjenega elektronskega sporočila je mogoče ugotoviti, od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema, in

- uporabljena tehnologija in postopki v zadostni meri onemogočajo spremembo ali izbris podatkov, oziroma obstaja zanesljivo jamstvo glede nespremenljivosti podatkov oziroma sporočil."

6.3.2 Podpisniki

Ta del politike določa osebe v organizaciji izdajatelja računa, ki so po svoji funkciji (oz. poslovni vlogi - business role) pooblaščene izstavljati elektronske račune. Politika elektronskega podpisa jim seveda tega pooblastila ne podeljuje, dobijo ga drugje (statutarni zastopniki kot npr. direktor po zakonu, pooblaščenci kot. npr vodja računovodstva po posebnem pooblastilu ali pogodbi o delovnem razmerju). Politika elektronskega podpisa samo določa, kdaj se bo elektronski račun štel za veljavnega: če ga bo izstavila kakšna od oseb v navedenih funkcijah (direktor, finančni direktor ter vodja računovodstva). Če bi ga izstavila kakšna od drugih oseb oz. poslovnih funkcij, ki v politiki ni navedena (četudi bi sicer imela pooblastilo za izdajo računov) in bi se pri tem sklicevala na to politiko (in ne mogoče na kakšno drugo, ki bi štela tak podpis za veljaven), potem se tak elektronski račune ne bi štel za veljavnega. Kar se tiče podpisnikov bi bilo sicer možno tudi, da bi bili ti navedeni poimensko (redko), ali pa sploh ne bi bili navedeni, kar pomeni, da bi se štelo, da je podpisnik lahko kdorkoli, ki je sicer pooblaščen za izdajo računov. Poimenovanje funkcij oz. poslovnih vlog, ki so upravičene do izdaje elektronskih računov je splošnejše kot navedba konkretnih oseb, kar tudi pritiče splošnemu pravnemu aktu, kakršna je politika elektronskega podpisa.

6.3.3 Dokazilo o pooblastilu podpisnikov

Poleg navedbe funkcij, ki lahko izdajajo elektronske račune je potrebno določiti tudi na kakšen način se omenjene osebe identificirajo kot nosilci pooblastil. Vsakršno zatrjevanje obstoja pooblastila je namreč lahko dokazano ali pa zgolj zatrjevano. V primeru samo zatrjevanega pooblastila se postavlja vprašanje kaj se zgodi, če račun izda oseba, ki samo zatrjuje, da ga ima pravico izdati, v primeru dokazanega pooblastila pa se postavi vprašanje, kakšen naj bo ta dokaz. Ena od možnosti glede napačnega zatrjevanja, ki je implicitno sprejeta v predloženem vzorčnem tekstu politike je ta, da je prejemnik računa sam odgovoren za to verifikacijo: če je izdajo računa podpisala oseba, ki v resnici tega pooblastila nima, potem tak račun ni veljaven. Prejemnik računa mora zato sam storiti vse, da ugotovi, kakšna pooblastila ima nasprotna stranka. Kar se tiče drugega vprašanja ga je najlažje rešiti tako, da se elektronskemu računu priloži drug (elektronski) dokument – pooblastilo, ki dokazuje upravičenost podpisnika do izdajanja računov.

V predloženem vzorčnem tekstu za račune, ki jih izdata direktor in finančni direktor velja pravilo zatrjevanega pooblastila; račun namreč ne vsebuje dokumenta, ki bi dokazoval njuna pooblastila. Za veljavnost računa je seveda nujno, da je račun varno elektronsko podpisan ter da podpis spremlja kvalificirano digitalno potrdilo, vendar se tega ne sme zamenjevati s pooblastilom za izdajanje računov; tega pridobi direktor na podlagi zakona z izvolitvijo v direktorsko funkcijo. Če lahko predpostavljamo, da prejemnik računa pozna organizacijo izdajatelja računa, potem je zatrjevano pooblastilo dovolj; če prejemnik računa pozna direktorja podjetja, ki je izdalo račun, potem na podlagi njegovih zakonskih pooblastil lahko sklepa, da je upravičen tudi do izdaje računov.

