ID-kaardi turvarisk
Õiguslikud probleemid

Kristiina Laanest (Riigi Infosüsteemi Amet)
Laura Kask (Majandus- ja Kommunikatsiooniministeerium)

2017 Tallinn

Sisukord

Sissejuhatus 3
Sertifikaatide kehtivuse peatamine ja kehtetuks tunnistamine 4
Sertifikaadid isikut tõendava dokumendi osana 4
Sertifikaatide kehtivuse peatamine 5
Tingimused 5
Teavitamine 8
E-allkirjade kehtivus sertifikaatide kehtivuse peatamise korral 9
Kvalifitseeritud e-allkirjade kehtivus 9
Järelevalve 11
MsÜS ja HOS järelevalve 12
Vastutus 14
Teise isiku sertifikaatide kasutamine 14
Riigivastutus 15
Lepinguline vastutus 16

Sissejuhatus

2017. aasta augusti lõpus avastati ID-kaardil oleva protsessorkiibi riistvara juhtprogrammi (inglise keeles *firmware*) krüpteerimisvõtmete genereerimise funktsioonis turvarisk, mis seisneb selles, et elektrooniliseks isiku tuvastamiseks ja digitaalseks allkirjastamiseks vajalikust avalikust krüpteerimisvõtmest on võimalik piisava arvutusvõimekuse olemasolu korral välja arvutada kasutaja privaatvõti. Selle tulemusel on võimalik elektrooniliselt isikut tuvastada ja anda digitaalallkirja ilma ID-kaardil olevale kiibile juurdepääsu omamata ning PIN-koode teadmata, st kasutada ID-kaarti elektroonilises keskkonnas ilma selle omaniku teadmiseta.

Turvarisk puudutab kõiki alates 2014. aasta 16. oktoobrist väljastatud isikutunnistusi, samuti elamisloakaarte ja digitaalseid isikutunnistusi ning e-residendi isikutunnistusi (edaspidi ID-kaart). Mobiil-ID ja enne 2014. aasta 16. oktoobrit väljastatud ID-kaardid turvanõrkusest puudutatud ei ole.

Käesolev analüüs lahkab ID-kaardi turvariskiga seotud õiguslikke küsimusi lähtuvalt kehtivast õigusest. Analüüs ei kajasta pooltevahelistest lepingutest tulenevaid detaile, kuivõrd analüüsi eesmärk on välja selgitada kehtiva õiguse kitsaskohad hindamaks valdkondliku regulatsiooni muutmisvajadust.

Valdkondlik regulatsioon:

Õigusaktid

- Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (eIDAS);
- Isikut tõendavate dokumentide seadus (ITDS);
- E-identimise ja e-tehingute usaldusteenuste seadus (EUTS);
- Hädaolukorra seadus (HOS);
- Majandustegevuse seadustiku üldosa seadus (MsÜS);
- Tsiviilseadustiku üldosa seadus (TsÜS);
- Karistusseadustik (KarS).

Hea tava

- Sertifitseerimispõhimõtted, mis kirjeldavad SK ID Solutions AS (SK) tegevust Eesti Vabariigi poolt välja antavale isikutunnistusele (ID-kaart), elamisloakaardile (EL-kaart), digitaalsele isikutunnistusele (Digi-ID) ja Mobiil-ID vormis digitaalsele isikutunnistusele kvalifitseeritud e-allkirja ja e-identimist võimaldavate sertifikaatide väljastamisel ja teenindamisel (kehtiv alates 01.11.2016).

Sertifikaatide kehtivuse peatamine ja kehtetuks tunnistamine

EUTS § 17 lõike 1 kohaselt võib olla sertifikaatide kehtivuse peatamise üheks ajendiks kahtlus, et sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaja nõusolekuta. Analoogselt on EUTS § 19 lõike 4 punkti 2 kohaselt alus sertifikaadi kehtetuks tunnistamiseks sertifikaadis nimetatud avalikule võtmele vastava privaatvõtme kasutamise võimalus ilma sertifikaadi omaja nõusolekuta.

ITDS § 9^5 viitab sertifikaatide kehtivuse peatamise osas EUTS-is sätestatud üldregulatsioonile. Sertifikaatide kehtetuks tunnistamine on aga reguleeritud ITDS §-s 9^6, mille lõike 2 punkti 3 kohaselt võib dokumendi väljaandja sertifikaadi kehtetuks tunnistada, kui on põhjendatud alus arvata, et sertifikaadis nimetatud avalikule võtmele vastavat privaatvõtit on võimalik kasutada dokumendi kasutaja nõusolekuta.

Arvestades ID-kaardi turvariski olemust ja probleemi lahendusvõimalusi on otstarbekas esmajärjekorras sertifikaatide kehtivus peatada.

Kui sertifikaatide kehtivus on peatatud ei ole võimalik nende sertifikaatidega e-allkirju ega e-templeid anda, mis omakorda tähendab seda, et sel ajal ei ole võimalik sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit sertifikaadi omaja nõusolekuta kasutada. Ühtlasi on erinevalt sertifikaatide kehtetuks tunnistamisest võimalik EUTS §-s 18 sätestatud tingimustel peatatud sertifikaadi kehtivus taastada. Usaldusteenuse osutaja taastab peatatud sertifikaadi kehtivuse peatamist nõudnud asutuse taotluse alusel kehtivuse taastamise andmete kandmisega usaldusteenuse osutaja peetavasse sertifikaatide andmebaasi. Eelnenud protsessile võib järgneda sertifikaadi kehtetuks tunnistamine ITDS §-s 9^6 ja EUTS §-s 19 sätestatud korras.[1] Sertifikaatide kehtivuse peatamine ise ei saa olla viimane toiming, sellele peab järgnema kehtivuse taastamine või kehtetuks tunnistamine.

Eeltooduga kooskõlas toimuks ka turvariskiga ID-kaartide uuendamisprotsess, mille puhul on võimalik esmalt peatada dokumenti kantud sertifikaatide kehtivus, seejärel taastada sertifikaatide kehtivus tarkvara uuendamiseks, millele omakorda järgneb vanade sertifikaatide kehtetuks tunnistamine ja uute sertifikaatide dokumenti kandmine.

Sertifikaadid isikut tõendava dokumendi osana

ITDS § 9 lõige 5 sätestab, et dokumenti võib kanda digitaalset isiku tuvastamist võimaldavat informatsiooni, sealhulgas digitaalset tuvastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ja digitaalset allkirjastamist võimaldavat informatsiooni, sealhulgas digitaalset allkirjastamist võimaldavat krüptograafilist võtit ning sellele vastavat sertifikaati ning teisi digitaalseid andmeid.

Vastavalt ITDS § 9^4 lõikele 1 annab dokumenti kantava digitaalset tuvastamist võimaldava sertifikaadi ja digitaalset allkirjastamist võimaldava sertifikaadi välja dokumendi väljaandja. Dokumendi väljaandjad on ITDS § 12^1 lõike 1 kohaselt Politsei- ja Piirivalveamet ning Välisministeerium.

