LĒMUMI

EIROPAS CENTRĀLĀS BANKAS LĒMUMS (ES) 2016/187

(2015. gada 11. decembris),

ar kuru groza Lēmumu ECB/2013/1, ar ko nosaka Eiropas Centrālo banku sistēmas publiskās atslēgas infrastruktūras regulējumu (ECB/2015/46)

EIROPAS CENTRĀLĀS BANKAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 127. pantu,

ņemot vērā Eiropas Centrālo banku sistēmas un Eiropas Centrālās bankas Statūtus un jo īpaši to 12.1. pantu saistībā ar 3.1. pantu, 5. pantu, 12.3. pantu, kā arī 16.–24. pantu un 34. pantu,

tā kā:

(1) Ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 ([1]) no 2016. gada 1. jūlija atcelta Eiropas Parlamenta un Padomes Direktīva 1999/93/EK ([2]). Tādēļ Lēmumā ECB/2013/1 ([3]) jāatsaucas uz Regulu (ES) Nr. 910/2014.

(2) Jāatjaunina informācija par ECBS PAI sertificēšanas iestādi, t. sk. tās identitāti un tās tehniskajiem komponentiem, kas izklāstīta Lēmuma ECB/2013/1 pielikumā.

(3) Tādēļ attiecīgi jāgroza Lēmums ECB/2013/1,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Grozījumi

Lēmumu ECB/2013/1 groza šādi:

1) ar šādu punktu aizstāj 1. panta 10. punktu:

"10) ECBS PAI sertificēšanas iestāde (*ESCB-PKI certification authority*) ir iestāde, kurai uzticas lietotāji un kura izsniedz, pārvalda, atsauc un atjauno ECBS PAI sertifikātus, ievērojot ECBS/VUM sertifikātu pieņemšanas regulējumu;";

2) ar šādu punktu aizstāj 4. panta 4. punktu:

"4. ECBS PAI sertificēšanas prakses deklarācija ir noteikumu kopums, kas regulē elektronisko sertifikātu "dzīves ciklu" no sākotnējā pieprasījuma līdz abonenta beigām vai tā atsaukšanai, kā arī attiecības starp sertifikāta pieteikuma iesniedzēju vai abonentu, ECBS PAI sertificēšanas iestādi un personām, kas paļaujas uz sertifikātu. Tā attiecas gan uz

([1]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).
([2]) Eiropas Parlamenta un Padomes Direktīva 1999/93/EK (1999. gada 13. decembris) par Kopienas elektronisko parakstu sistēmu (OV L 13, 19.1.2000., 12. lpp.).
([3]) Eiropas Centrālās bankas Lēmums ECB/2013/1 (2013. gada 11. janvāris), ar ko nosaka Eiropas Centrālo banku sistēmas publiskās atslēgas infrastruktūras regulējumu (OV L 74, 16.3.2013., 30. lpp.).

sertifikātiem, kas ietilpst Eiropas Parlamenta un Padomes Direktīvas 1999/93/EK un Regulas (ES) Nr. 910/2014 (*) piemērošanas jomā, gan sertifikātiem, kas to piemērošanas jomā neietilpst. Tas arī izklāsta visu pušu lomas un pienākumus un nosaka procedūras sertifikātu izsniegšanai un pārvaldīšanai. To pievieno 2. līmeņa–3. līmeņa līgumam.

(*) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).";

3) ar šādu tekstu aizstāj 10. panta 1. punkta ievaddaļu un a) apakšpunktu:

"1. Ja vien Eurosistēmas centrālās bankas nepierāda, ka tās nav rīkojušās nolaidīgi, tās saskaņā ar savām funkcijām un pienākumiem ECBS PAI atbild par zaudējumiem, kas radušies lietotājiem, kuri pamatoti paļāvušies uz kvalificētu sertifikātu, kā tas noteikts Direktīvā 1999/93/EK un Regulā (ES) Nr. 910/2014, attiecībā uz:

a) visas tās informācijas pareizumu izsniegšanas brīdī, kas ietverta kvalificētā sertifikātā, un to, vai sertifikātā iekļauti visi dati, kas paredzēti kvalificētiem sertifikātiem, kā tas noteikts Direktīvā 1999/93/EK un Regulā (ES) Nr. 910/2014;";

4) pielikumu aizstāj ar šā lēmuma pielikumu.