Glede izdajanja računov s strani vodje računovodstva (ki je lahko notranja vloga v organizaciji ali pa pogodbeni partner) pa je v vzorčnem tekstu prevzeta druga rešitev, namreč dokazano pooblastilo. Ker se ne more pričakovati, da bo prejemnik računa vedno poznal vso osebje izdajatelja računa (npr. računovodstvo), mora v primeru da račun izda vodja računovodstva, tak račun vsebovati tudi varno elektronsko podpisano pooblastilo s strani kakšne od zaupanja vrednih funkcij (direktorja ali finančnega direktorja). V takem primeru bo elektronski račun torej veljaven samo če mu bo priloženo pooblastilo, na katerega se nasprotna stran lahko zanese, se pravi pooblastilo, ki je elektronsko podpisano s strani kakšne od zaupanja vrednih oseb. Seveda mora biti tudi takemu pooblastilu priloženo kvalificirano digitalno potrdilo overitelja kvalificiranih potrdil, ki jamči za identiteto podpisnika. Lahko je določeno še, da mora biti tako pooblastilo izdano v skladu z določeno politiko elektronskega podpisa (npr. politiko, ki se uporablja za podeljevanje pooblastil znotraj organizacije), kot drugod v politiki pa je lahko določeno, kdo mora biti overitelj priloženih kvalificiranih digitalnih potrdil, da se dokument šteje za veljavnega.

6.3.4 Vrsta zaveze (odgovornosti)

Ena najpomembnejših funkcij politike elektronskega podpisa je natančna določitev vrste zaveze (oz. odgovornosti) za katero se uporablja. Kot rečeno je možno elektronski podpis uporabiti v zelo različne namene, od gole identifikacije in

odgovornosti za vsebino do izražanja pravne volje oz. pravnega zavezovanja. Možno je ločiti vsaj naslednje tipe zavez oz. odgovornosti, za katere se uporablja elektronski podpis:

- avtentikacija,
- potrditev sprejema dokumenta,
- avtorstvo oz. odgovornost za vsebino dokumenta
- avtorizacija dokumenta,
- pregled dokumenta,
- notarski zapis itd.

V priloženem dokumentu gre za izdajanje elektronskih računov. Se pravi, gre za izpolnjevanje obveznosti, ki jo pravnim osebam nalaga Zakon o DDV. Račun ima dvojno naravo: po eni strani gre za formalen poziv nasprotni stranki naj plača pogodbeno dogovorjeno vsoto, po drugi strani pa gre za napoved davčnega bremena, se pravi gre za kontrolni dokument, s katerim država ugotavlja davčne obveznosti davčnih zavezancev. V prvem primeru gre torej za izjavo volje (poziv k plačilu), v drugem pa za ugotovitev dejstev (o davčnem bremenu). Kot tak je račun *sui generis* dokument, taka pa je tudi vrsta zaveze, ki mu jo mora podeliti politika elektronskega podpisa. Vzorčni tekst politike se zato sklicuje na 33. člen Zakona o DDV, ki določa obveznost izdajanja računov, hkrati pa določa, da je račun poziv prejemniku računa, naj plača v njem navedeno vsoto.

6.3.5 Časovne omejitve

V primeru pravnih poslov (npr. ponudb) se lahko določi časovna omejitev delovanja take ponudbe, ki vsebuje ali se sklicuje na določeno politiko elektronskega podpisa. V primeru izdaje računov take omejitve ni, saj gre za poziv k plačilu oziroma ugotovitev davčnega bremena. Zakon določa, da je potrebno izdane (in prejete) račune hraniti najmanj 10 let od njihovega nastanka, v primeru računov, ki se nanašajo na nepremičnine pa najmanj 20 let.

