SPRENDIMAI

EUROPOS CENTRINIO BANKO SPRENDIMAS (ES) 2016/187

2015 m. gruodžio 11 d.

kuriuo iš dalies keičiamas Sprendimas ECB/2013/1, kuriuo nustatoma Europos centrinių bankų sistemos viešojo rakto infrastruktūros sistema (ECB/2015/46)

EUROPOS CENTRINIO BANKO VALDANČIOJI TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 127 straipsnį,

atsižvelgdama į Europos centrinių bankų sistemos ir Europos Centrinio Banko statutą, ypač į jo 12 straipsnio 1 dalį kartu su 3 straipsnio 1 dalimi, 5 straipsniu, 12 straipsnio 3 dalimi, 16–24 straipsniais ir 34 straipsniu,

kadangi:

(1) Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 ([1]) nuo 2016 m. liepos 1 d. panaikino Europos Parlamento ir Tarybos direktyvą 1999/93/EB ([2]). Todėl Sprendime ECB/2013/1 ([3]) reikia daryti nuorodą į Reglamentą (ES) Nr. 910/2014;

(2) reikia atnaujinti informaciją, susijusią su ECBS-VRI sertifikavimo įstaiga, taip pat apie jos tapatybę ir jos techninius komponentus, nurodytus Sprendimo ECB/2013/1 priede;

(3) todėl reikia iš dalies pakeisti Sprendimą ECB/2013/1,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Daliniai pakeitimai

Sprendimas ECB/2013/1 iš dalies pakeičiamas taip:

1. 1 straipsnio 10 dalis pakeičiama taip:

„10. ECBS-VRI sertifikavimo įstaiga – subjektas, kuriuo vartotojai pasikliauja ir kuris išduoda, tvarko, panaikina ir atnaujina ECBS-VRI sertifikatus pagal ECBS/BPM sertifikatų pripažinimo sistemą.“;

2. 4 straipsnio 4 dalis pakeičiama taip:

„4. ECBS-VRI sertifikavimo praktikos dokumentas yra rinkinys taisyklių, reglamentuojančių elektroninių sertifikatų gyvavimo ciklą – nuo pradinio prašymo iki abonemento pabaigos arba panaikinimo, taip pat santykius tarp sertifikato prašytojo arba abonento, ECBS-VRI sertifikavimo įstaigos ir pasikliaujančių šalių. Jis apima sertifikatus,

([1]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

([2]) 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (OL L 13, 2000 1 19, p. 12).

([3]) 2013 m. sausio 11 d. Europos Centrinio Banko sprendimas ECB/2013/1, kuriuo nustatoma Europos centrinių bankų sistemos viešojo rakto infrastruktūros sistema (OL L 74, 2013 3 16, p. 30).

kuriems taikoma Direktyva 1999/93/EB ir Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 (*), ir sertifikatus, kuriems jie netaikomi. Jame taip pat nustatomi visų šalių vaidmenys ir pareigos bei sertifikatų išdavimo ir tvarkymo procedūros. Jis pridėtas prie 2 ir 3 lygių susitarimo.

(*) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).“;

3. 10 straipsnio įžanginė dalis ir 1 dalies a punktas pakeičiami taip:

„1. Išskyrus atvejus, kai Eurosistemos centriniai bankai įrodo, kad nesielgė neatsargiai, savo funkcijų ir pareigų ECBS-VRI kontekste Eurosistemos centriniai bankai atsako už bet kokią vartotojui, kuris pagrįstai pasikliauja kvalifikuotu sertifikatu, kaip apibrėžta Direktyvoje 1999/93/EB ir Reglamente (ES) Nr. 910/2014, padarytą žalą, susijusią su:

a) kvalifikuoto sertifikato išdavimo metu visos jame esančios informacijos tikslumu ir tuo, ar sertifikate yra visa informacija, kuri turi būti pagal Direktyvą 1999/93/EB ir Reglamentą (ES) Nr. 910/2014;“;

4. Priedas pakeičiamas šio sprendimo priedu.

2 straipsnis

Įsigaliojimas

Šis sprendimas įsigalioja trečią dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Frankfurte prie Maino 2015 m. gruodžio 11 d.