[1] EUTS § 19 lõike 5 kohaselt lähtutakse isikut tõendavate dokumentide seaduse § 2 lõikes 2 nimetatud dokumendile kantud sertifikaadi kehtetuks tunnistamisel isikut tõendavate dokumentide seaduses sätestatust.

Dokumendi väljaandja võib ITDS § 9^4 lõike 3 kohaselt dokumenti kantava sertifikaadi väljaandmiseks anda lepingu alusel üle kohustusi e-identimise ja e-tehingute usaldusteenuste seaduse nõuete kohasesse usaldusnimekirja kantud kvalifitseeritud usaldusteenuse osutajale. Lisaks võib dokumendi väljaandja ITDS § 9^4 lõike 4 alusel dokumenti kantava digitaalset tuvastamist võimaldava sertifikaadi tehnilise moodustamise anda lepingu alusel üle sellealast pädevust omavale teenuse osutajale.

Eeltooduga kooskõlas hõlmab 2010. a Politsei- ja Piirivalveameti ja Gemalto AG vahel sõlmitud leping lisaks ID-1 formaadis dokumentide plankide ja isikustamise teenuse tellimisele sertifitseerimisteenuse osutamist.

Samas on kohustuste üleandmise puhuks seadusandja ette näinud piirangud: isikut tõendava dokumendi väljaandmise, kehtivuse peatamise ja kehtetuks tunnistamise otsuse tegemise pädevust ei või ITDS § 3^1 lõike 3 kohaselt halduslepinguga üle anda. Antud juhul ei esine selgusetust isikut tõendava dokumendi väljaandmise pädevuse määratlemisel. Küll aga võib-olla vaieldav, kas vastavalt EUTS § 17 lõikele 1 on dokumenti kantud sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise otsuse pädev tegema üksnes dokumendi väljaandja või on vastav otsustusõigus teatud juhtudel ka usaldusteenuse osutajal. Võimalike vaidluste ennetamiseks ja tõlgendamisprobleemide ületamiseks tuleks kaaluda eelkirjeldatud seadusandja tahte konkretiseerimist.

Järelevalvet halduslepingu täitmise üle teostavad vastavalt ITDS § 3^1 lõikele 4 Siseministeerium ja valdkonna eest vastutava ministri volitusel Politsei- ja Piirivalveamet. Eeldatavasti peaks järelevalve hõlmama ka kontrolli, kas kohustuste lepinguga üleandmine on olnud õiguspärane. Käesoleval juhul ei ole põhjust kahelda kõnealuse lepingu puhul ITDS § 3^1 lõikes 3 nimetatud piirangute järgimises.

Sertifikaatide kehtivuse peatamine

Tingimused

ITDS § 9^5 kohaselt võib dokumendi väljaandja isikut tõendavasse dokumenti kantud sertifikaadi kehtivuse peatada ning peatatud kehtivusega sertifikaadi kehtivuse taastada EUTS §-des 17 ja 18 sätestatud tingimustel. Seega on Politsei- ja Piirivalveamet ning Välisministeerium kohustatud sertifikaatide kehtivuse peatamisel juhinduma EUTS-is sätestatud tingimustest.

EUTS reguleerib e-identimist ja e-tehinguteks vajalikke usaldusteenuseid ulatuses, milles need ei ole reguleeritud eIDAS määruses. eIDAS määruse artikli 28 kohaselt kohaldatakse e-allkirja kvalifitseeritud sertifikaatide ajutisele peatamisele siseriiklikku regulatsiooni, kui see on kehtestatud. Sertifikaadi ajutine peatamine toob eIDAS määruse kohaselt kaasa sertifikaadi kehtetuse vastaval ajavahemikul. Ühtlasi peab eIDAS määruse kohaselt olema sertifikaadi kehtivuse peatamise ajavahemik sertifikaatide andmebaasis selgesti märgitud ja sertifikaatide staatuse kohta teavet andva teenuse kaudu peab saama peatamise ajavahemikul teavet peatamisstaatuse kohta.

EUTS-is on sertifikaatide kehtivuse peatamisega seonduv reguleeritud §-des 17–18 ja §-s 21. EUTS § 17 lõike 1 kohaselt on usaldusteenuse osutajal õigus peatada usaldusteenuse sertifikaadi kehtivus, kui tekib kahtlus, et sertifikaati on kantud valeandmed või sertifikaadis

sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaja nõusolekuta. Usaldusteenuse osutaja käesoleval juhul on SK ID Solutions AS.

Lähtudes erinormi ITDS § 9^5 ja üldnormi EUTS § 17 lõike 1 koosmõjust ning arvestades, et ITDS § 9^5 kohaselt tuleb sertifikaadi kehtivuse peatamisel juhinduda EUTS §-s 17 sätestatud tingimustest, tuleb asuda seisukohale, et sertifikaadi kehtivuse peatamise diskretsiooniotsuse saab vastu võtta dokumendi väljaandja, kui tekib kahtlus sertifikaati kantud andmete õigsuses või kui kolmandal isikul on võimalik privaatvõti välja arvutada ja seda kasutada sertifikaadi omaja nõusolekuta.

EUTS § 17 lõike 2 kohaselt on usaldusteenuse osutaja kohustatud sertifikaadi kehtivuse peatama, kui seda taotleb sertifikaadi omaja, pädev asutus, infoturbe pädev astutus või Andmekaitse Inspektsioon või kohus, prokuratuur või kriminaalasjas kohtueelne uurimisasutus süüteo tõkestamiseks. EUTS § 17 lõige 2 ei näe ette kaalutlusruumi, vaid sätestab imperatiivse sertifikaadi peatamise kohustuse eelloetletud asutuste vastavasisulise nõude esitamise korral. Seega võib Riigi Infosüsteemi Amet (infoturbe pädev asutus) ja Tehnilise Järelevalve Amet (pädev asutus) EUTS § 17 lõike 2 alusel esitada nõude sertifikaatide kehtivuse peatamiseks otse SK ID Solutions AS-ile.[2] Nõude esitamisele peaks aga eelnema vähem intensiivne reageerimismeede, antud juhul vastavasisulise ettepanekuga dokumendi väljaandja poole pöördumine, et dokumendi väljaandja saaks esmajärjekorras olukorra ise lahendada.

