OTSUSED

EUROOPA KESKPANGA OTSUS (EL) 2016/187,

11. detsember 2015,

millega muudetakse otsust EKP/2013/1, millega kehtestatakse avaliku võtme infrastruktuuri raamistik Euroopa Keskpankade Süsteemi jaoks (EKP/2015/46)

EUROOPA KESKPANGA NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eelkõige selle artiklit 127,

võttes arvesse Euroopa Keskpankade Süsteemi ja Euroopa Keskpanga põhikirja, eelkõige selle artiklit 12.1 koosmõjus artiklitega 3.1, 5 ja 12.3 ning artikleid 16–24 ja 34,

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014 ([1]) tunnistati kehtetuks Euroopa Parlamendi ja nõukogu direktiiviga 1999/93/EÜ ([2]) alates 1. juulist 2016. Seetõttu tuleb otsuses EKP/2013/1 viidata määrusele (EL) nr 910/2014 ([3]).

(2) Ajakohastada tuleb teavet ESCB-PKI sertiftseerimisasutuse kohta, sh selle isik ja tehnilised komponendid, mis on sätestatud otsuse EKP/2013/1 lisas.

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

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Muudatused

Otsust EKP/2013/1 muudetakse järgmiselt.

1) Artikli 1 punkt 10 asendatakse järgmisega:

„10) „ESCB-PKI sertifitseerimisasutus" (ESCB-PKI certification authority) – üksus, millele kasutajad on teinud ülesandeks välja anda, tühistada ja uuendada ESCB-PKI sertifikaate kooskõlas EKPS/SSM sertifikaatide aktseptimise raamistikuga;".

2) Artikli 4 lõige 4 asendatakse järgmisega:

„4. ESCB-PKI sertifitseerimispõhimõtted on reeglite kogum, mis reguleerib elektrooniliste sertifikaatide kehtivusaega alates esialgsest taotlusest kasutamise lõpuni või tühistamiseni, samuti suhteid sertifikaadi taotleja või kasutaja, ESCB-PKI sertifitseerimisasutuse ja sõltuvate osapoolte vahel. See hõlmab direktiivi 1999/93/EÜ ja Euroopa

([1]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, (ELT L 257, 28.8.2014, lk 73).

([2]) Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ, 13. detsember 1999, elektroonilisi allkirju käsitleva ühenduse raamistiku kohta (EÜT L 13, 19.1.2000, lk 12).

([3]) 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).

Parlamendi ja nõukogu määruse (EL) nr 910/2014 (*) reguleerimisalasse ja sellest välja jäävaid sertifikaate. Samuti sätestab see kõikide osapoolte ülesanded ja vastutuse ning sertifikaatide väljaandmise ja haldamise korra. See on lisatud 2. tasandi – 3. tasandi lepingule.

(*) Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ, (ELT L 257, 28.8.2014, lk 73)."

3) Artikli 10 lõike 1 sissejuhatav lause ja alapunkt a asendatakse järgmisega:

„1. Kui eurosüsteemi keskpangad ei tõenda, et nad ei ole käitunud hooletult, vastutavad nad oma funktsioonide ja vastusala piires ESCB-PKIs mis tahes kahju eest, mis tekib kasutajale, kes on mõistlikult tuginenud kvaliteedisertifikaadile direktiivi 1999/93/EÜ ja määruse (EL) nr 910/2014 määratluse kohaselt järgmise osas:

a) kvaliteedisertifikaadis sisalduva kogu teave õigsus väljaandmise ajal ja küsimus, kas sertifikaat sisaldab kõiki üksikasju, mis on kvaliteedisertifikaadi jaoks ette nähtud direktiiviga 1999/93/EÜ ja määrusega (EL) nr 910/2014;".

4) Lisa asendatakse käesoleva otsuse lisaga.

Artikkel 2

Jõustumine

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

Frankfurt Maini ääres, 11. detsember 2015

EKP president
Mario DRAGHI

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 väljaandmine;

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 arvutisüsteeme, millele on pandud ülesanne anda välja elektroonilisi sertifikaate ja määrata neid sertifikaatide kasutajatele.

ESCB-PKI sertifitseerimisasutus koosneb kahest tehnilisest komponendist:

— **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:

a) SHA-1 sertifikaat ([1]):

Unikaalne nimi (Distinguished name)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Seerianumber (Serial number)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
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 11:58:26 kuni 21-06-2041 11:58:26
Räsi (SHA1) (Message digest (SHA-1))	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Räsi (SHA256) (Message digest (SHA-256))	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Krüptimise algoritmid (Cryptographic algorithms)	SHA-1/RSA 4096

b) SHA-256 sertifikaat:

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

([1]) Seda sertifikaati kasutatakse ainult süsteemide puhul, mis ei toeta kõrgema taseme algoritme.

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 (SHA1) (Message digest (SHA-1))	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Räsi (SHA256) (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

— **Alltaseme ESCB-PKI (online ESCB-PKI) sertifitseerimisasutus**: see teise tasandi sertifitseerimisasutus on algtaseme ESCB-PKI sertifitseerimisasutusest järgmisel tasandil. Selle vastutusel on ESCB-PKI kasutajate jaoks sertifikaatide välja andmine. Tema olulisemad andmed on järgmised:

a) SHA-1 sertifikaat ([1]):

Unikaalne nimi (Distinguished name)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Seerianumber (Serial number)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
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 (SHA1) (Message digest (SHA-1))	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Räsi (SHA256) (Message digest (SHA-256))	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Krüptimise algoritmid (Cryptographic algorithms)	SHA-1/RSA 4096

b) SHA-256 sertifikaat:

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 (SHA1) (Message digest (SHA-1))	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Räsi (SHA256) (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”

([1]) Seda sertifikaati kasutatakse ainult süsteemide puhul, mis ei toeta kõrgema taseme algoritme.