

Majandus- ja taristuministri määruse „Usaldusnimekirja kinnitamiseks kasutatav avalik võti ja sellele vastava privaatvõtme kasutusala“ muutmise eelnõu seletuskiri

1. Sissejuhatus

Määrus kehtestatakse e-identimise ja e-tehingute usaldusteenuste seaduse § 15 lõike 4 alusel.

Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93 EÜ (ET 28.08.2014 L 257/73) (edaspidi *eIDAS määrus*) rakendus alates 01.07.2016 ja sellega loodi üleeuroopaline usaldusteenuste (e-allkiri, e-tempel jt) regulatsioon. Vastavalt eIDAS määrusele peavad liikmesriigid kvalifitseeritud usaldusteenuste ja nende osutajate kohta usaldusnimekirju. Usaldusnimekirjadesse võivad liikmesriigid kanda ka kvalifitseerimata usaldusteenuseid ja nende osutajaid, kui riigisisene õigus seda ette näeb.

Usaldusnimekirjad on masinloetavad ning neid kasutatakse usaldusteenuste usaldusväärsuse automatiseeritud kontrolliks. Seetõttu on ette nähtud, et usaldusnimekirjad kaitstakse krüptograafiliselt e-allkirja või e-templiga. Vastavat privaatvõtit hoitakse usaldusnimekirja pidaja valduses ning sellele vastav avalik võti tehakse avalikuks usaldusväärsusest allikast, milleks antud juhul on käesolev määrus. Käesoleva määruse eesmärgiks on määrata usaldusnimekirja kinnitamiseks (krüptograafiliseks kaitsmiseks) kasutatava privaatvõtme kasutusala ning kinnitada sellele privaatvõtmele vastav avalik võti. Määruse eesmärk on uuendada võtmepaari, et kasutada uuendatud ja turvalisemaid tehnoloogiaid. Varasem võtmepaar oli kasutuses aasta.

Määruse eelnõu ja seletuskirja koostasid Majandus- ja Kommunikatsiooniministeeriumi riigi infosüsteemide osakonna nõunik Laura Kask (tel: 639 7645, e-post: laura.kask@mkm.ee) ja Majandus- ja Kommunikatsiooniministeeriumi nõunik Mait Heidelberg (tel: 639 7613, e-post: mait.heidelberg@mkm.ee).

Eelnõu juriidilist kvaliteeti kontrollis Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Anne-Ly Normak (tel 715 3403, e-post: anne-ly.normak@mkm.ee) ja keeleteoimetuse tegi Kristiane Liivoja (tel: 625 6370, e-post: kristiane.liivoja@mkm.ee).

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb ühest paragrahvist.

Eelnõu punkt 1 kinnitab avaliku võtme võtmepaarist, mida kasutatakse usaldusnimekirja kinnitamiseks. Vastavalt e-identimise ja e-tehingute usaldusteenuste seaduse § 15 lõikele 3 korraldab valdkonna eest vastutav minister käskkirjaga usaldusnimekirja kinnitamiseks kasutatava avaliku võtme ja sellele vastava privaatvõtme loomise. Võtmepaari loomise tulemusena tekkinud avaliku võtme kehtestamine käesolevas määruses annab kinnituse just sellise unikaalse võtmepaari eksisteerimisest. Määruses on toodud avalikud võtmed kahe ettevalmistatud võtmepaari jaoks, mis võimaldab ühe võtmepaari aegumisel või muul põhjusel kasutuskõlbmatuks muutumisel usaldusnimekirja kinnitamist jätkata sujuvalt teise võtmepaariga. Eelnõus on avalikuks võtmeks esitatud isegenereeritud sertifikaadil esinev

sõnumilühend, mille korrektsust SHA512 räsiialgoritmi kaudu on võimalik tuvastada allkirja usaldamisel.

Eelnõu punktiga 2 täiendatakse § 3 lõikega 2, mille kohaselt on kuni 1.03.2018.a võimalik vajadusel kasutada enne selle määruse redaktsiooni jõustumist kasutatud võtmepaare. Nimetatud üleminekuperioodil toimub uute avalike võtmete kasutusele võtmisest asjaosaliste teavitamine ja usaldusnimekirjaga seotud rakenduste seadistamine ning samal ajal on järelevalveasutusel vaja teha muudatusi usaldusnimekirjas. Selle rakendussätte kehtestamisega tagatakse usaldusnimekirja pidev ning katkematu kehtivate andmete ajakohastamine.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu vastab Euroopa Liidu õigusele ja on vajalik otsekohalduva eIDAS määruse korrektseks rakendamiseks.

4. Määruse mõjud

Määrusega ei kaasne otseseid mõjusid riigi julgeolekule ja välissuhetele, majanduslikke mõjusid ega mõjusid riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele. Määrus on vajalik otsekohalduvas eIDAS määruks sätetatud liikmesriikide usaldusnimekirjade pidamise kohustuse täitmiseks.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Määrusele tuginedes on usaldusnimekirja pidaval pädeval asutusel (Tehnilise Järelevalve Ametil) võimalik korrektselt oma ülesandeid täita ning tagada usaldusnimekirja nõuetele vastavus ning usaldusväärsus. Määruse rakendamine ei too kaasa otseseid kulusid ega tulu.

6. Määruse jõustumine

Määrus jõustub üldises korras.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitati kooskõlastamiseks eelnõude infosüsteemi EIS kaudu Siseministeeriumile ja arvamuse avaldamiseks Tehnilise Järelevalve Ametile.

Urve Palo
ettevõtlus- ja infotehnoloogiaminister