Kuigi ITDS § 9^5 viitab dokumendi väljaandja diskretsiooniotsuse tegemise aluseks olevate tingimuste puhul EUTS §-le 17 tervikuna, ei ole võimalik rakendada § 17 lõiget 2 üldnormina ITDS § 9^5 suhtes ja asuda seisukohale, et hoolimata pädeva asutuse seaduspärasest ettekirjutusest usaldusteenuse osutajale, on dokumendi väljaandjal täiendav kaalutlusruum sertifikaatide kehtivuse peatamise otsustuse langetamiseks. Sisuliselt on EUTS § 17 lõikes 2 sätestatud volitusnormi puhul tegemist pädeva asutuse poolt riikliku järelevalve meetme kohaldamisega usaldusteenuse osutaja kui konkreetsel juhul avaliku korra eest vastutava isiku suhtes ning dokumendi väljaandjal puudub õigus otsustada, kas kohustatud isik peab ettekirjutuse täitma või mitte. Eeltoodu ei piira aga dokumendi väljaandja õigust võtta koostöös usaldusteenuse osutajaga asjakohased meetmed ise kasutusele enne järelevalveasutuse sekkumist.

Vastavalt EUTS § 17 lõikele 3 peab usaldusteenuse osutaja pärast sertifikaadi kehtivuse peatamist viivitamata kandma andmed kehtivuse peatamise kohta enda peetavasse sertifikaatide andmebaasi ning pidama arvestust sertifikaadi kehtivuse peatamise aja, aluse ja taotleja ning peatatuse lõpetamise kohta. eIDAS määruse kohaselt on õiguskindluse huvides, et sertifikaadi peatatud staatus oleks alati selgesti märgitud. Seetõttu peaks usaldusteenuse osutajad olema kohustatud selgelt märkima sertifikaadi staatuse ja selle peatamise korral täpse ajavahemiku, mille jooksul sertifikaat on peatatud.

Järelikult, kui usaldusteenuse osutaja sertifikaatide kehtivuse peatab, tuleb igal juhul kindlaks määrata konkreetne ajavahemik, mille jooksul sertifikaadid peatatud on. Samas ei tulene õigusaktidest, milliste ajaühikute kaudu peab sertifikaatide peatatuse periood olema

[2] Kuigi EUTS § 17 lg 2 punkti 3 kohaselt võib sertifikaadi peatamist taotleda ka kohus, prokuratuur või kriminaalasjas kohtueelne uurimisasutus süüteo tõkestamiseks, ei ole viimatinimetatud asutuste pädevuste analüüsimine ID-kaardi turvariski olemust arvestades käesoleval ajal otstarbekas, sest juhtum ei ole seotud süüteo tõkestamisega.

määratletud.[3] Seetõttu ei näi olevat ebaõige ka olukord, mille puhul peatamise periood loetakse lõppenuks konkreetse sündmuse saabumisega – kauguuendamise protseduuri alustamisega. Vastav tähtaeg on võimalik välja tuua juba sertifikaatide peatamise aluseks oleva otsuse tegemise ajal.

Lisaks peatamise perioodile tuleb ära määratleda sertifikaatide kehtivuse peatamise alus. Arvestades, et peatamine on aktuaalne olukorras, kus sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaja nõusolekuta, on peatamise otsustust õigustava alusena asjakohane viidata EUTS § 17 lõikes 1 kirjeldatud juhtumi realiseerumisele.

Vastavalt ITDS § 9 lõikele 5 kantakse dokumenti kaks sertifikaati:

1) digitaalset tuvastamist võimaldav krüptograafiline võti ning sellele vastav sertifikaat;
2) digitaalset allkirjastamist võimaldav krüptograafiline võti ning sellele vastav sertifikaat.

Kui dokumendi väljaandja ITDS § 9^5 kohaselt isikut tõendavasse dokumenti kantud sertifikaadi kehtivuse peatab ning peatatud kehtivusega sertifikaadi kehtivuse taastab EUTS §-des 17 ja 18 sätestatud tingimustel, tekib küsimus, kas ja millises ulatuses on ITDS § 9^5 kohaldatav, kui võtta arvesse, et nii EUTS kui ka eIDAS määrus reguleerivad üksnes digitaalset allkirjastamist võimaldavate sertifikaatide kehtivuse küsimusi. Tõsi, kui asuda seisukohale, et sertifikaatide kehtivuse peatamise tingimuste osas saabki dokumendi väljaandja tugineda eelkõige EUTS § 17 lõikele 1, on selles nimetatud eeldused sertifikaatide kehtivuse peatamise korral täidetavad mõlemat tüüpi sertifikaadi puhul. Seega on võimalik tõlgendada ITDS § 9^5 ja EUTS § 17 lõiget 1 nii, et dokumendi väljaandjal on õigus peatada nii digitaalset tuvastamist võimaldava sertifikaadi kui ka digitaalset allkirjastamist võimaldava sertifikaadi kehtivus, kui tekib kahtlus, et sertifikaati on kantud valeandmed või sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada sertifikaadi omaja nõusolekuta.

EUTS § 17 lõiked 2–6 reguleerivad siiski konkreetselt usaldusteenustega seonduvat, mistõttu saab nii järelevalveasutuste poolne sekkumisõigus kui ka usaldusteenuse osutajale pandud kohustused kohalduda niivõrd, kuivõrd see puudutab digitaalset allkirjastamist võimaldavate sertifikaatide kehtivuse peatamise küsimusi. Eelnev aga ei tähenda, et digitaalset isikutuvastamist võimaldavate sertifikaatide kehtivuse osas puuduksid sekkumismehhanismid üldse, sest kaarditootja ning Politsei- ja Piirivalveameti vahel sõlmitud lepingu üle teostavad järelevalvet vastavalt ITDS § 3^1 lõikele 4 Siseministeerium ja valdkonna eest vastutava ministri volitusel Politsei- ja Piirivalveamet. Lisaks võivad pooled lepingus täpsustada pooltevahelisi sertifikaatide kehtivuse peatamisega seonduvaid kohustusi. Kuigi Politsei- ja Piirivalveametil puudub otsene leping usaldusteenuse osutajaga, vastutab kaarditootja lepinguliste kohustuste täitmise eest, olgugi et kohustuste täitmiseks võib olla tal omakorda sõlmitud leping usaldusteenuse osutajaga.

Lähtuvalt ITDS § 3^1 lõikest 3 ei või isikut tõendava dokumendi väljaandmise, kehtivuse peatamise ja kehtetuks tunnistamise otsuse tegemise pädevust halduslepinguga üle anda. Kas eeltoodud ITDS § 3^1 lõikes 3 toodud loetelu hõlmab ka õigust otsustada sertifikaatide kehtivuse üle, jääb ebaselgeks. Kui eelnevale küsimusele on vastus jaatav, saabki sertifikaatide kehtivuse peatamise osas otsuse langetada üksnes dokumendi väljaandja ja ITDS § 3^1 lõike 3 erisus

[3] Tsiviilseadustiku üldosa seaduse (TsÜS) § 134 lõike 2 kohaselt määratakse tähtaeg aastate, kuude, nädalate, päevade, tundide või väiksemate ajaühikute või kindlalt saabuva sündmusega.

koosmõjus §-ga 9^5 on ülimuslikum võrreldes EUTS § 17 lõikega 1, milles vastav õigus nähakse ette usaldusteenuse osutajale.

