Obvestilo uporabnikom digitalnih kvalificiranih potrdil (certifikatov) overitelja

Agencije za certificiranje NLB

1. UVOD

36. člen Zakona o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001), določa, da mora vsak imetnik digitalnega kvalificiranega potrdila (certifikata), prejeti Obvestilo uporabnikom kvalificiranih potrdil (v nadaljevanju: obvestilo). To obvestilo je namenjeno seznanitvi uporabnika z delovanjem elektronskega podpisa, vključuje pa povzetek notranjih pravil AC NLB in povzetek veljavnih predpisov v Republiki Sloveniji, ki urejajo področje elektronskega poslovanja.

V nadaljevanju vas želimo seznaniti s pojmom ter vlogo elektronskega podpisa in njegovo povezavo s pojmom varnega elektronskega podpisovanja. Prav tako vas želimo seznaniti z veljavnimi predpisi na področju elektronskega poslovanja in elektronskega podpisovanja ter vlogo overitelja AC NLB v infrastrukturi javnih ključev. Na koncu tega obvestila se nahaja seznam dodatnih virov, ki podrobneje pojasnjujejo obravnavano tematiko.

2. ELEKTRONSKI PODPIS

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

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

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

Ena izmed tehnologij elektronskega podpisovanja je digitalni podpis, ki ga ustvarimo in preverjamo s pomočjo šifriranja. Digitalni podpis uporablja asimetrično šifriranje in potrebuje za šifriranje in dešifriranje dva različna ključa. Zaradi tega dejstva je uporaben tako za dokazovanje celovitosti in izvora podatkov kakor tudi za varovanje zaupnosti podatkov.

Ključa, ki se uporabljata za digitalno podpisovanje in se medsebojno dopolnjujeta, sta zasebni ključ in javni ključ. Zasebnega uporablja izključno podpisnik. Z njim ustvari svoj digitalni podpis. Drugi ključ - javni ključ, je navadno poznan širši skupini oseb in ga le-te uporabljajo za preverjanje digitalnega podpisa. Za podpisnika je nujno, da skrbno varuje svoj zasebni ključ, ki ga včasih niti ne pozna. Navadno pozna samo postopek in geslo, ki omogočata, da lahko prebere ključ s pametne kartice ali podobnega varnega medija za shranjevanje podatkov.

V zvezi s tovrstnim šifriranjem se uporablja tudi izraz sistem javnih ključev. Da bi lahko udeleženci elektronskega poslovanja preverili podpisnikov digitalni podpis, mora biti njegov javni ključ dostopen ali posredovan vsakemu od njih. To lahko dosežemo z objavo v posebnih evidencah oziroma imenikih.

Overitelj potrdil izda digitalno potrdilo (certifikat), s katerim poveže javni ključ in ime oziroma naziv imetnika potrdila (podpisnika). Bistvena vloga potrdila v sistemu javnih ključev je vzpostavitev zveze med javnim ključem in določenim podpisnikom.

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

3. POVZETEK VELJAVNIH PREDPISOV IN NOTRANJIH PRAVIL

Hiter tehnološki razvoj in pospešeno uvajanje elektronskega poslovanja ureja Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001, v nadaljevanju ZEPEP) in iz njega izhajajoča Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur. l. RS št. 77/2000, 2/2001, v nadaljevanju uredba). ZEPEP je pravno izenačil elektronsko obliko poslovanja z dosedanjim klasičnim papirnatim poslovanjem, razen v nekaterih primerih za katere je potrebna strožja obličnost in jih ZEPEP posebej našteva. Prav tako je pod posebnimi pogoji elektronskemu podpisu priznal enako veljavo, kot jo ima lastnoročni podpis na papirju ali na kakšnem drugem mediju podobne namembnosti.

