SKLADNOST HRAMBE ZASEBNIH KLJUČEV NA STROJNEM VARNOSTNEM MODULU Z DIREKTIVO 1999/93/ES IN SLOVENSKO ZAKONODAJO

izdelal: Inštitut za ekonomijo, pravo in informatiko (c), www.iepri.si

1. Uvod

V tem pravnem mnenju so predstavljeni pomembnejši pravni vidiki sistema e-identitet, ki bi se v Sloveniji lahko uvedel z uporabo varnih elektronskih podpisov. Za uvajanje tega sistema so relevantne zahteve zakonodaje glede varnega elektronskega podpisa in zahteve glede sredstev, ki se uporabljajo za varno elektronsko podpisovanje. Poudarek mnenja je na rešitvi (in na skladnosti te rešitve z obstoječo evropsko in domačo zakonodajo), pri kateri bi se vsi zasebni ključi podpisnikov hranili skupaj na namenski napravi - na strojnem varnostnem modulu (angl.: *hardware security module* - HSM).

2. Zakonodajna podlaga

Direktiva Evropskega parlamenta in Sveta 1999/93/ES, z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (Ur. l. L 13, 19/01/2000, v nadaljevanju: Direktiva) v 2. členu opredeljuje napreden elektronski podpis kot elektronski podpis, ki izpolnjuje naslednje zahteve:
(a) povezan je izključno s podpisnikom;
(b) iz njega je mogoče identificirati podpisnika;
(c) ustvarjen je s sredstvi, ki so izključno pod podpisnikovim nadzorom; in
(d) je tako povezan s podatki, na katere se nanaša, da je opazna vsaka kasnejša sprememba teh podatkov.

V Sloveniji je bila navedena zahteva Direktive implementirana v 4. točki 2. člena Zakona o elektronskem poslovanju in elektronskem podpisu (Ur. l. RS, št. 98/2004 – UPB1, v nadaljevanju: ZEPEP), ki v Direktivi imenovan napreden elektronski podpis imenuje varen elektronski podpis in ga opredeljuje kot elektronski podpis, ki izpolnjuje naslednje zahteve:
– da je povezan izključno s podpisnikom;
– da je iz njega mogoče zanesljivo ugotoviti podpisnika;
– da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
– da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

3. Zahteve za varen elektronski podpis

Pri hrambi zasebnih ključev na strojnem varnostnem modulu izpolnjevanje večine zahtev za varen elektronski podpis (tj. zahteve po povezanosti izključno s podpisnikom, zahteve po možnosti zanesljive ugotovitve podpisnika in zahteve po povezanosti s podatki, tako da je opazna vsaka kasnejša sprememba) ni problematično, dvom pa se pojavi glede izpolnjevanja zahteve po izključnem podpisnikovem nadzoru sredstev za podpisovanje, saj podpisnik pri takšni rešitvi nima neposrednega dostopa do modula, na katerem je shranjen njegov zasebni ključ, hkrati pa imajo takšen dostop tretje osebe. Namen zahteve po izključnem podpisnikovem nadzoru (angl.: *sole control*) je podpisniku zagotavljati možnost, da zaščiti

svoje podatke za ustvarjanje elektronskega podpisa pred nepooblaščenim dostopom na takšen način, da lahko izdelavo elektronskega podpisa sproži (oziroma odredi) le on. Vprašanje, ki se pri tem postavi je, ali je mogoče (oziroma dopustno) takšno zaščito zasebnega ključa zagotavljati le z lastno hrambo ključa, ali pa lahko ključ zanj hranijo in varujejo tudi druge osebe na oddaljeni lokaciji.