6.3.6 Varovanje zaupnih podatkov

Računi ponavadi niso poslovna skrivnost, lahko pa stranka, ki ga izda njegovo vsebino določi za poslovno skrivnost (ta določba seveda nima učinka nasproti državnim organom). V zvezi s to in podobnimi določbami se pojavi zanimivo vprašanje, namreč kakšen pravni učinek ima kršenje takih določb. Medtem ko je namreč jasno, da kršenje določb o pooblastilu podpisnikov in njihovih dokazilih, o časovnih omejitvah, o posebnem dovoljenju za izdajanje elektronskih računov ipd. privede do neveljavnosti samega dokumenta, pa bi bilo npr. pri nespoštovanju varovanja zaupnih podatkov ali pa npr. pri nespoštovanju določb o mirnem reševanju sporov seveda čudno zahtevati, da zaradi tega dokument nima pravne veljave. Tu je zelo pomembno razlikovati med določbami politike podpisa, ki se nanašajo na samo veljavnost podpisanega dokumenta (generiranje, verifikacija, arhiviranje) in določbami, ki pomenijo splošne pogoje poslovanja ene stranke, ki jih druga stranka s sprejetjem dokumenta sprejme. Pri kršitvi prvih bo posledica namreč neveljavnost določenega elektronskega dokumenta, pri kršitvi drugih pa veljavnost dokumenta ne bo prizadeta, pač pa bo šlo za kršitev pogodbenih določil ene stranke, na podlagi česar bo lahko imela nasprotna stranka do nje določene odškodninske zahtevke.

6.3.7 Reševanje sporov

Dobro je določiti, kako se bodo reševali morebitni spori v zvezi s to politiko. Pri tem gre za spore dveh vrst: kot prvo gre za spore v zvezi z določili te politike, kot drugo pa za spore v zvezi s posameznimi posli, ki bodo kot splošne pogoje vključevali ali se sklicevali na to politiko. Na ta način torej politika določa razreševanje sporov, ki se tičejo nje same in tistih, ki se tičejo poslov, nastalih na njeni podlagi.

6.3.8 Vsebina računa

Račun je veljaven samo, če vsebuje vse zakonsko določene sestavine. To predpisuje že sam zakon, tu pa je določba zaradi preglednosti ponovljena.

6.3.9 Dovoljenje DURS za izdajo računov v nematerializirani obliki

5. odstavek 33. člena ZDDV določa, da lahko račune izdaja (in prejema) samo davčni zavezanec, ki ima dovoljenje davčnega organa za takšno obliko izdaje. Zato je nujno, da ima davčni zavezanec, ki hoče take račune izdajati v nematerializirani obliki tako dovoljenje. Za nasprotno stranko pa ni dovolj, da ima izdajatelj računa tako dovoljenje, podobno kot pri pooblastilih bo nasprotna stranka morala za to vedeti, sicer bi se ji lahko zgodilo, da bi za prave račune smatrala račune izdane brez dovoljenja davčnega organa, ki nimajo pravne veljave. Izdajatelj računov lahko prejemniku na različne sporoči, da omenjeno dovoljenje poseduje, najbolj elegantno bo seveda kar s priložitvijo takega dovoljenja v elektronski obliki. Za Davčno upravo RS veljajo določbe ZUPa, ki državnim organom dovoljujejo izdajanje elektronskih odločb. Če bo izdajatelj elektronskega računa pridobil tako elektronsko odločbo, jo bo priložil računu, kar bo dokazilo nasprotni stranki, da je tak račun veljaven.

6.3.10 Prehodno obdobje

Prehodno obdobje (cautionary period) je obdobje po časovnem žigosanju dokumenta (računa) s strani nasprotne stranke v katerem se račun zaradi pravne varnosti (izdajatelja računa) še ne šteje za veljavnega. Če je bilo namreč digitalno potrdilo izdajatelja preklicano, traja nekaj časa preden se preklicano potrdilo pojavi na seznamu preklicanih potrdil (CRL), v tem času pa bi prejemnik tak račun lahko že verificiral. Prehodno obdobje je odvisno od obdobja, v katerem se seznam preklicanih potrdil obnavlja.

6.3.11 Potrdila

Politika elektronskega podpisa lahko določi (kvalificirana) potrdila (med njimi tudi časovne žige, ki so pravzaprav posebna vrsta potrdil), ki jih bosta stranki uporabljali za kreiranje, verificiranje in arhiviranje elektronskih računov. Pri tem lahko stranki določita, da se bodo za sprejemljiva štela tudi potrdila tistih overiteljev, za katere posredno ali neposredno jamčijo v tem členu eksplicitno navedeni overitelji.

6.3.12 Kreiranje elektronskega računa

Politika določa ukrepe, ki jih mora pri kreiranju računa izvesti izdajatelj računa, da se bo ta štel za veljavnega. S pravnega vidika bo moral izdajatelj predvsem zagotoviti, da bo račun:

- vseboval zakonsko določene elemente
- mu bo priloženo kvalificirano digitalno potrdilo, ki bo identificiralo podpisnika,
- mu bo priložena elektronska odločba DURSa, ki izdajatelju dovoljuje izdajanje takih računov,
- mu bodo priložena ustrezna pooblastila podpisnikov.