ZEPEP in uredba, sta usklajena z določili Modelnega zakona Komisije OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju ter z določili primarne evropske zakonodaje. Prevzemata tudi vse določbe Direktive 1999/93/EC Evropskega parlamenta in sveta EU z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise. ZEPEP in uredba sta torej oblikovana v skladu z načeli, ki so povsem usklajena z načeli evropskih in tudi mednarodnih predpisov.

3.1. POVZETEK VSEBINE ZEPEP IN UREDBE

Splošne določbe ZEPEP

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

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

1. **Elektronski podpis** je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;

2. **Varen elektronski podpis**, je elektronski podpis, ki izpolnjuje štiri predpisane zahteve (povezan je izključno s podpisnikom; iz njega je mogoče zanesljivo ugotoviti podpisnika; ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom; povezan je s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi);

3. **Podatki za elektronsko podpisovanje** so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
4. **Sredstvo za elektronsko podpisovanje** je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;

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

6. **Sredstvo za preverjanje elektronskega podpisa** je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;

7. **Potrdilo** je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.

8. **Overitelj** je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Elektronski podpis

Nihče se ne more sklicevati, da elektronski podpis ni veljaven oziroma nima dokazne vrednosti, samo zaradi tega, ker je v elektronski obliki ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.
Kljub temu, pa nima vsak elektronski podpis enake vrednosti kot lastnoročni podpis, temveč le elektronski podpis overjen s kvalificiranim potrdilom. Iz takega potrdila mora biti razvidno vse kar določa ZEPEP v 28. členu (npr. navedba da gre za kvalificirano potrdilo, ime oziroma psevdonim imetnika potrdila, podatki za preverjanje elektronskega podpisa, začetek in konec veljavnosti potrdila, varen elektronski podpis overitelja, ki je potrdilo izdal,…). Podatke ali sredstva za elektronsko podpisovanje je prepovedano uporabljati brez vednosti podpisnika ali imetnika potrdila.

Kvalificirana potrdila lahko veljajo največ 5 let.

Overitelj, ki izdaja kvalificirana potrdila

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

Overitelj odgovarja vsaki osebi, ki se upravičeno zanaša na kvalificirano potrdilo, ki ga je izdal in daje zagotovilo:

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

V kvalificiranem potrdilu se lahko označi meje uporabnosti ali najvišje transakcijske vrednosti določenega potrdila. Tako overitelj izključi svojo odgovornost za posledice uporabe potrdila izven določenih meja, če so omejitve prepoznavne tretjim osebam.

Osebo, ki zahteva potrdilo, mora overitelj obvestiti o vseh pomembnejših okoliščinah uporabe potrdila in jo identificirati s pomočjo uradnega osebnega dokumenta s fotografijo za fizične osebe oziroma uradno potrjenega dokumenta za pravne osebe še pred sklenitvijo pogodbe.

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

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

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

Nadzorstvo

Inšpekcijsko nadzorstvo nad izvajanjem določb ZEPEP izvaja pristojno ministrstvo.

3.2 POVZETEK NOTRANJIH PRAVIL AC NLB

Overitelj AC NLB sodi med tiste, ki izdajajo kvalificirana potrdila in zato zanj veljajo posebni pogoji glede varovanja infrastrukture, prijavne službe, zaposlenih overitelja, zavarovanja odgovornosti in notranjih pravil. Ti pogoji so strožji in v skladu z ZEPEP. AC NLB je vpisan v register overiteljev RS pod zaporedno številko 3 pri Direkciji Republike Slovenije za poslovno informacijsko središče.

