SKLEPI

SKLEP EVROPSKE CENTRALNE BANKE (EU) 2016/187

z dne 11. decembra 2015

o spremembi Sklepa ECB/2013/1 o določitvi okvira za infrastrukturo javnih ključev za Evropski sistem centralnih bank (ECB/2015/46)

SVET EVROPSKE CENTRALNE BANKE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 127 Pogodbe,

ob upoštevanju Statuta Evropskega sistema centralnih bank in Evropske centralne banke ter zlasti člena 12.1 v povezavi s členom 3.1, členom 5, členom 12.3, členi 16 do 24 in členom 34 Statuta,

ob upoštevanju naslednjega:

(1) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta ([1]) je razveljavila Direktivo Evropskega parlamenta in Sveta 1999/93/ES ([2]) z učinkom od 1. julija 2016. Zato se je v Sklepu ECB/2013/1 ([3]) primerno sklicevati na Uredbo (EU) št. 910/2014.

(2) Informacije o overitelju ESCB-PKI, vključno z njegovo identiteto, in njegovih tehničnih komponentah, kakor so določene v Prilogi k Sklepu ECB/2013/1, je treba posodobiti.

(3) Zato je treba Sklep ECB/2013/1 ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Spremembe

Sklep ECB/2013/1 se spremeni:

1. v členu 1 se točka 10 nadomesti z naslednjim:

„10. ‚overitelj ESCB-PKI' pomeni subjekt, ki mu uporabniki zaupajo, da izdaja, upravlja, preklicuje in obnavlja potrdila ESCB-PKI v skladu z okvirom ESCB/EMN za sprejem potrdil;";

2. v členu 4 se odstavek 4 nadomesti z naslednjim:

„4. Pravila overjanja ESCB-PKI so niz pravil, ki urejajo življenjski cikel elektronskih potrdil od prvotne prošnje do izteka ali preklica ter tudi razmerja med prosilcem za potrdilo ali imetnikom potrdila, overiteljem ESCB-PKI in osebami, ki se zanašajo na potrdilo. Zajemajo potrdila, ki sodijo v področje uporabe Direktive 1999/93/ES in Uredbe

([1]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).
([2]) Direktiva Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (UL L 13, 19.1.2000, str. 12).
([3]) Sklep ECB/2013/1 Evropske centralne banke z dne 11. januarja 2013 o določitvi okvira za infrastrukturo javnih ključev za Evropski sistem centralnih bank (UL L 74, 16.3.2013, str. 30).

(EU) št. 910/2014 Evropskega parlamenta in Sveta (*), ter potrdila, ki vanj ne sodijo. Določajo tudi vloge in odgovornosti vseh strank ter postopke v zvezi z izdajo in upravljanjem potrdil. Priložena so k sporazumu med ravnema 2 in 3.

(*) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).“;

3. v členu 10 se uvodno besedilo in točka (a) odstavka 1 nadomestita z naslednjim:

„1. Razen če dokažejo, da niso delovale malomarno, so centralne banke Eurosistema v skladu s svojimi funkcijami in odgovornostmi v zvezi z infrastrukturo ESCB-PKI odgovorne za vso škodo, povzročeno uporabniku, ki se upravičeno zanaša na kvalificirano potrdilo, kakor je opredeljeno v Direktivi 1999/93/ES in Uredbi (EU) št. 910/2014, kar zadeva:

(a) pravilnost vseh informacij v kvalificiranem potrdilu v času njegove izdaje in vprašanje, ali potrdilo vsebuje vse podrobnosti, ki so predpisane za kvalificirano potrdilo, kakor je opredeljeno v Direktivi 1999/93/ES in Uredbi (EU) št. 910/2014;“;

4. Priloga se nadomesti z besedilom iz Priloge k temu sklepu.

Člen 2

Začetek veljavnosti

Ta sklep začne veljati tretji dan po objavi v *Uradnem listu Evropske unije*.

V Frankfurtu na Majni, 11. decembra 2015

Predsednik ECB

Mario DRAGHI

PRILOGA

„PRILOGA

Informacije o overitelju ESCB-PKI, vključno z njegovo identiteto, in njegovih tehničnih komponentah

Overitelj ESCB-PKI je v svojem potrdilu naveden kot izdajatelj in njegov zasebni ključ se uporablja za podpisovanje potrdil. Overitelj ESCB-PKI je pristojen za:

(i) izdajo potrdil za zasebne in javne ključe;

(ii) izdajo seznamov preklicanih potrdil;

(iii) tvorjenje parov ključev, ki so povezani z določenimi potrdili, npr. tistimi, ki zahtevajo povrnitev ključa;

(iv) ohranjanje splošne odgovornosti za infrastrukturo ESCB-PKI in zagotavljanje, da so izpolnjene vse zahteve za njeno upravljanje.

Overitelj ESCB-PKI vključuje vse posameznike, politike, postopke in računalniške sisteme, ki so namenjeni za izdajo elektronskih potrdil in njihovo dodeljevanje imetnikom potrdil.

Overitelj ESCB-PKI vključuje dve tehnični komponenti:

— **overitelj korenskih potrdil ESCB-PKI**: ta overitelj na prvi ravni izdaja potrdila samo zase in sebi podrejene overitelje. Deluje samo takrat, ko izvaja svoje ozko določene odgovornosti. Njegovi ključni podatki so:

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

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

(b) potrdilo SHA-256:

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

([1]) To potrdilo se bo uporabljalo samo v sistemih, ki ne podpirajo višjih algoritmov.

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

— **overitelj spletnih potrdil ESCB-PKI**: ta overitelj je na drugi ravni podrejen overitelju korenskih potrdil ESCB-PKI. Odgovoren je za izdajo potrdil ESCB-PKI za uporabnike. Njegovi ključni podatki so:

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

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

(b) potrdilo SHA-256:

Distinguished name (razločevalno ime)	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (serijska številka)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of issuer (razločevalno ime izdajatelja)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (obdobje veljavnosti)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (SHA-1) (zgoščena vrednost (SHA-1))	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest (SHA-256) (zgoščena vrednost (SHA-256))	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (kriptografski algoritmi)	SHA-256/RSA 4096“

([1]) To potrdilo se bo uporabljalo samo v sistemih, ki ne podpirajo višjih algoritmov.