Če se najprej osredotočimo na besedno razlago dikcije »*izključen nadzor*« oziroma »*sole control*« ugotovimo, da sama po sebi ne izključuje možnosti, da bi se takšen nadzor zagotavljal na daljavo, prav tako tudi ne možnosti, da bi se nadzor zagotavljal preko tretje osebe. Uporabljena dikcija je splošna in pomensko široka, saj govori le o nadzoru, ne pa na primer o neposrednem fizičnem nadzoru. Tudi zahteva izključnosti *a priori* ne onemogoča sodelovanja tretjih oseb, saj lahko takšne osebe delujejo tudi po podpisnikovih navodilih in za njegov račun, kot podaljšana roka podpisnika. Splošnost ubeseditve Direktive je tudi skladna z načelom, da morajo biti zakoni pisani tehnološko nevtralno, s čimer se prepreči nesorazmerno omejevanje načina njihovega izvajanja. Odsotnost izrecne omembe strojnega varnostnega modula torej sama po sebi ne pomeni njegovo neskladnost z Direktivo in ZEPEP, temveč pomeni le določeno mero izvedbene svobode, ki omogoča neomejeno število rešitev, skladnih s postavljenimi pogoji. Ker gre pri interpretaciji zahteve po izključnem nadzoru za vprašanje z razsežnostjo v celotni Evropski uniji (dikcija v ZEPEP ima enak pomen, kot dikcija v Direktivi; isto direktivo so morale implementirati vse države članice EU), lahko odgovor poiščemo tudi na mednarodni ravni.

Forum evropskih nadzornih organov za elektronske podpise (Forum of European Supervisory Authorities for Electronic Signatures - FESA) je v Delovnem dokumentu o naprednih elektronskih podpisih (Working paper on advanced electronic signatures) zapisal, da zahteva po izključnem nadzoru ne pomeni obvezne uporabe posebnih strojnih naprav za izdelovanje podpisov (s čimer so mišljeni na primer USB ključi ali pametne kartice), pomeni pa obvezno uporabo varnostnih ukrepov s strani podpisnika, s katerimi obdrži nadzor nad njegovim ključem. Takšni varnostni ukrepi so na primer enkripcija datoteke, v kateri je shranjen zasebni ključ, omejitev dostopa do naprave za hrambo zasebnega ključa in do datoteke, ki vsebuje ključ. V Javni izjavi o strežniško osnovanih storitvah podpisovanja (Public statement on server based signature services) FESA dalje poudarja, da morata varnostna zasnova in sistemska konfiguracija strežnika zagotavljati, da ima le podpisnik nadzor nad podatki za izdelavo podpisa.

Za razumevanje takšne interpretacije kriterija izključnega nadzora FESA dalje navaja, da v primeru avtomatske izdelave varnega elektronskega podpisa, ki bi ga izdelal podpisnikov strežnik, podpisnik pri izdelavi podpisa ni nujno prisoten ob zasebnem ključu, vendar pa ima nadzor nad varnostnimi ukrepi in odgovornost za izbor ustreznih varnostnih ukrepov. Kadar pa se varen elektronski podpis izdela na oddaljenem strežniku kot storitev, podpisnik ni ne prisoten ob izdelavi podpisa, niti ne more izbrati ustreznih varnostnih ukrepov. Kljub temu pa se lahko podpisnik odloči, ali so varnostni ukrepi, ki jih izvaja ponudnik storitve, zanj ustrezni. Za takšno odločitev mora imeti podpisnik dostop do razumljive oz. doumljive razlage varnostne zasnove sistema, poleg tega pa mora imeti (za pozitivno odločitev) tudi zaupanje, da se bodo varnostni ukrepi v resnici izvajali. Zaupanje se lahko vzpostavi ali okrepi s pregledi, izvedenimi s strani zaupanja vredne tretje osebe (na primer neodvisnega revizijskega strokovnjaka ali nadzornega organa).

Poleg tega mora biti za izpolnjevanje kriterija izključnega nadzora zagotovljena tudi določena kriptografska kakovost algoritmov in podatkov za izdelavo podpisa.