Kui ITDS § 3^1 lõike 3 kohaselt võib sertifikaatide kehtivuse peatamise üle otsustada usaldusteenuse osutaja asemel dokumendi väljaandja, tekib küsimus, kuidas kohaldada antud erisust kooskõlas eIDAS määruse artikliga 24, mille kohaselt on usaldusteenuse osutajal muuhulgas kohustus kasutada usaldusväärseid süsteeme ja tooteid, mis on kaitstud muutmise eest, ja tagada neid süsteeme ja tooteid toetatavate toimingute tehniline turvalisus ja usaldusväärsus. eIDAS määruse artikli 28 kohaselt kehtestatakse kvalifitseeritud e-allkirja andmist võimaldavate sertifikaatide kehtivuse peatamise täpsemad reeglid liikmesriigi siseriikliku õigusega. Eesti seadusandja otsused ei või aga erisuste kehtestamisel kaasa tuua olukorda, mille puhul eIDAS määruses sätestatud tingimusi ei ole võimalik täita. Järelikult: isegi kui usaldusteenuse osutajal puudub ITDS § 3^1 lõikest 3 tulenevalt autonoomne õigus otsustada sertifikaatide kehtivuse peatamise üle, peab dokumendi väljaandja tegema koostööd usaldusteenuse osutajaga, et vastava otsustuse tegemisel oleks täidetud eIDAS määruse artikliga 24 usaldusteenuse osutajale pandud kohustused. Teisisõnu peab sertifikaatide kehtivuse peatamist tingiva olukorra esinemisel dokumendi väljaandja astuma viivitamatult samme selleks, et otsus sertifikaatide kehtivuse peatamiseks võimalikult kiiresti langetada, misjärel saaks usaldusteenuse osutaja korraldada sertifikaatide kehtivuse tehnilise peatamise.

Teavitamine

Usaldusteenuse osutaja peab EUTS § 17 lõike 4 kohaselt teavitama sertifikaadi kehtivuse peatamisest viivitamata sertifikaadi omajat. Kuidas sertifikaadi omaja teavitamine toimub, ei ole EUTS-is reguleeritud.

Haldusmenetluses on oluline eristada isiku teavitamist dokumendi kättetoimetamisest, millest viimase suhtes kehtivad konkreetsed tingimused. Haldusmenetluses kehtib vormivabaduse põhimõte, kui seaduse või seaduse alusel kehtestatud määrusega ei ole sätestatud teisiti (haldusmenetluse seadus § 5 lõige 1). Vabas vormis isiku teavitamine on lubatud ka vastavalt HMS § 25 lõikele 3. Avaliku korra eest vastutava isiku poolsete teavituste tegemisele ei sätesta vorminõudeid ka korrakaitseseadus.

Sertifikaatide kehtivuse masspeatamise korral on tehniliselt keeruline teavitada viivitamatult personaalselt sertifikaatide peatamise toimingust kõiki isikuid. Teavituste edastamine igale isikule võib hinnanguliselt aega võtta nädalaid. ID-kaardi laialdase kasutusala tõttu on oluline valida meetod, mis võimaldaks peatamisest teavitada koheselt igaühte. Eeltoodust lähtuvalt näib antud olukorras otstarbekas korraldada isikute teavitamine massimeediavahendite kaudu, et täita esmalt EUTS § 17 lõikes 4 sätestatud „viivitamatu teavitamise“ nõue.

Täitmaks konkreetse isiku teavitamise nõuet, tuleks lisaks avalikkusele edastatud teatele saata teade igale sertifikaadi omajale, kes saab personaalse teate kätte vastavalt tehnilistele võimalustele. Edaspidi tuleks aga täiendavalt analüüsida, kas sertifikaatide kehtivuse peatamisest teavitamine peaks toimuma mingis kindlas vormis, kas taoliste masspeatamiste puhuks tuleks sätestada eriregulatsioon, eelkõige peatamisest teavitamisele, ning kas on võimalik arendada tehniline lahendus, mille kaudu saaks igaühte vajaduse korral operatiivselt teavitada.

E-allkirjade kehtivus sertifikaatide kehtivuse peatamise korral

E-allkirju liigitatakse eIDAS määruse artikli 3 punktide 10–12 kohaselt kolmeks:

- e-allkiri – elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida allkirja andja kasutab allkirja andmiseks;
- täiustatud e-allkiri – e-allkiri, mis vastab artiklis 26 sätestatud nõuetele;
  - täiustatud e-allkirja alla kuulub täiustatud e-allkiri kvalifitseeritud sertifikaadiga, mis erineb kvalifitseeritud e-allkirjast vaid selle poolest, et seda ei anta turvalise ehk sertifitseeritud e-allkirja andmise vahendiga.
- kvalifitseeritud e-allkiri – täiustatud e-allkiri, mis antakse kvalifitseeritud e-allkirja andmise vahendi abil ja mis põhineb e-allkirja kvalifitseeritud sertifikaadil.

ID-kaardi turvariski valguses saame rääkida üksnes kvalifitseeritud e-allkirjadest, sest Eesti ID-kaardiga saab anda kvalifitseeritud e-allkirju. Ka ei puuduta turvarisk peale ID-kaardi teiste vahenditega antud e-allkirju. Alternatiivselt saab Eestis kvalifitseeritud e-allkirju anda mobiil-ID-ga. Täiustatud e-allkirju saab anda näiteks smart-ID-ga.

Kuivõrd ID-kaardi turvarisk puudutab üksnes peale 2014. a välja antud ID-kaardi abil antud kvalifitseeritud e-allkirju, ei analüüsita alljärgnevalt turvariskist puutumata ID-kaartide ja mobiil-ID abil antud kvalifitseeritud allkirjadega seotud küsimusi. Ühtlasi ei puuduta probleem muus kui kvalifitseeritud e-allkirja formaadis antud (sh täiustatud) e-allkirju, mistõttu ei hõlma alljärgnev ka madalama tasemega e-allkirju.

Kvalifitseeritud e-allkirjade kehtivus

Kvalifitseeritud e-allkirja kehtimiseks peavad olema täidetud eIDAS määruse artikli 3 punktis 12 toodud eeldused. eIDAS määruse artikli 25 kohaselt on kvalifitseeritud e-allkirjal käsitsi kirjutatud allkirjaga samaväärne õiguslik toime, st kvalifitseeritud e-allkiri on võrdväärne omakäelise allkirjaga. EUTS § 24 lõike 1 üleminekusätte kohaselt loetakse Eesti õiguses digitaalallkirja all tuntud e-allkirjad vastavaks kvalifitseeritud e-allkirjale eIDAS mõttes.