6.3.13 Verifikacija elektronskega računa

Podobo bo verifikacija določala ukrepe, ki jih bo moral izvesti prejemnik računa oz. njegov verifikator, da se bo prejeti račun štel za veljavnega. Spet gledano z vidika pravne veljavnosti se bo moral verifikator predvsem prepričati, da je račun pravno veljaven, se pravi, da vsebuje vse elemente iz prejšnje točke, ki jih je moral zagotoviti izdajatelj računa.

6.3.14 Arhiviranje elektronskega računa

Arhiviranje je določeno z vidika zakonskih zahtev (4. odstavek 57. člen ZDDV), ki povzemajo določbe ZEPEPa.
Tem bo zadoščeno, če bo stranka, ki želi račune arhivirati (to velja za obe stranki, saj ena hrani izdane, druga pa prejete račune):

- shrani vso verigo potrdil ter ustrezne CRLje oziroma OCSPje v trenutku verifikacije za vsak element računa (račun, potrdila, pooblastila, dovoljenja) ,
- časovno žigosa vso verigo potrdil oz. CRLjev (OCSPjev) za vsak element računa ter
- periodično obnavlja časovne žige na vseh zgoraj naštetih elementih.

Omenjeni postopki so nujni za ohranjanje dolgoročno veljavnosti elektronskih dokumentov.

6.3.15 Elektronski računi v zvezi z nepremičninami

Ta člen vsebuje posebna pravila za račune v zvezi z nepremičninami (ki jih zakon definira kot izročitev novozgrajenih objektov ter prenos stvarnih pravic in deležev na nepremičninah, ki dajejo imetniku lastninsko pravico oziroma pravico posesti na nepremičnini ali delu nepremičnine). Predvsem zanje veljajo 20 letni roki shranjevanja namesto 10 letnih.

7. TERMINOLOŠKI SLOVAR

Elektronski arhiv je celota storitev povezanih s kratkoročnim in dolgoročnim shranjevanjem elektronskih dokumentov in njihovih metapodatkov (kot so avtorji,čas nastanka itd.).

Varen elektronski arhiv je elektronski arhiv, ki vzdržuje metapodatke o shranjenih dokumentih (kot so elektronski podpis, časovni žig itd.), ki dolgoročno zagotavljajo nespremenljivost vsebine shranjenih dokumentov, enolično identifikacijo njihovih avtorjev oz. predložiteljev ter čas njihovega nastanka.

Centraliziran elektronski arhiv je elektronski arhiv, ki poleg dokazil o obstoju in vsebini posameznih dokumentov hrani tudi dokumente same. Na poziv strank mora tak elektronski arhiv strankam predložiti tako posamezne dokumente kot vsa dokazila o njihovem izvoru, istovetnosti in času nastanka.

Decentraliziran elektronski arhiv je elektronski arhiv, ki ne hrani dokumentov, pač pa samo dokazilo o njihovem obstoju in vsebini v določenem časovnem trenutku. Dokumente hranijo stranke same, s pomočjo dokazil iz elektronskega arhiva pa dokazujejo njihov izvor, istovetnost in čas nastanka.

Kratkoročno arhiviranje elektronskih dokumentov pomeni njihovo arhiviranje v roku, ko so vsi podatki za preverjanje elektronskih podpisov dokumentov v arhivu še na voljo 'on-line' (v obliki veljavnih potrdil overiteljev, to se pravi pred njihovim potekom) in ko so hkrati že na voljo podatki o morebitni neveljavnosti takih potrdil (registri CRL oz. odgovori OCSP).

Srednjeročno arhiviranje elektronskih dokumentov pomeni njihovo arhiviranje v roku, ko so nekatera potrdila v verigi potrdil lahko že neveljavna oz. ko nekatere informacije kot so seznam preklicanih potrdil (CRL) niso več na voljo. Pri takem arhiviranju je potrebno hkrati shranjevati celotno verigo certifikatov, podpisano in časovno žigosano še v času njihove veljavnosti.