Ob izpolnjevanju zgoraj navedenih pogojev je po mnenju FESA mogoče doseči izključen nadzor in je posledično napredne (varne) elektronske podpise mogoče izdelovati tudi preko oddaljene naprave. V prid takšni interpretaciji govori tudi dejstvo, da je avstrijski zakonodajni organ ob spremembi zakonodaje o elektronskem podpisovanju Evropski Komisiji posredoval pojasnjevalni memorandum, v katerem je zagovarjal stališče, da je izključen nadzor mogoče doseči tudi z drugimi, še posebej tehničnimi in organizacijskimi ukrepi in zato uporaba posebne strojne opreme (na primer USB ključa, pametne kartice) za shranjevanja zasebnega ključa ni potrebna. Memorandum tudi navaja, da so v zadnjih letih enako interpretacijo v praksi podale tudi vse države članice EU, ki so se do tega vprašanja opredelile. Hkrati pa je v memorandumu tudi poudarjeno, da morajo biti v primeru, ko je zasebni ključ shranjen na podatkovnem mediju (ki ni namensko ločen in v posesti podpisnika), zagotovljeni varnostni ukrepi, ki podpisniku omogočajo, da obdrži nadzor nad ključem. Za primere varnostnih ukrepov, tako kot FESA, navaja enkripcijo datoteke, v kateri je shranjen zasebni ključ ter omejitev dostopa do naprave za hrambo zasebnega ključa in do datoteke, ki vsebuje ključ. Pojasnjevalni memorandum je bil s strani Evropske Komisije dobro sprejet in ni spodbudil nadaljnje razprave.

Zaključimo lahko torej, da »*izključen nadzor*« ne pomeni nujno neposrednega dostopa do zasebnega ključa za tvorjenje elektronskih podpisov, prav tako ne pomeni nujno hrambe ključa na posebnem namenskem strojnem mediju. Različni viri priznavajo možnost izpolnjevanja standarda izključnega nadzora pri rešitvah, ki uporabljajo varnostni strojni modul, pri tem pa je hkrati poudarjena tudi zahteva po ustreznem zagotavljanju zaupnosti in varnosti hranjenega zasebnega ključa, na primer s programskimi, strojnimi, organizacijskimi in/ali drugimi rešitvami. Interpretacije, rešitve in predlogi, predstavljeni v tem poglavju, so kljub njihovi navezavi na Direktivo ali na pravne sisteme drugih držav članic relevantni tudi za domač pravni sistem, saj imajo implementirane zahteve Direktive za varen elektronski podpis v ZEZEP enak pomen, kot izvirno besedilo Direktive, zaradi česar se naša ureditev ne razlikuje od ureditev v drugih državah članicah, ki so Direktivo prav tako dosledno implementirale.

4. Naprava oz. sredstvo za varno elektronsko podpisovanje

Naprava za tvorjenje podpisa je skladno z Direktivo oblikovana programska ali strojna oprema za uporabo podatkov v zvezi s tvorjenjem podpisa. Naprava za varno tvorjenje podpisa pa je takšna naprava za tvorjenje podpisa, ki izpolnjuje zahteve iz Priloge III.

V prilogi III Direktive so navedene sledeče navedene zahteve, ki jih mora z ustrezno tehnologijo in postopki zagotavljati naprava za varno tvorjenje podpisa:
(a) se lahko podatki za tvorjenje podpisa, uporabljeni za tvorbo elektronskega podpisa, dejansko pojavijo le enkrat in je njihova tajnost ustrezno zagotovljena;
(b) podatkov za tvorjenje podpisa, uporabljenih za tvorbo elektronskega podpisa, ni mogoče pridobiti z razumno stopnjo zanesljivosti in da je elektronski podpis z uporabo trenutno dostopne tehnologije zaščiten pred ponarejanjem;
(c) lahko zakoniti podpisnik zanesljivo varuje podatke za elektronsko podpisovanje, uporabljene za tvorbo elektronskega podpisa, pred njihovo uporabo s strani drugih.
Naprave za varno tvorjenje podpisa ne smejo spreminjati podatkov, namenjenih podpisovanju, ali preprečiti prikaza teh podatkov podpisniku pred podpisom.