Posebni, strožji pogoji za overitelja kvalificiranih potrdil:

1. **Varovanje infrastrukture** - Overitelj, ki izdaja kvalificirana potrdila, razpolaga pri svojem delu z zaupnimi podatki. Zato mora poleg splošnih pogojev za poslovanje izpolnjevati še strožje, ki od njega terjajo zanesljivejše in temeljitejše postopke varovanja vseh elementov infrastrukture za upravljanje s kvalificiranimi potrdili in izpolnjevanje posebnih varnostnih postopkov za zaposlene;

2. **Prijavna služba** – Predpisani so nekateri dodatni pogoji za prijavno službo overitelja. Tisto službo torej, ki mora sprejeti vlogo bodočega imetnika potrdila in ugotoviti njegovo istovetnost;

3. **Zaposleni pri overitelju** - Zaradi strogih pogojev za delovanje overitelja, ki izdaja kvalificirana potrdila, mora zaposlovati najmanj tri osebe z univerzitetno izobrazbo. Overitelj mora zaradi posebnih zahtev dela zaposliti strokovnjake s področja tehničnih in naravoslovnih smeri, ki morajo imeti najmanj dve leti delovnih izkušenj ter pridobljena še dodatna posebna znanja. Zaposleni pri overitelju morajo imeti, zaradi varnosti, jasno ločena in porazdeljena področja upravljanja s kvalificiranimi potrdili, upravljanja z informacijskih sistemom overitelja in varovanja ter kontrole, ki jih opravljajo;

4. **Zavarovanje odgovornosti** – Ker ZEPEP določa obvezno zavarovanje overiteljeve odgovornosti, je Vlada z uredbo predpisala najnižji znesek te zavarovalne vsote, ki znaša petdeset milijonov tolarjev.;

5. **Notranja pravila overitelja** - Zakon o elektronskem poslovanju in elektronskem podpisu glede ureditve določenih vprašanj pogosto kaže na notranja pravila overiteljev. Vlada je z uredbo predpisala minimalno vsebino teh pravil in s tem minimalni nabor vnaprej predvidljivega obnašanja overiteljev, imetnikov potrdil in tretjih oseb, ki se na potrdila zanašajo. Uredba zato v nekaj členih določa sestavo notranjih pravil overitelja z obveznimi sestavnimi deli ter uvaja v svetu uveljavljeno ločitev notranjih pravil na dva dela – javni in zaupni. Javni del je namenjen seznanitvi imetnikov in tretjih oseb s pravili delovanja overitelja

in predstavlja nekakšne splošne pogoje za uporabo overiteljevih storitev. Zaupni del notranjih pravil vsebuje predvsem določbe o postopkih, ukrepih in varnostnih mehanizmih znotraj overitelja, ki morajo že zaradi svoje narave ostati zaupni in so tako dostopni le zaposlenim overitelja ter nadzornima (inšpekcijskemu in akreditacijskemu) organoma.

Potrdila so namenjena uporabi v specifičnih aplikacijah in za namene, ki jih potrdi in javno objavi AC NLB.

Omogočeno je šifriranje, varno brisanje, digitalno podpisovanje in overjanje identitete podpisnika podatkov ter sporočil v elektronski obliki.

Potrdilo temelji na tehnologiji Entrust. Za podpisovanje potrdil se uporablja algoritem RSA s parom ključev dolžine 1024 bitov, za šifriranje podatkov algoritmi Triple DES, CAST-128 in RC2, (standardi FIPS PUB 81, ANSI X3.106 in ISO/IEC 10116).

Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri overitelju.

Več lahko preberete v Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Ur.l. RS, št. 57/2000, 30/2001) in iz njega izhajajoči Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur. l. RS št. 77/2000, 2/2001).

4. MOREBITNE OMEJITVE UPORABE POTRDILA

Imetnik potrdila lahko digitalno podpiše le dokumente, katerih zahteva po veljavnosti ni daljša od roka veljavnosti potrdila. Če je zahteva po veljavnosti dokumentov daljša od roka veljavnosti potrdila, mora pred potekom veljavnosti potrdila zagotoviti, da bodo takšni dokumenti znova ustrezno podpisani z uporabo novega veljavnega potrdila.

Imetnik potrdila mora prav tako izpolnjevati zahteve iz Javnega dela notranjih pravil AC NLB za kvalificirana digitalna potrdila in veljavnih predpisov. Imetnik potrdila se zavezuje, da bo uporabljal svoj par ključev le v obdobju veljavnosti svojega potrdila.

