Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/2683

2024 10 15

EUROPOS CENTRINIO BANKO SPRENDIMAS (ES) 2024/2683

2024 m. spalio 8 d.

kuriuo iš dalies keičiamas Sprendimas ECB/2013/1, kuriuo nustatoma Europos centrinių bankų sistemos viešojo rakto infrastruktūros sistema *(ECB/2024/26)*

Europos Centrinio Banko valdančioji taryba,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 127 straipsnį ir 132 straipsnio 1 dalį,

atsižvelgdama į Europos centrinių bankų sistemos ir Europos Centrinio Banko statutą, ypač į jo 12 straipsnio 1 dalį kartu su 3 straipsnio 1 dalimi ir 12 straipsnio 3 dalimi, ir į jo 34 straipsnį,

kadangi:

(1) Europos Centrinio Banko sprendimu ECB/2013/1 [1] buvo nustatyta Europos centrinių bankų sistemos viešojo rakto infrastruktūros (toliau – ECBS-VRI) sistema, skirta reglamentuoti elektroninių sertifikatų, reikalingų naudojantis vidutinės arba didesnės svarbos ECBS ir Eurosistemos elektroninėmis programomis, sistemomis, platformomis ir paslaugomis, išdavimą ir valdymą;

(2) ECBS-VRI naudojamos technologijos galiojimo laikas pasibaigė ir ji buvo pakeista. Todėl reikia nustatyti naują internetinę ECBS-VRI sertifikavimo įstaigą (toliau – internetinė ECBS-VRI sertifikavimo įstaiga V1.2), taip pat atsižvelgiant į tai, kad ECBS vartotojams ir ECBS nepriklausantiems vartotojams išduotų sertifikatų ir internetinės ECBS-VRI sertifikavimo įstaigos valdomų techninių komponentų trejų metų galiojimo laikotarpis negali baigtis vėliau nei pačios internetinės ECBS-VRI sertifikavimo įstaigos sertifikato galiojimo laikotarpis. Esamos internetinės ECBS-VRI sertifikavimo įstaigos sertifikatas nustoja galioti 2026 m. liepos 22 d., tad po to internetinė ECBS-VRI sertifikavimo įstaiga V1.2 būtų vienintelė internetinė ECBS-VRI sertifikavimo įstaiga iki jos sertifikato galiojimo pabaigos;

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

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Dalinis pakeitimas

Sprendimo ECB/2013/1 priedas pakeičiamas šio sprendimo priedu.

2 straipsnis

Įsigaliojimas

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

Priimta Frankfurte prie Maino 2024 m. spalio 8 d.

ECB Pirmininkė
Christine LAGARDE

[1] 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).

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, t. y. 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 trys techniniai komponentai:

1. **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:

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
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

2. **Internetinė ECBS-VRI sertifikavimo įstaiga:** antruoju lygiu ši sertifikavimo įstaiga yra pavaldi pagrindinei ECBS-VRI sertifikavimo įstaigai. Ji atsako už ECBS-VRI sertifikatų išdavimą vartotojams. Ji nustoja galioti 2026 m. liepos 22 d. Svarbiausi jos duomenys:

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

3. **Internetinė ECBS-VRI sertifikavimo įstaiga V1.2:** antruoju lygiu ši sertifikavimo įstaiga yra pavaldi pagrindinei ECBS-VRI sertifikavimo įstaigai. Ji atsako už ECBS-VRI sertifikatų išdavimą vartotojams. Po 2026 m. liepos 22 d. ji yra vienintelė internetinė ECBS-VRI sertifikavimo įstaiga iki jos galiojimo pabaigos. Svarbiausi jos duomenys:

Distinguished name (unikalus pavadinimas)	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (serijinis numeris)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
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 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (pranešimo maišos reikšmė) (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message Digest (pranešimo maišos reikšmė) (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms (kriptografiniai algoritmai)	SHA-256/RSA 4096“