Dolgoročno arhiviranje elektronskih dokumentov pomeni njihovo arhiviranje v roku, v katerem prenehajo veljati za varne kriptografske metode, ki se uporabljajo za časovno žigosanje dokumentov in metapodatkov v samem arhivu. Pri takem arhiviranju je potrebno periodično, pred potekom veljavnosti prejšnjih časovnih žigov, ponovno časovno žigosati dokumente v arhivu.

Osebni podatki so podatki, ki kažejo na lastnosti, stanja ali razmerja posameznika ne glede na obliko, v kateri so izraženi.

Zaupni podatki so podatki, ki jih kot zaupne določa zakon, pogodba ali konkretni pravni akt državnega organa

Tajni podatki so podatki, ki jih kot tajne določa zakon ali konkretni pravni akt državnega organa

Elektronski podpis so metapodatki v kakršnikoli (elektronski) obliki , ki so dodani obstoječim podatkom in ki pričajo o izvoru teh podatkov.

Varen elektronski podpis so metapodatki, ki so dodani obstoječim podatkom, ali transformacija obstoječih podatkov, ki omogočajo prejemniku podatkov, da preveri njihovo integriteto in izvor.

Časovni žig so metapodatki, ki so dodani obstoječim podatkom, ali transformacija obstoječih podatkov, ki omogočajo prejemniku podatkov, da preveri čas njihovega nastanka.

Podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa

Sredstvo za elektronsko podpisovanje pomenijo nastavljeno programsko ali strojno oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa

Podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa

Sredstva za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa

Potrdilo je z zasebnim ključem overitelja podpisano elektronsko potrdilo, ki jamči, da je javni ključ uporabnika, ki ga potrdilo vsebuje kot enega izmed podpisanih podatkov (poleg imena overitelja, obdobja veljavnosti potrdila, politike potrdila itd.) povezano s tem uporabnikom oz. identificira podpisnika na podlagi njegovega javnega ključa.

Kvalificirano potrdilo je potrdilo, ki izpolnjuje posebne zakonske zahteve glede oblike in vsebine potrdila.

Veriga potrdil (certifikatov) je zaporedje potrdil overiteljev od korenskega potrdila do potrdila overitelja podpisnikovega javnega ključa, ki jamčijo, da podrejeno potrdilo (oz. elektronski podpis uporabnika na koncu verige) pripada podrejenemu overitelju (oz. uporabniku na koncu verige).

CRL (Certificate Revocation List) je seznam preklicanih potrdil s časom preklica, ki ga overitelj objavlja on-line in ki se osvežuje v kratkih, rednih časovnih razmikih.

OCSP (Online Certificate Status Protocol) je s strani overitelja elektronsko podpisana izjava o veljavnosti oz. neveljavnosti določenega potrdila v določenem trenutku.

Politika elektronskega podpisa je množica pravnih in tehničnih pravil za ustvarjanje in preverjanje elektronskega podpisa, ki opredeljujejo pogoje za veljavnost elektronskega podpisa in določajo področje njegove uporabe.

Politika digitalnega potrdila je množica pravil overiteljev digitalnih potrdil, ki se nanašajo na izdajanje digitalnih potrdil in načinov njihove uporabe pri verifikaciji elektronskih podpsov.

Sporazum o elektronskem poslovanju je pogodba med strankami, ki želijo poslovati v elektronski obliki, ki vsebuje določitev načinov elektronskega komuniciranja med strankama ter pogojev za pravno veljavnost take komunikacije.

Elektronska pogodba je pogodba, sklenjena v elektronski obliki, ki se od navadne pogodbe razlikuje v množici pravil glede tolmačenja elektronskih dejanj strank pri njenem sklepanju in izvrševanju.

Viri in literatura

[1] Berčič,B., Bojanec, A., Krkoč, P.,Mrhar, P., Patru, P., Valenčič, I., Šinigoj, A.: Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut za informacijsko varnost, 2003.

