

Justiits- ja digiministri määruse „Usaldusnimekirja kinnitamiseks kasutatav avalik võti ja sellele vastava privaativõtme kasutusala“ eelnõu SELETUSKIRI

1. Sissejuhatus

Eelnõukohase määrusega nähakse ette usaldusnimekirja kinnitamiseks kasutatavad avalikud võtmed. Avalike võtmete üheseks tuvastamiseks kasutatakse räsialgoritmi abil arvutatud sõnumilühendeid. Usaldusnimekirjad on masinloetavad ja neid kasutatakse usaldusteenuste usaldusväärsuse automaatkontrolliks. Seetõttu on ette nähtud, et usaldusnimekirjad kaitstakse krüptograafiliselt e-allkirja või e-templiga. Privaativõtit hoitakse usaldusnimekirja pidaja valduses ning sellele vastav avalik võti tehakse avalikuks usaldusväärsusest allikast, milleks praegusel juhul on kõnesolev määrus.

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

Määruse eelnõu ja seletuskirja on Riigi Infosüsteemi Ameti ettepaneku alusel koostanud Justiits- ja Digiministeeriumi riikliku IKT taristu talituse juhataja Erik Janson (erik.janson@justdigi.ee). Eelnõu keeletoimetuse tegi nimetatud ministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Helen Noormägi (helen.noormagi@justdigi.ee).

Eelnõu on seotud Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määrusega (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.08.2014, lk 73–114) (edaspidi *eIDAS-i määrus*).

Eelnõu ei mõjuta ettevõtjate, inimeste ega vabaühenduste halduskoormust, riigi- ega kohaliku omavalitsuse asutuste töökoormust.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast paragrahvist.

Eelnõu § 1. E-identimise ja e-tehingute usaldusteenuste seaduse § 15 lõike 3 kohaselt korraldab valdkonna eest vastutav minister käskkirjaga usaldusnimekirja kinnitamiseks kasutatava avaliku võtme ja sellele vastava privaativõtme loomise¹. Usaldusnimekirja kinnitamiseks kasutatav avalik võti sisaldub sertifikaadis. Avalike võtmete tuvastamiseks kasutatakse räsialgoritmi abil arvutatud sõnumilühendeid. Avalike võtmete üheseks tuvastamiseks esitatakse määruks kahe räsialgoritmi (SHA-512 ja SHA-256) abil arvutatud sõnumilühendid. Eelnõukohases määruks nähakse ette kummagi räsialgoritmi puhul kaks võtit: kui üks võti aegub või muutub muul põhjusel kasutuskõlbmatuks, saaks usaldusnimekirja kinnitamist jätkata sujuvalt teise võtmega.

¹ Justiits- ja digiministri 5. mai 2026. a käskkirja nr 39 „Usaldusnimekirja kinnitamiseks kasutatava avaliku võtme ja sellele vastava privaativõtme loomine ning vastava nõuandva komisjoni moodustamine ja juhendi kehtestamine“.

Räsialgoritmi SHA-512 abil tuvastatav avalik võti on kasutatav kuni 31. detsembrini 2027. Tähtaja seadmisel on arvestatud, et sõnumilühend on kasutusel juba 22. veebruarist 2019 (eelnoü § 3 alusel kehtetuks tunnistatava määruse alusel).

Räsialgoritmi SHA-512 abil tuvastatav võti on kasutatav eelnõukohase määruse jõustumisest arvates. Uue võtme lisamine toimub lähtuvalt otsekohalduvas eIDAS-i määrukses sätestatud liikmesriikide usaldusnimekirjade pidamise kohustusest.

Eelnõu § 2 sätestab usaldusnimekirja kinnitamiseks kasutatavasse võtmepaari kuuluva privaatvõtme kasutusala, milleks on määruse kohaselt usaldusnimekirja ja selles sisalduvate andmete õigsuse kinnitamine ning usaldusteenuse osutaja avaliku võtme kinnitamine. Seega ei ole mingid muud kasutusvaldkonnad taolisele privaatvõtmele ette nähtud.

Eelnõu §-ga 3 tunnistatakse kehtetuks majandus- ja taristuministri 22. novembri 2016. a määrus nr 68 „Usaldusnimekirja kinnitamiseks kasutatav avalik võti ja sellele vastava privaatvõtme kasutusala“.

Eelnõu §-s 4 nähakse rakendussättes ette räsialgoritmi SHA-512 abil tuvastatav avalik võtme (eelnoü § 1 lõige 2) kasutamise lõpptähtaeg, milleks on 31. detsember 2027. aastal. (vt ka § 1 selgitust)

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu vastab eIDAS-i määruse artikli 22 lõigetele 1 ja 2.

4. Määruse mõjud

Määrusega kehtestatakse avalike võtmete kirjeldus (tehniline muudatus) ja sellega ei kaasne otseseid mõjusid üheski mõjuvaldkonnas..

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

Määruse jõustumisega ei kaasne riigieelarvele otseseid kulusid ega tõuse sellest tulu.

6. Määruse jõustumine

Eelnõukohane määrus jõustub üldises korras, sest sellega ei kaasne vahetuid muudatusi ettevõtjate ja valitsusasutuste tegevuses.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitati kooskõlastamiseks eelnõude infosüsteemi kaudu Majandus- ja Kommunikatsiooniministeeriumile ning Siseministeeriumile. Eelnõu saadeti arvamuse avaldamiseks Riigi Infosüsteemi Ametile. Majandus- ja Kommunikatsiooniministeerium kooskõlastas eelnõu vaikimisi ning Siseministeerium kooskõlastas eelnõu märkusteta. Eelnõu teksti kohta tegi keelemärkusi Riigi Infosüsteemi Amet ja nende märkustega arvestati ka uue teksti koostamisel.