2. pants

Stāšanās spēkā

Šis lēmums stājas spēkā trešajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Frankfurtē pie Mainas, 2015. gada 11. decembrī

ECB prezidents
Mario DRAGHI

PIELIKUMS

"PIELIKUMS

Informācija par ECBS PAI sertificēšanas iestādi, t. sk. tās identitāti un tās tehniskajiem komponentiem

ECBS PAI sertificēšanas iestādi tās sertifikātos norāda kā izsniedzēju, un sertifikātu parakstīšanai izmanto tās privāto atslēgu. ECBS PAI sertificēšanas iestāde atbild par:

i) privātās un publiskās atslēgas sertifikātu izsniegšanu;

ii) atsaukšanas sarakstu izsniegšanu;

iii) atslēgu pāru radīšanu saistībā ar konkrētiem sertifikātiem, piemēram, tiem, kam nepieciešama atslēgas atgūšana;

iv) vispārīgās atbildības par ECBS PAI saglabāšanu un visu tās darbībai vajadzīgo prasību izpildes nodrošināšanu.

ECBS PAI sertificēšanas iestāde ietver visas personas, politiku, procedūras un datorsistēmas, kam uzticēta elektronisko sertifikātu izsniegšana un to piešķiršana sertifikātu abonentiem.

ECBS PAI sertificēšanas iestāde ietver divus tehniskos komponentus:

— **Galvenā ECBS PAI sertificēšanas iestāde.** Šī pirmā līmeņa sertificēšanas iestāde izsniedz sertifikātus tikai sev pašai un sev pakļautajām sertificēšanas iestādēm. Tā darbojas, vienīgi veicot tās šauri definētos pienākumus. Tās nozīmīgākie dati ir šādi:

a) SHA-1 sertifikāts ([1]):

***Distinguished name* (Atšķirams nosaukums)**	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Serial number* (Sērijas numurs)**	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
***Distinguished name of issuer* (Izsniedzēja atšķirams nosaukums)**	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Validity period* (Derīguma termiņš)**	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
***Message digest* (SHA-1) (Ziņojuma īssavilkums (SHA-1))**	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
***Message digest* (SHA-256) (Ziņojuma īssavilkums (SHA-256))**	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
***Cryptographic algorithms* (Kriptogrāfiskie algoritmi)**	SHA-1/RSA 4096

b) SHA-256 sertifikāts:

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

([1]) Šis sertifikāts tiks izmantots vienīgi sistēmās, kuras neatbalsta augstākus algoritmus.

***Distinguished name of issuer* (Izsniedzēja atšķirams nosaukums)**	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Validity period* (Derīguma termiņš)**	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
***Message digest* (SHA-1) (Ziņojuma īssavilkums (SHA-1))**	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
***Message digest* (SHA-256) (Ziņojuma īssavilkums (SHA-256))**	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
***Cryptographic algorithms* (Kriptogrāfiskie algoritmi)**	SHA-256/RSA 4096

— **Tiešsaistes ECBS PAI sertificēšanas iestāde.** Šī otrā līmeņa sertificēšanas iestāde ir pakļauta Galvenajai ECBS PAI sertificēšanas iestādei. Tā atbild par ECBS PAI sertifikātu izsniegšanu lietotājiem. Tās nozīmīgākie dati ir šādi:

a) SHA-1 sertifikāts ([1]):

***Distinguished name* (Atšķirams nosaukums)**	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Serial number* (Sērijas numurs)**	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
***Distinguished name of issuer* (Izsniedzēja atšķirams nosaukums)**	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Validity period* (Derīguma termiņš)**	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
***Message digest* (SHA-1) (Ziņojuma īssavilkums (SHA-1))**	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
***Message digest* (SHA-256) (Ziņojuma īssavilkums (SHA-256))**	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
***Cryptographic algorithms* (Kriptogrāfiskie algoritmi)**	SHA-1/RSA 4096

b) SHA-256 sertifikāts:

***Distinguished name* (Atšķirams nosaukums)**	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Serial number* (Sērijas numurs)**	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
***Distinguished name of issuer* (Izsniedzēja atšķirams nosaukums)**	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
***Validity period* (Derīguma termiņš)**	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
***Message digest* (SHA-1) (Ziņojuma īssavilkums (SHA-1))**	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
***Message digest* (SHA-256) (Ziņojuma īssavilkums (SHA-256))**	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
***Cryptographic algorithms* (Kriptogrāfiskie algoritmi)**	SHA-256/RSA 4096”

([1]) Šis sertifikāts tiks izmantots vienīgi sistēmās, kuras neatbalsta augstākus algoritmus.