E-allkirja kvalifitseeritud sertifikaat peab olema allkirja andmise ajal kehtiv. Vastavalt EUTS § 17 lõikele 5 on sertifikaadi kehtivuse peatatuse ajal antud e-allkiri või e-tempel kehtetu. Seega on kõik ID-kaardiga antud kvalifitseeritud e-allkirjad sertifikaatide kehtivuse peatamiseni kehtivad, olenemata sellest, kas e-allkiri on antud nn turvariskiga kaardiga või mitte.

eIDAS määruse artikli 25 kohaselt ei tunnistata e-allkirja õiguslikult kehtetuks ega kohtumenetlustes tõenduskõlbmatuks ainuüksi seetõttu, et see on elektroonilisel kujul või ei vasta kvalifitseeritud e-allkirjadele esitatavatele nõuetele.

Selleks, et seada kahtluse alla, kas isik on oma tahteavalduse esitanud e-allkirja andes, tuleb hinnata isiku poolt tehtud kõiki samme tahteavalduse esitamisel tervikuna. Isik, kes väidab, et e-allkiri ei väljenda tema tegelikku tahet, peab tõendama väite tõesust (näiteks tellima allkirjaekspertiisi).

Tsiviilkohtumenetluse seadustiku (TsMS) § 277 lõike 3 kohaselt saab digitaalallkirjaga varustatud elektroonilise dokumendi ehtsust vaidlustada üksnes asjaolude põhistamisega, mille põhjal võib eeldada, et dokumenti ei ole koostanud digitaalallkirja omaja. See kehtib ka sellise elektroonilise dokumendi kohta, mis on koostatud muul turvalisel viisil, mis võimaldab

tuvastada koostaja ja koostamise aja.Tuginedes üldisele tehingu vormivabaduse põhimõttele võivad pooled tehingu vormis, sh millise tasemega e-allkirja tahteavalduse esitamiseks nõutakse, kokku leppida. Samuti võib digitaalallkirja kasutamise vajadus tuleneda seaduses sätestatud tehingu vorminõudest (näiteks tarbijakäendusleping – VÕS § 144 lg 2). Valdavalt on tsiviilõiguslike lepingute puhul aga nõutav lepingu sõlmimine kirjalikku taasesitamist võimaldavas vormis, mille puhul võib tahteavalduse esitada ka täiustatud e-allkirjaga.

Rangemad reeglid on kehtestatud tahteavalduse esitamisele haldusmenetluses, kohtuvälises menetluses ja kohtumenetluses, kus elektroonilises asjaajamises nõutakse kvalifitseeritud e-allkirja kasutamist (HMS § 14 lg 4, 27 lg 1; KrMS § 160^3 lg 2; VTMS § 51 lg 2; TsMS § 336, 338 lg 1 p 8, § 441 jne). Arvestada tuleb, et haldusakti kehtetuks tunnistamist ei saa nõuda üksnes põhjusel, et haldusakti andmisel rikuti menetlusnõudeid või et haldusakt ei vasta vorminõuetele, kui eelnimetatud rikkumised ei võinud mõjutada asja otsustamist (HMS § 58).

Kohtupraktikas on aga asutud seisukohale, et vähemasti sunnivahendit ettenägevate aktide puhul on allkirjastamine akti kehtivuse vältimatu eeldus ning allkirja puudumise korral on akt tühine ehk kehtetu algusest peale. Riigikohtu halduskolleegium märkis 22. veebruari 2006. aasta otsuses haldusasjas nr 3-3-1-71-05 (p 10) järgmist: „Allkirjastamise nõue ei ole pelgalt akti vormi küsimus. Riigikohtu halduskolleegium leiab, et allkiri tõendab, et haldusakt on antud ning selle on andnud akti allkirjastanud isik. Sunnivahendi kohaldamisel, kui seadus näeb ette kirjaliku haldusakti andmise kohustuse, ei või haldusorgan oma tahet väljendada teisiti kui kirjaliku allkirjastatud haldusaktiga.“ Kokkuvõtteks leidis kolleegium, et allkirjastamata karistusotsust on põhjust käsitada tühise haldusaktina, sest see ei ole sundtäidetav ja selle täitmist ei või akti adressaadilt nõuda. Kuigi HMS-i § 63 haldusakti allkirjastamata jätmist selle tühisuse aluseks ei pea, vastab allkirjastamata karistusotsus oma olemuselt tühise haldusakti tunnustele.[4] Kas haldusakti või karistusotsuse elektroonilise allkirjastamise korral nõutavast kvalifitseeritud e-allkirja tasemest madalama e-allkirjaga toob kaasa akti või otsuse tühisuse, jääb kohtupraktika kujundada.

HMS § 14 lõike 4 kohaselt peab elektrooniliselt edastatud taotlusele lisatud olema digitaalallkiri ning vajaduse korral digitaalne tempel. Digitaalallkirja puudumine taotlusel võib olla alus anda taotluse esitajale tähtaeg puuduste kõrvaldamiseks kooskõlas HMS §-ga 15.

Kvalifitseeritud e-allkirja andmise vahendite nimekiri

Enne eIDAS määruse jõustumist esitas Majandus- ja Kommunikatsiooniministeerium (MKM) digitaalallkirja seaduse (edaspidi DAS) ja e-allkirja direktiivi alusel Eestis kasutusel olevate turvaliste e-allkirja andmise vahendite loetelu Euroopa Komisjoni peetavasse nimekirja.[5] Sel ajal ei nõutud nende vahendite sertifitseerimist klassikaliste sertifitseerimisasutuste poolt. Vahendite turvanõuetele vastavuse kinnitamine oli DAS-i ja e-allkirja direktiivi kohaselt liikmesriigi vastava asutuse pädevuses. Turvalisuse hinnangu andmisel kasutati vahendite komponentidele väljastatud sertifikaate, kättesaadavat tehnilist infot ja pädevaid eksperte. Selline praktika toimis kuni 01.07.2016 (eIDAS määruse üleminekuprotsess).

eIDAS määruse art 51 (üleminekumeetmed) sätestab, et selliseid turvalisi allkirja andmise vahendeid, mille vastavus on direktiivi 1999/93/EÜ artikli 3 lõike 4 kohaselt kindlaks määratud,

[4] Saarmets, V. „Kuidas sünnib õigusakt, haldusakt, kohtulahend?“, Õiguskeel 2008/3.
[5] Liikmesriikide turvaliste e-allkirja andmise vahendite nimekiri (Compilation of Member States notification on SSCDs and QSCDs): https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

käsitatakse käesoleva määruse kohaselt kvalifitseeritud e-allkirja andmise vahenditena. Üleminekumeede tähendab seda, et liikmesriigid esitasid nimekirja oma senised eelnevalt kehtinud e-allkirja direktiivi nõuetele vastavad vahendid, ilma et nende puhul oleks eelnevalt tarvis läbida eIDAS määruse kohast sertifitseerimisprotsessi. Taoline nimekirja kandmine oli võimalik kuni 1.07.2016. Üleminekumeede võimaldas teenuste järjepidevat toimimist, aeganõudev ja kulukas eIDAS sertifitseerimisprotsess võinuks kaasa tuua katkestusi teenuste toimimises.