Imetnik potrdila lahko kadarkoli zahteva vse informacije glede veljavnosti potrdila, glede določb Javnega dela notranjih pravil AC NLB za kvalificirana digitalna potrdila ter glede obvestil AC NLB.

5. PROSTOVOLJNA AKREDITACIJA

ZEPEP v 42. členu dopušča prostovoljno akreditacijo in kot akreditacijski organ pooblasti Agencijo za telekomunikacije. Tako domači kot tuji overitelji, ki dokažejo, da izpolnjujejo vse z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi določene pogoje za svoje delovanje, lahko zahtevajo vpis v register akreditiranih overiteljev. Overitelji, ki so vpisani v register akreditiranih overiteljev, lahko poslujejo z navedbo svoje akreditiranosti ter to dejstvo označijo tudi v izdanih potrdilih.

V Sloveniji za zdaj še ne obstajajo prostovoljno akreditirani overitelji. AC NLB si bo prizadevala pridobiti akreditacijo, ko bo to mogoče.

6. REŠEVANJE PRITOŽB IN MIRNO REŠEVANJE SPOROV

Imetniki lahko vložijo pritožbo pisno ali v elektronski obliki na naslov AC NLB objavljen na spletnih straneh AC NLB. Pritožbe se naslovijo na nadzorno skupino, ki je pristojna za njihovo reševanje. Tričlansko nadzorno skupino sestavljajo strokovnjaki z ustreznimi tehnološkimi in pravnimi znanji, ki ne opravljajo nalog v zvezi z upravljanjem potrdil. Nadzorna skupina je dolžna obvestiti o svoji odločitvi, imetnika kvalificiranega digitalnega potrdila ki se pritoži, v roku 15 dni po prejemu pritožbe na naslov, ki ga imetnik navede v svoji pritožbi. Nadzorna skupina v primeru odkritih pomanjkljivosti odredi

ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je AC NLB dolžan izvesti. Nadzorna skupina nadzoruje izvedbo odrejenih ukrepov.

Imetnik potrdila in AC NLB bosta medsebojne spore reševale sporazumno. Če sporazumna rešitev ne bo mogoča, je za rešitev spora pristojno sodišče v Ljubljani.

7. UKREPI IMETNIKA POTRDILA ZA VARNO ELEKTRONSKO PODPISOVANJE

Imetnik potrdila je dolžan:

- Še pred podpisom naročilnice za potrdilo skrbno prebrati Javni del notranjih pravil AC NLB. Imetnik mora spremljati vsa obvestila AC NLB in ravnati v skladu z njimi.;
- Zaradi varnega dela s potrdil mora imetnik spremljati razvoj tehnologije oziroma slediti obvestilom AC NLB in ustrezno posodabljati potrebno strojno ter programsko opremo;
- Prav tako mora uporabljati programsko opremo, ki jo z obvestili predpiše AC NLB (npr. z dovolj močnimi kriptografskimi moduli);
- Imetnik mora ključ za podpisovanje in vse druge zaupne podatke ščititi s primernim geslom ali na drug način tako, da ima dostop do njih le on;
- če pride do kakršnih koli sprememb, kot so spremembe podatkov, programske opreme in ostalih elementov, ki so kakorkoli povezani s potrdilom, o tem nemudoma obvestiti AC NLB;
- Imetnik mora zahtevati preklic potrdila, če je bil ključ za podpisovanje ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe oziroma, če so se spremenili podatki, ki so navedeni v potrdilu.

8. OPOZORILO O ZMANJŠANI VARNOSTI ELEKTRONSKEGA PODPISA

V skladu s 6. točko drugega odstavka 36. člena ZEPEP je potrebno opozoriti, da bo morda potrebno elektronsko podpisane podatke ponovno elektronsko podpisati preden bo varnost obstoječega elektronskega podpisa s časom zmanjšana.

9. DODATNI VIRI

Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001);

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001).