2024/2683

15.10.2024

EUROOPA KESKPANGA OTSUS (EL) 2024/2683,

8. oktoober 2024,

millega muudetakse otsust EKP/2013/1, millega kehtestatakse avaliku võtme infrastruktuuri raamistik Euroopa Keskpankade Süsteemi jaoks *(EKP/2024/26)*

EUROOPA KESKPANGA NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eelkõige selle artiklit 127 ja artikli 132 lõiget 1,

võttes arvesse Euroopa Keskpankade Süsteemi ja Euroopa Keskpanga põhikirja, eelkõige selle artiklit 12.1 koosmõjus artiklitega 3.1 ja 12.3 ning artiklit 34,

ning arvestades järgmist:

(1) Euroopa Keskpanga otsusega EKP/2013/1 ([1]) kehtestati eurosüsteemi avaliku võtme infrastruktuuri raamistik (edaspidi „ESCB-PKI“), et reguleerida selliste elektrooniliste sertifikaatide väljaandmist ja haldamist, mis on vajalikud juurdepääsuks EKPSi ja eurosüsteemi keskmise või sellest kõrgema kriitilise tähtsusega elektroonilistele rakendustele, süsteemidele, platvormidele ja teenustele.

(2) ESCB-PKI kasutatav tehnoloogia on jõudnud oma kasutusaja lõpuni ning see on asendatud. Seetõttu on vaja kasutusele võtta uus veebipõhine ESCB-PKI sertifitseerimisasutus (edaspidi „veebipõhine ESCB-PKI sertifitseerimisasutus V1.2“), võttes arvesse ka asjaolu, et EKPSi ja EKPSi-välistele kasutajatele väljastatud sertifikaatide ja veebipõhise ESCB-PKI sertifitseerimisasutuse tehniliste komponentide kolmeaastane kehtivusaeg ei saa lõppeda hiljem kui veebipõhise ESCB-PKI sertifitseerimisasutuse enda sertifikaadi kehtivusaeg. Veebipõhise ESCB-PKI sertifitseerimisasutuse kehtivusaeg lõppeb 22. juulil 2026; seejärel on veebipõhine ESCB-PKI sertifitseerimisasutus V1.2 kuni oma sertifikaadi kehtivusaja lõpuni ainus ESCB-PKI sertifitseerimisasutus.

(3) Seetõttu tuleb otsust EKP/2013/1 vastavalt muuta,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Muudatus

Otsuse EKP/2013/1 lisa asendatakse käesoleva otsuse lisaga.

Artikkel 2

Jõustumine

Käesolev otsus jõustub viiendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Frankfurt Maini ääres, 8. oktoober 2024

EKP president
Christine LAGARDE

([1]) Euroopa Keskpanga otsus EKP/2013/1, 11. jaanuar 2013, millega kehtestatakse avaliku võtme infrastruktuuri raamistik Euroopa Keskpankade Süsteemi jaoks (ELT L 74, 16.3.2013, lk 30).

LISA

„LISA

Teave ESCB-PKI sertifitseerimisasutuse kohta, sh selle isik ja tehnilised komponendid

ESCB-PKI sertifitseerimisasutus on osutatud sertifikaadis kui väljaandja ja selle salajast võtit kasutatakse sertifikaatide allkirjastamisel. ESCB-PKI sertifitseerimisasutus vastutab järgmise eest:

i) isiklike ja avaliku võtme sertifikaatide välja andmine;

ii) tühistusnimekirja koostamine;

iii) võtmepaaride loomine konkreetsetele sertifikaatidele, näiteks nendele, mis vajavad võtme taastamist;

iv) üldine vastutus ESCB-PKI halduse eest ja kõikide tegevuseks vajalike nõuete täitmine;

ESCB-PKI sertifitseerimisasutus hõlmab kõiki isikuid, põhimõtteid, menetlusi ja arvutisüsteem, mille on pandud ülesanne anda välja elektroonilisi sertifikaate ja määrata neid sertifikaatide kasutajatele.

ESCB-PKI sertifitseerimisasutus koosneb kolmest tehnilisest komponendist:

1. **ESCB-PKI (*Root ESCB-PKI*) juur-sertifitseerimisasutus**: See sertifitseerimisasutus on esimesel tasandil ja annab välja sertifikaadi iseendale ja temast järgmistele sertifitseerimisasutustele. See tegutseb ainult oma kitsalt määratletud ülesannete teostamiseks. Tema olulisemad andmed on järgmised:

Unikaalne nimi (Distinguished name)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Seerianumber (Serial number)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8
Väljaandja unikaalne nimi (Distinguished name of issuer)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Kehtivusaeg (Validity period)	Alates 21-06-2011 12:35:34 kuni 21-06-2041 12:35:34
Räsi (SHA-1) (Message digest (SHA-1))	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Räsi (SHA-256) (Message digest (SHA-256))	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Krüptimise algoritmid (Cryptographic algorithms)	SHA-256/RSA 4096

2. **Veebipõhine ESCB-PKI (*Online ESCB-PKI*) sertifitseerimisasutus**: See teise tasandi sertifitseerimisasutus on ESCB-PKI juur-sertifitseerimisasutusest järgmisel tasandil. Selle vastutusel on ESCB-PKI kasutajate jaoks sertifikaatide välja andmine. See kaotab kehtivuse 22. juulil 2026. Selle olulisemad andmed on järgmised:

Unikaalne nimi (Distinguished name)	CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Seerianumber (Serial number)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Väljaandja unikaalne nimi (Distinguished name of issuer)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Kehtivusaeg (Validity period)	Alates 22-07-2011 12:46:35 kuni 22-07-2026 12:46:35
Räsi (SHA-1) (Message digest (SHA-1))	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Räsi (SHA-256) (Message digest (SHA-256))	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Krüptimise algoritmid (Cryptographic algorithms)	SHA-256/RSA 4096

3. **Veebipõhine ESCB-PKI (*Online ESCB-PKI*) sertifitseerimisasutus V1.2**: See teise tasandi sertifitseerimisasutus on ESCB-PKI juur-sertifitseerimisasutusest järgmisel tasandil. Selle vastutusel on ESCB-PKI kasutajate jaoks sertifikaatide välja andmine. Pärast 22. juulit 2026 on ta kuni oma kehtivusaja lõpuni ainus veebipõhine ESCB-PKI sertifitseerimisasutus. Selle olulisemad andmed on järgmised:

Unikaalne nimi (Distinguished name)	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Seerianumber (Serial number)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Väljaandja unikaalne nimi (Distinguished name of issuer)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Kehtivusaeg (Validity period)	Alates 08-06-2023 17:07:00 kuni 08-06-2038 17:07:00
Räsi (SHA-1) (Message digest (SHA-1))	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Räsi (SHA-256) (Message digest (SHA-256))	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Krüptimise algoritmid (Cryptographic algorithms)	SHA-256/RSA 4096“