14.07.2026

Justiits- ja digiministri määruse „Usaldusnimekirja kinnitamiseks kasutatav SHA256 räsialgoritmil põhinev avalik võti ja sellele vastava privaatvõtme kasutusala“ eelnõu SELETUSKIRI

1. Sissejuhatus

Eelnõukohase määrusega uuendatakse usaldusnimekirja kinnitamiseks kasutatavaid avalike võtmete algoritme. Usaldusnimekirjad on masinloetavad ja neid kasutatakse usaldusteenuste usaldusväärsuse automatiseeritud kontrolliks. Seetõttu on ette nähtud, et usaldusnimekirjad kaitstakse krüptograafiliselt e-allkirja või e-templiga. Privaatvõtit hoitakse usaldusnimekirja pidaja valduses ning sellele vastav avalik võti tehakse avalikuks usaldusväärsest allikast, milleks praegusel juhul on käesolev määrus. Uuendamisel on arvestatud uuemate ja turvalisemate tehnoloogiate kasutusele võtmisega ning vananenud tehnoloogiatel põhineva kasutuselt äravõtmisega, et tagada usaldusteenuste usaldusväärsus.

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@jutsdigi.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 *eIDASe määrus*).

Eelnõu ei mõjuta ettevõtjate, inimeste ega vabaühenduste halduskoormust.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist.

Eelnõu §-ga 1 nähakse ette avaliku võtme võtmepaar, mida kasutatakse usaldusnimekirja kinnitamiseks. 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 privaatvõtme loomise.[1] Võtmepaari loomise tulemusena tekkinud avaliku võtme kehtestamine kinnitab, et just selline unikaalne võtmepaar on olemas. Eelnõukohases määruses on avalikud võtmed kahe ettevalmistatud võtmepaari jaoks, et juhul, kui üks võtmepaar aegub või muutub muul põhjusel kasutuskõlbmatuks, saaks usaldusnimekirja kinnitamist jätkata sujuvalt teise võtmepaariga. Avalikuks võtmeks on esitatud isegenereeritud sertifikaadil esinev sõnumilühend, mille korrektsust on SHA256 räsialgoritmi kaudu võimalik tuvastada allkirja usaldamisel.

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

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 tehakse muudatus majandus- ja taristuministri 22. novembri 2016. a määruses nr 68 „Usaldusnimekirja kinnitamiseks kasutatav avalik võti ja sellele vastava privaatvõtme kasutusala“ (RT I, 19.02.2019, 42, edaspidi *määrus nr 68*). Määrust nr 68 *täiendatakse uue paragrahviga 4*, millega nähakse ette määruse kehtivuse lõppemine 31. detsembril 2027 a. (kaasa arvatud). Muudatus võimaldab kasutada määruses nr 68 ette nähtud võtmepaare kuni 2027. aasta lõpuni. Eelnõukohase määruse jõustumise ja 2027. aasta 31 detsembrini jääval perioodil teavitatakse asjaosalisi uute avalike võtmete kasutusele võtmisest ja seadistatakse usaldusnimekirjaga seotud rakendused. Samal ajal on järelevalveasutusel võimalik teha muudatusi usaldusnimekirjas arvestades ka uusi võtmepaare. Sellega tagatakse usaldusnimekirja pidev ja katkematu kehtivate andmete ajakohastamine.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu vastab eIDASe määruse artikli 22 lõigetele 1 ja 2.

4. Määruse mõjud

Määrusega ei kaasne otseseid mõjusid üheski mõjuvaldkonnas. Eelnõukohane määrus on vajalik, et täita otsekohalduvas eIDASe määruses sätestatud liikmesriikide usaldusnimekirjade pidamise kohustust.

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

Eelnõukohase määruse jõustumisega ei kaasne riigieelarvele otseseid kulusid ega tõuse tulu.

6. Määruse jõustumine

Eelnõukohane määrus jõustub üldises korras.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse kooskõlastamiseks eelnõude infosüsteemi kaudu Majandus- ja Kommunikatsiooniministeeriumile ning Siseministeeriumile. Eelnõu saadetakse arvamuse avaldamiseks Riigi Infosüsteemi Ametile.