ECB Pirmininkas

Mario DRAGHI

PRIEDAS

„PRIEDAS

Informacija apie ECBS-VRI sertifikavimo įstaigą, įskaitant jos tapatybę ir jos techninius komponentus

ECBS-VRI sertifikavimo įstaiga jos sertifikate yra nurodoma kaip išduodanti įstaiga, ir jos privatus raktas naudojamas sertifikatams pasirašyti. ECBS-VRI sertifikavimo įstaiga atsako už:

i) privataus ir viešojo rakto sertifikatų išdavimą;

ii) sertifikatų galiojimo panaikinimo sąrašų sudarymą;

iii) raktų porų, susijusių su tam tikrais sertifikatais, pvz., tokiais, kuriems reikia rakto atgaminimo, generavimą;

iv) bendrą atsakomybę už ECBS-VRI ir užtikrinimą, kad laikomasi visų jai eksploatuoti reikalingų reikalavimų.

ECBS-VRI sertifikavimo įstaiga apima visus asmenis, politikas, procedūras ir kompiuterių sistemas, kurių pagalba jai patikėta išduoti elektroninius sertifikatus ir priskirti juos sertifikatų abonentams.

ECBS-VRI sertifikavimo įstaigą sudaro du techniniai komponentai:

— **Pagrindinė ECBS-VRI sertifikavimo įstaiga:** pirmuoju lygiu ši sertifikavimo įstaiga išduoda sertifikatus tik sau pačiai ir jai pavaldžioms sertifikavimo įstaigoms. Ji vykdo veiklą tik atlikdama šias siaurai apibrėžtas savo pareigas. Svarbiausi jos duomenys:

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

Distinguished name (unikalus pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (serijinis numeris)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer (unikalus išduodančios įstaigos pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (galiojimo laikotarpis)	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (pranešimo maišos reikšmė) (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message Digest (pranešimo maišos reikšmė) (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (kriptografiniai algoritmai)	SHA-1/RSA 4096

b) SHA-256 sertifikatas:

Distinguished name (unikalus pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (serijinis numeris)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

([1]) Šis sertifikatas bus naudojamas tik sudėtingesnių algoritmų nepriimančiose sistemose.

Distinguished name of Issuer (unikalus išduodančios įstaigos pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (galiojimo laikotarpis)	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest (pranešimo maišos reikšmė) (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message Digest (pranešimo maišos reikšmė) (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (kriptografiniai algoritmai)	SHA-256/RSA 4096

— **ECBS-VRI sertifikavimo įstaiga *online*:** antruoju lygiu ši sertifikavimo įstaiga yra pavaldi pagrindinei ECBS-VRI sertifikavimo įstaigai. Ji atsako už ECBS-VRI sertifikatų išdavimą vartotojams. Svarbiausi jos duomenys:

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

Distinguished name (unikalus pavadinimas)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (serijinis numeris)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer (unikalus išduodančios įstaigos pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (galiojimo laikotarpis)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (pranešimo maišos reikšmė) (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message Digest (pranešimo maišos reikšmė) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (kriptografiniai algoritmai)	SHA-1/RSA 4096

b) SHA-256 sertifikatas:

Distinguished name (unikalus pavadinimas)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (serijinis numeris)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of Issuer (unikalus išduodančios įstaigos pavadinimas)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (galiojimo laikotarpis)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (pranešimo maišos reikšmė) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message Digest (pranešimo maišos reikšmė) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (kriptografiniai algoritmai)	SHA-256/RSA 4096“

([1]) Šis sertifikatas bus naudojamas tik sudėtingesnių algoritmų nepriimančiose sistemose.