



RIIGI INFOSÜSTEEMI AMET

Justiits- ja Digiministeerium
info.delta@justdigi.ee

Teie 17.07.2026 nr 8-1/5420-1

Meie 07.08.2026 nr 1.1-20/261551

Usaldusnimekirja kinnitamiseks kasutatava avaliku võtme SHA-256 sõnumilühend ja sellele vastava privaatvõtme kasutusala

Austatud

Riigi Infosüsteemi Ametile on arvamuse avaldamiseks saadetud usaldusnimekirja kinnitamiseks kasutatava avaliku võtme SHA-256 sõnumilühend ja sellele vastava privaatvõtme kasutusala eelnõu.

Ülaltooduga seondult teeb RIA ettepaneku täpsustada eelnõu pealkirja, § 1 ja seletuskirja sõnastust.

Praegune sõnastus jätab mulje, et avalik võti põhineb SHA-256 räsialgoritmil või et räsiväärtus ise on avalik võti. Tegelikult kasutatakse SHA-256 räsiväärtust avaliku võtme üheseks tuvastamiseks.

Palume sõnastada eelnõu nii, et avalik võti ja selle tuvastamiseks kasutatav räsiväärtus oleksid selgelt eristatud. Samuti palume vastavalt täpsustada seletuskirja, eelkõige osa, milles sõnumilühendit käsitatakse avaliku võtmena.

Lugupidamisega

(allkirjastatud digitaalselt)

Taavi Ploompuu
peadirektori asetäitja riigi infosüsteemi alal

Margus Reitalus
mehis.lohmus@ria.ee