[2] Cigoj, S.:Komentar obligacijskih razmerij Veliki komentar zakona o obligacijskih razmerjih, Časopisni zavod Uradni list SR Slovenije,1984-1986

[3] ETSI TR 102 041 V1.1.1 (2002-02) Signature Policies Report

[4] ETSI TR 102 045 V1.1.1 (2003-03) Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model

[5] ETSI TS 101 733 V1.3.1 (2002-02) Electronic signature formats

[6] ETSI TS 101 903 V1.1.1 (2002-02) XML Advanced Electronic Siganture (XadES)

[7] Gospodarska zbornica Slovenije: Skrivnosti elektronskega poslovanja, Priročnik za mala in srednje velika podjetja, Ljubljana, marec 2002

[8] K.U.Leuven: European Electronic Signature Standardization Initiative EESSI Trusted Archival Sources Phase 3 Final Report

[9] Landwell law firms: The implementation of the European Directive On Electronic Signatures Status Report January 2003

[10] LEA 2003: The Law and Electronic Agents Proceedings of the second LEA Workshop, 24th June 2003, In Connection with ICAIL 2003 Conference (Ninth International Conference on Artificial Intelligence and Law), Edinburgh, Soctland,UK

[11] Pavliha M.,Jerman Blažič B. Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem, Založba Gospodarski vestnik, Ljubljana 2002

[12] Šinkovec, J. , Tratar, B.: Obligacijski zakonik s komentarjem in sodno prakso, Založba Oziris, Lesce 2001

[13] W3C: XML-Signature Syntax and Processing W3C Recommendation 12 February 2002

[14] Council of Europe: Convention on Cybercrime, [URL:http://conventions.coe.int]

[15] Direktiva št. 1999/93/EC Evropskega parlamenta in sveta EU z dne 13.decembra 1999 o skupnem okviru Skupnosti za elektronske podpise (Directive 1999/93/EC of the European Parliament and of the Cuncil on Community Framework for Electronic Signatures-2001)

[16] Direktiva št. 2000/31/EC Evropskega parlamenta in sveta EU z dne 8. junija 2000 o določenih pravnih vidikih stroitev informacijske družbe, predvsem elektronskega poslovanja, na notranjem trgu (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market)

[17] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, Bundesgesetzblatt Jahrgang 2001 I/ 22, Bonn, 2001

[18] OZ Obligacijski zakonik, Uradni list RS, št..83/01

[19] Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji, Uradni list Rs, št.99/01

[20] SigG Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, *Bundesgesetzblatt Jahrgang 2001 1/ 22*, Bonn, 2001

[21] Slovenski računovodski standardi, Uradni list RS, št. 107/01 in 67/03

[22] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Uradni list RS, št. 77/00 in 2/01

[23] Uredba o poslovanju organov javne uprave z dokumentarnim gradivom, Uradni list RS, št. 91/01

[24] Vzorčni zakon Komisije Združenih narodov za mednarodno trgovinsko pravo (UNCITRAL) o elektronskem poslovanju iz leta 1996 (Uncitral Model Law on Electronic Commerce – 1996)

[25] Vzorčni zakon Komisije Združenih narodov za mednarodno trgovinsko pravo (UNCITRAL) o elektronskih podpisih iz leta 2001 (UNICTRAL Model Law on Electronic Signatures –2001)

[26] ZAGA Zakon o arhivskem gradivu in arhivih, Uradni List RS, št. 20/97

[27] ZDIZ Zakon o dostopu do informacij javnega značaja ZDIZ, Uradni List RS št. 24/2003

[28] ZEPEP Zakon o elektronskem poslovanju in elektronskem podpisu, Uradni List RS, št. 57/00

[29] ZEPEP-A Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu, Uradni List RS 25-1066/2004

[30] ZGD Zakon o gospodarskih družbah, Uradni list RS, št. 30/93, 29/94, 82/94, 20/98, 84/98, 6/99 in 45/01

[31] ZKP Zakon o kazenskem postopku, Uradni list Rs, št. 63/94, 70/94, 25/96, 5/98, 72/98

[32] ZN Zakon o notariatu, Uradni list RS, št. 13/94, 84/94 in 82/94

[33] ZOR Zakon o obligacijskih razmerjih, Uradni list SFRJ, št. 29/78, 39/85 in 57/89

[34] ZPP Zakon o pravdnem postopku, Uradni list RS, št. 26/99

[35] ZUP Zakon o splošnem upravnem postopku, Uradni list RS, št. 80/99 in 70/00

[36] ZVOP Zakon o varstvu osebnih podatkov, Uradni list RS, št. 59/99 in 57/01

[37] ZVPot Zakon o varstvu potrošnikov, Uradni list RS, št. 20-815/1998, RS 25-1/1998,RS 110-5391/2002