Navedena zahteva je bila implementirana v 1. odstavku 37. člena ZEPEP:
Sredstva za varno elektronsko podpisovanje morajo z uporabo ustreznih postopkov in infrastrukture zagotavljati naslednje:
1. podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena;
2. podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa, elektronski podpis pa je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije;
3. podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom.
Sredstvo za varno elektronsko podpisovanje ne sme spremeniti podatkov, ki se podpisujejo, ali preprečiti prikaza podatkov podpisniku pred podpisom.

Izmed zgoraj navedenih zahtev je z vidika hrambe zasebnih ključev na strojnem varnostnem modulu relevantna predvsem zahteva, da mora biti podpisniku omogočeno zanesljivo varovanje njegovih podatkov za elektronsko podpisovanje. FESA v Javni izjavi o strežniško osnovanih storitvah podpisovanja glede te zahteve poudarja, da morajo biti avtentikacijski podatki zaščiteni vse od uporabniškega vmesnika, do strežnika. Vsa komunikacija med podpisnikom in strežnikom mora biti torej izvedena preko zaupnih kanalov. Upravljavec strežnika poleg tega avtentikacijskih podatkov ne sme shraniti na način, ki bi omogočal zlorabo teh podatkov s strani njegovih zaposlenih ali tretjih oseb.

Podobne zahteve podaja tudi CEN Workshop Agreement 14169 (CWA 14169), referenčni dokument Evropskega odbora za standardizacijo (Comité européen de normalisation - CEN), ki govori o napravah za izdelovanje podpisov. Dokument sicer ni uraden standard, vsebuje pa dobre prakse s tega področja. CWA 14169 postavlja zahtevo po zaupni poti (angl.: *trusted path*) za avtentikacijo uporabnika, kadar uporabniškega vmesnika ne zagotavlja naprava za izdelavo varnega podpisa. Postavlja tudi zahtevo po zaupnem kanalu med aplikacijo za izdelavo podpisa in napravo za izdelavo varnega podpisa. Zakonodaja sicer ne zahteva upoštevanja navedenega ali drugih standardov, vendar pa lahko organ, ki preverja skladnost naprav za varno elektronsko podpisovanje z zakonodajo (skladno s 4. točko 3. člena Direktive skladnost naprav za varno elektronsko podpisovanje z zahtevami iz Priloge III ugotavljajo pristojni javni ali zasebni organi, ki jih imenujejo države članice) te standarde upošteva.

V času izdaje CWA 14169 (marec 2004), prav tako tudi v času izdaje Javne izjave o strežniško osnovanih storitvah podpisovanja (oktober 2005) nobena strežniško osnovana rešitev podpisovanja ni bila overjena kot naprava za varno tvorjenje podpisa. Ob upoštevanju dejstva, da pristojni organi večine držav članic za ugotovitev skladnosti z Direktivo postavljajo stroge pogoje (na primer certificiranje po standardih) je FESA v Javni izjavi izrazila dvom, da bo v bližnji prihodnosti prišlo do uporabe takšnih rešitev. Kljub temu se rešitev s strojnim varnostnim modulom v EU danes že uporablja (Avstrija), nekatere države pa o tem razmišljajo (na primer Romunija). Pri tem velja poudariti, da je bila avstrijska rešitev uvedena z veliko mero skrbnosti za varovanje podatkov za elektronsko podpisovanje (točka c priloge III Direktive). Avstrijski HSM strežnik se tako nahaja v visoko varovanem območju, v sefu, do katerega ima dostop samo varnostno osebje.

Skladno z navedenim je ob izpolnjevanju relativno strogih pogojev tudi strojni varnostni modul lahko naprava za varno elektronsko podpisovanje.