E-allkirja andmise vahendite turvalisuse nõuetele vastavuse hindamine oli liikmesriikide sobivate avalik-õiguslike või eraõiguslike organite pädevuses.[6]

Alates eIDAS määruse jõustumisest on võimalik uusi vahendeid nimekirja lisada peale sertifitseerimisprotsessi läbimist pädeva asutuse poolt, nt ANSI, BSI. Eestis selline asutus puudub. Sertifitseerimisprotsess võtab aega hinnanguliselt 6–12 kuud.

Kui ID-kaardi tehnilises lahenduses uuendamise protseduuriga tehtavad muudatused on minimaalsed, on endiselt tegemist sama, juba nimekirja kantud e-allkirja andmise vahendiga. Suuremate muudatuste korral tuleb paratamatult läbida aeganõudev sertifitseerimisprotsess või võtta kasutusele mõne teise liikmesriigi poolt nimekirja kantud vahend. Viimane on aeganõudev, kuna eeldab suures mahus täiendavaid arendustöid ja koosvõime tekitamist.

eIDAS määruse kohaselt ei ole võimalik teistel osapooltel (sh ENISA-l) nimekirja kantud vahendeid sellest välja arvata. Nimekirja esitatud vahend on kehtiv seni, kuni MKM vahendit nimekirjast ise ei eemalda. Sellegipoolest saavad välised osapooled esitada arvamusi nimekirja kantud e-allkirja andmise vahendite turvalisuse kohta.

Järelevalve

Usaldusteenuse osutajale näeb eIDAS määrus (eelkõige artikkel 19) ette ranged turvanõuded. Kvalifitseeritud usaldusteenuse osutaja peab võtma asjakohased tehnilised ja korralduslikud meetmed, et ohjata osutatavate usaldusteenuste turvalisusega seotud riske. Tehnoloogia viimaseid arenguid arvesse võttes tagatakse nende meetmetega riski astmele vastav turvalisuse tase. Eelkõige võetakse meetmeid turvaintsidentide vältimiseks ja nende mõju minimeerimiseks ning sidusrühmade teavitamiseks intsidentide kahjulikust mõjust. Kui turvarikkumisel või tervikluse kaol on tõenäoliselt kahjulik mõju füüsilisele või juriidilisele isikule, kellele usaldusteenus on osutatud, teavitab usaldusteenuse osutaja põhjendamatu viivituseta ka füüsilist või juriidilist isikut turvarikkumisest või tervikluse kaost.

EUTS § 4 kohaselt on usaldusteenuse osutaja kohustatud teavitama infoturbe pädevat asutust eIDAS määruse artikli 19 lõike 2 kohasest turvaintsidendist viivitamata, kuid mitte hiljem kui 24 tunni jooksul pärast sellest teadasaamist.

EUTS § 2 lg 4 kohaselt täidab eIDAS määruse artiklis 19 sätestatud järelevalveasutuse ülesandeid Riigi Infosüsteemi Amet. Muus osas laienevad eIDAS määruses sätestatud järelevalveülesanded Tehnilise Järelevalve Ametile (EUTS § 2 lg 3).

[6] Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta (EÜT L 13, 19.1.2000, lk 12—20).

Kui see on asjakohane ja eelkõige juhul, kui turvarikkumine või tervikluse kadu hõlmab kahte või enamat liikmesriiki, peab RIA EUTS § 2 lg 4 ja eIDAS määruse artikli 19 lõike 2 kohaselt turvarikkumisest teavitama teiste asjaomaste liikmesriikide järelevalveasutusi ning ENISA-t. Kui turvarikkumise või tervikluse kao avalikustamine on avalikes huvides, võib RIA teavitada üldsust või nõuda üldsuse teavitamist asjaomaselt usaldusteenuse osutajalt.

MsÜS ja HOS järelevalve

EUTS § 1 lg 4 kohaselt kohaldatakse usaldusteenuse osutaja majandustegevuse alustamisele, teostamisele ja lõppemisele majandustegevuse seadustiku üldosa seadust (MsÜS). HOS § 36 lg 1 p 8 kohaselt on elektrooniline isikutuvastamine ja digitaalne allkirjastamine elutähtsad teenused. ITDS § 9^4 lõike 3^1 kohaselt on ITDS-i alusel välja antud dokumentidele kantud sertifikaadiga digitaalset tuvastamist ja digitaalset allkirjastamist võimaldava sertifitseerimisteenuse osutaja HOS § 36 lõike 1 punktis 8 nimetatud elutähtsa teenuse osutaja. MsÜS § 5 lõike 3 kohaselt on elutähtsat teenust osutav ettevõtja üldist majandushuvi pakkuva teenuse osutaja (üldhuviteenuse osutaja). Seega on usaldusteenuse osutaja ühtlasi elutähtsa teenuse osutaja ja üldhuviteenuse osutaja.

HOS § 38 lõike 3 kohaselt on elutähtsa teenuse osutaja kohustatud tagama hädaolukorra või muu sarnase olukorra ajal, sealhulgas tehnilise rikke ning tarne ja teise elutähtsa teenuse katkestuse korral, enda osutatava teenuse järjepideva toimimise ja kiire taastamise võime.

MsÜS § 35 sätestab üldhuviteenuse toimepidevuse tagamise. MsÜS § 35 lõike 1 kohaselt peab üldhuviteenuse osutaja, kes soovib vähemalt osaliselt või ajutiselt loobuda üldhuviteenuse osutamisest, sealhulgas loobuda üldhuviteenuse osutamisest seda takistavate asjaolude olemasolu tõttu, teatama majandushaldusasutusele (antud juhul Tehnilise Järelevalve Ametile (edaspidi TJA)) sellest vähemalt kolm kuud ette. Sama paragrahvi lõike 2 kohaselt tagab üldhuviteenuse osutamisest loobumisel majandushaldusasutus üldhuviteenuse osutaja klientidele teenuse toimepidevuse. Kui üldhuviteenuse osutaja loobumise ajaks mujalt teenuse saamine on võimatu või ebamõistlikult kulukas, võib majandushaldusasutus teha üldhuviteenuse osutajale ettekirjutuse üldhuviteenuse osutamise jätkamiseks. Sama paragrahvi lõike 3 kohaselt võib jätkamise ettekirjutusega üldhuviteenuse osutajat kohustada jätkama üldhuviteenuse osutamist pärast kavandatud loobumise tähtaega senistel tingimustel või võimaluse korral ettekirjutuses märgitud tingimustel, mis on ettevõtjale senistest vähem koormavad. Ettekirjutusega määratud jätkamise kohustuse tähtaeg võib olla kuni üheksa kuud, arvates ettevõtja poolt üldhuviteenuse osutamise loobumise kavatsusest teatamisest või sellise kavatsuse muul viisil majandushaldusasutusele teatavaks saamisest. Sama paragrahvi lõike 6 kohaselt on asjaomaseks majandushaldusasutuseks loakohustusega tegevusalal majandushaldusasutus, kes on pädev tegevusloa andmiseks, muul tegevusalal aga majandushaldusasutus, kes on pädev määrama ettevõtja tegevuspiirkonna või lõpetama ettevõtjaga üldhuviteenuse osutamiseks sõlmitud lepingu.

MsÜS § 35 lg 5 kohaselt on üldhuviteenuse osutajal õigus nõuda teenuse jätkamise ettekirjutuse täitmisest tingitud kahju hüvitamist, kui tema poolt üldhuviteenuse osutamisest loobumine ei olnud vastuolus temale seadusest, haldusaktist või lepingust tulenevate kohustustega.

Kui usaldusteenuse osutajal on kohustus loobuda digitaalset allkirjastamist võimaldava sertifikaadi osas teatud tingimustel usaldusteenuse osutamisest ja TJA kohustab ettekirjutusega teenuse osutamist jätkama, on usaldusteenuse osutajal õigus nõuda ettekirjutuse jätkamisest tingitud kahju hüvitamist. Selline olukord võib tekkida, kui usaldusteenuse osutaja ja TJA on

erinevatel seisukohtadel, kas esinevad asjaolud, mis vältimatult tingiksid sertifikaatide peatamise. Kui usaldusteenuse osutaja jätkab TJA ettekirjutuse alusel teenuse osutamist ega peata sertifikaate, siis on usaldusteenuse osutajal õigus nõuda sellest tuleneva kahju hüvitamist.

Usaldusteenuse osutaja on usaldusteenuse osutamisel seotud sertifitseerimisauditiga. Audiitori ülesanne on pidevalt teha ülevaate auditeid, mis kinnitab usaldusteenuse osutaja vastavust eIDAS määruse nõuetele. Kuigi eIDAS määruse järgi on kohustus auditeerida kord 24 kuu jooksul (artikkel 20 (1)), võib TJA nõuda vastavushindamise teostamist kinnituse saamiseks, et kvalifitseeritud usaldusteenuse osutaja ja osutatav kvalifitseeritud usaldusteenus vastab eIDAS määruses sätestatud nõuetele (artikkel 20 (2)).

Lisaks on usaldusteenuse osutajal kohustus oma audiitori ees olla kogu teenuse osutamise aja nõuetele vastav. Juhul, kui usaldusteenuse osutaja audiitorid leiavad, et risk on realiseerunud, mistõttu on usaldusteenuse osutajal kohustus sertifikaadid peatada või kehtetuks tunnistada ning SK ei täida audiitori nõuet (TJA teenuse osutamise jätkamist nõudva ettekirjutuse tõttu), on audiitoritel õigus võtta tagasi teenuse vastavussertifikaat ning teha TJAle kui usaldusnimekirja pidajale ettepanek teenuse usaldusnimekirjast eemaldamiseks.

Vastavussertifikaat on kõigil ESTEID_SK alt välja antud kvalifitseeritud e-allkirjade sertifikaatidel ja sertifitseerimisteenustel. Seega ei ole küsimus vaid konkreetse usaldusteenuse kvalifitseerituse kaotamises, vaid selles, et usaldusteenuse osutaja võidakse üldse usaldusnimekirjast eemaldada (st kõik ESTEID-SK alt osutatavad teenused sh riiklik mobiil-ID eemaldatakse usaldusnimekirjast).

Kui vastavushindamisest ilmneb ja sellega on üheselt tõendatud, et digitaalset allkirjastamist võimaldav sertifikaat ei vasta kvalifitseeritud e-allkirjale esitatavatele nõuetele eIDAS määruse mõistes ja TJA kohustab usaldusteenuse osutajat jätkama teenuse osutamist, ei ole enam tegemist kvalifitseeritud e-allkirjaga, mida teised ELi liikmesriigid sellisena tunnustaksid. Seega oleks võimalik nende kasutamine üksnes Eesti siseselt. Samas ei oleks ka siseriiklikult tegemist enam omakäelise allkirjaga võrdväärse digitaalse allkirjaga.

Seega, kui on üheselt tõendatud, et digitaalset allkirjastamist võimaldav sertifikaat ei vasta kvalifitseeritud e-allkirjale esitatavatele nõuetele eIDAS määruse mõistes, ei ole võimalik käsitleda allkirja võrdväärsena omakäelise allkirjaga, kuna kvalifitseeritud e-allkirja võrdväärsus omakäelise allkirjaga on reguleeritud eIDAS määruse artikli 25 (2) kohaselt, millele viitab ka EUTS § 24 lg 1.

Kuna isikutuvastamist võimaldav sertifikaat ning selle peatamine või tühistamine allub ITDS-ile ning eIDAS määrus seda ei reguleeri, võib kohustada usaldusteenuse osutajat ettekirjutusega hoidma autentimist võimaldavat sertifikaati lühiajaliselt kehtivana, sest osa e-teenuseid, mis ei nõua kvalifitseeritud e-allkirja, töötavad.

Tulenevalt eeltoodust on kvalifitseeritud usaldusteenuse osutaja, kellele dokumendi väljaandja on lepingu alusel kohustusi andnud, kohustatud arvestama sertifikaatide kehtetuks tunnistamise kaalumisel ka üldhuviteenuse osutaja ja elutähtsa teenuse osutaja kohustustega ning vajadusel on võimalik teha talle ka ettekirjutus teenuse osutamise jätkamiseks kuni üheksaks kuuks. Üldhuviteenuse osutajal on õigus nõuda teenuse jätkamise ettekirjutuse täitmisest tingitud kahju hüvitamist, kui tema poolt üldhuviteenuse osutamisest loobumine ei olnud vastuolus temale õigusaktidest tulenevate kohustustega. Siiski võib sellise ettekirjutuse tegemisel ohtu sattuda terve Eesti autentimist ja allkirjastamist võimaldav ökosüsteem, kuna

vastavussertifikaat teenuse osutamiseks on kõigi ESTEID_SK alt välja antud dokumentide sertifikaatide osas.

Vastutus

ID-kaardi turvariskiga seoses saab mõjutatud ja puudutatud osapooli arvestades eristada mitmetasandilist vastutust.

Teise isiku sertifikaatide kasutamine

Teise isiku identiteedi ebaseaduslik kasutamine on KarS § 157^2 kohaselt kuritegu. Teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

Juhul kui saadakse ligi kirjavahetusele, võib olla kohaldatav ka sõnumisaladuse rikkumise kvalifikatsioon. Kirjavahetuse ja sidevahendi abil edastatud sõnumi saladuse rikkumise eest karistatakse vastavalt KarS §-le 156 rahalise karistusega.

Kui e-teenuse osutaja ei võta kasutusele piisavaid turvameetmeid isikuandmete kaitseks, näiteks lisaks ID-kaardiga autentimisele täiendavat autentimisviisi, võib aset leida KarS § 157^1 kvalifitseeritud süüteo toimepanemine. Delikaatsete isikuandmete ebaseadusliku avaldamise või neile ebaseadusliku juurdepääsu võimaldamise eest karistatakse rahatrahviga kuni 300 trahviühikut. Sama teo eest, kui see on toime pandud omakasu eesmärgil või kui sellega on tekitatud teisele isikule kahju, karistatakse rahalise karistuse või kuni üheaastase vangistusega. Seega võib olenevalt olukorrast tegemist olla kas väär- või kuriteoga.

Ühtlasi võib avalikule teenusele juurdepääsu võimaldamine ja seeläbi isikuandmete kättesaadavaks tegemine volitamata isikule olla liigitatav isikuandmete ebaseadusliku avaldamise alla (Kars § 157). Kutse- või ametitegevuses teatavaks saanud isikuandmete ebaseadusliku avaldamise eest isiku poolt, kellel oli seadusest tulenev kohustus andmeid mitte avaldada, ja kui puudub käesoleva seadustiku §-s 157^1 sätestatud süüteokoosseis, karistatakse rahatrahviga kuni 300 trahviühikut.

Kui infosüsteemi andmetes tehakse volitamata juurdepääsu tõttu muudatusi, võib olla tegemist KarS § 206 sätestatud arvutiandmetesse sekkumisega. Arvutisüsteemis olevate andmete ebaseadusliku muutmise, kustutamise, rikkumise või sulustamise eest karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.

KarS § 216^1 sätestab koosseisu arvutikuriteo ettevalmistamisele. Seadme või arvutiprogrammi, mis on loodud või kohandatud eelkõige KarS §-s 206, 207, 213 või 217 sätestatud kuritegude toimepanemiseks, või kaitsevahendi, mille abil on võimalik hankida juurdepääs arvutisüsteemile, hankimise, valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, et panna ise või võimaldada kolmandal isikul panna toime KarS §-s 206, 207, 213 või 217 sätestatud kuritegu, karistatakse rahalise karistuse või kuni kaheaastase vangistusega.

KarS § 217 sätestab koosseisu arvutisüsteemile ebaseaduslikult juurdepääsu hankimise eest. Arvutisüsteemile ebaseaduslikult juurdepääsu hankimise eest kaitsevahendi kõrvaldamise või vältimise teel karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. Sama teo eest, kui sellega on tekitatud oluline kahju või kui juurdepääs on hangitud riigisaladust, salastatud välisteavet või ainult ametialaseks kasutamiseks ettenähtud andmeid sisaldavale arvutisüsteemile või kui juurdepääs on hangitud elutähtsa valdkonna arvutisüsteemile, karistatakse rahalise karistuse või kuni viieaastase vangistusega.

Kaasneda võib ka muid väär- ja kuriteokoosseise, samuti tsiviilõiguslikke vaidlusi olenevalt sellest, millised tagajärjed teise isiku identiteedi volitamata töötlemine võib kaasa tuua.

Riigivastutus

Riigivastutus baseerub igaühe põhiõigusel nõuda talle ükskõik kelle poolt õigusvastaselt tekitatud moraalse ja materiaalse kahju hüvitamist (Eesti Vabariigi põhiseadus § 25). Põhiõiguse kui ennekõike riiki kohustava õigusena on § 25 esemeks avaliku võimu kandjate vastutus enda tegevusega kaasnenud õigusrikkumiste, sh sellega põhjustatud kahju eest.[7]

Kui toiminguga rikutakse isiku õigusi, võib isik haldusmenetluse seaduse (HMS) § 109 kohaselt nõuda haldusorganilt või kohtult toimingu ärajätmist või lõpetamist ning toimingu tagajärgede kõrvaldamist ja kahju hüvitamist vastavalt riigivastutuse seadusele ning pöörduda selleks halduskohtusse halduskohtumenetluse seadustikus ettenähtud korras.

Riigivastutuse seaduse (RVastS) § 7 lõike 1 kohaselt võib isik, kelle õigusi on avaliku võimu kandja õigusvastase tegevusega avalik-õiguslikus suhtes rikkunud, nõuda talle tekitatud kahju hüvitamist, kui kahju ei olnud võimalik vältida ega ole võimalik kõrvaldada haldusakti kehtetuks tunnistamise, toimingu lõpetamise või haldusakti andmise või toimingu sooritamisega. Sama paragrahvi lõike 2 kohaselt võib tegevusetusega tekitatud kahju hüvitamist nõuda üksnes juhul, kui haldusakt jäi õigeaegselt andmata või toiming õigeaegselt sooritamata ja sellega rikuti isiku õigusi.

RVastS reguleerib seega nii kahju hüvitamist kui ka muul viisil rikutud õiguste taastamist või heastamist, samuti rikkumise ärahoidmist avalik-õiguslikes suhetes. Ühtlasi on tähelepanuväärne, et RVastS § 7 lõikes 1 sätestatud kahju hüvitamise eeldus on riigi poolse tegevuse õigusvastasus. Samas, RVastS § 7 lõikes 2 sätestatud tegevusetusega tekitatud kahju hüvitamise puhul õigusvastasuse eeldus puudub.

RVastS ei erista avaliku võimu kandja lepingulist vastutust. Avalik-õigusliku lepingu (halduslepingu) rikkumisega tekitatud kahju kuulub hüvitamisele RVastS kohaselt üldistel alustel. Analoogia alusel võib paralleelselt rakendada VÕS lepingulise vastutuse sätteid (RVastS § 7 lg 4, HMS § 105 lg 1).[8]

Hüvitamisnõude esmaseks tingimuseks on kahju tekkimine hüvitise nõudjal. Kahju hüvitamiseks ei anna alust see, et õigusvastaselt käitunud isik on saanud kasu, kui hüvitise nõudja ei ole samal ajal kandnud kahju. Kahju on ühe isiku õigushüve vähenemine teise isiku

[7] Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, § 25 kommentaarid. Kättesaadav: http://www.pohiseadus.ee/index.php?sid=1&ptid=30&p=25.
[8] Samas.

teo tulemusena. Säärane hüve võib olla elu, tervis, kehaline puutumatus, au, väärikus, privaatsus, elukeskkond, vara jne.

Lepinguline vastutus

Politsei- ja Piirivalveameti ning kaarditootja vaheline vastutus on kokku lepitud 2010. a poolte vahel sõlmitud ID-1 formaadis dokumentide plankide, isikustamise ning sertifitseerimisteenuse osutamise lepingus.