ODLUKE

ODLUKA (EU) 2016/187 EUROPSKE SREDIŠNJE BANKE

od 11. prosinca 2015.

o izmjeni Odluke ESB/2013/1 o utvrđivanju okvira za infrastrukturu javnog ključa za Europski sustav središnjih banaka (ESB/2015/46)

UPRAVNO VIJEĆE EUROPSKE SREDIŠNJE BANKE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 127.,

uzimajući u obzir Statut Europskog sustava središnjih banaka i Europske središnje banke, a posebno njegov članak 12. stavak 1. u vezi s člankom 3. stavkom 1., člankom 5. i člancima 16. do 24. i člankom 34.,

budući da:

(1) Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća ([1]) stavljena je izvan snage Direktiva 1999/93/EZ Europskog parlamenta i Vijeća ([2]) s učinkom od 1. srpnja 2016. Stoga, u Odluci ESB/2013/1 ([3]) valja uputiti na Uredbu (EU) br. 910/2014.

(2) Informacije o tijelu za certificiranje infrastrukture javnog ključa ESSB-a, uključujući njegov identitet i tehničke komponente, navedene u Prilogu Odluci ESB/2013/1, potrebno je ažurirati.

(3) Odluku ESB/2013/1 trebalo bi stoga na odgovarajući način izmijeniti,

DONIJELO JE OVU ODLUKU:

Članak 1.

Izmjene

Odluka ESB/2013/1 mijenja se kako slijedi:

1. U članku 1. točka 10. zamjenjuje se sljedećim:

„10. ‚Tijelo za certificiranje infrastrukture javnog ključa ESSB-a' znači subjekt kojem korisnici vjeruju, a koje izdaje, upravlja, opoziva i obnavlja certifikate infrastrukture javnog ključa ESSB-a u skladu s okvirom ESSB-a/SSM-a za prihvaćanje certifikata;";

2. U članku 4. stavak 4. zamjenjuje se sljedećim:

„4. Izjava o certifikacijskim praksama infrastrukture javnog ključa ESSB-a jest skup pravila koja uređuju životni ciklus elektroničkih certifikata od inicijalnog zahtjeva do isteka certifikata ili opoziva, kao i odnose između podnositelja zahtjeva za certifikat i imatelja certifikata, tijela za certificiranje infrastrukture javnog ključa ESSB-a i osoba koje se pouzdaju u certifikat. Izjava obuhvaća elektroničke certifikate koji pripadaju području primjene

([1]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

([2]) Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise (SL L 13, 19.1.2000., str. 12.).

([3]) Odluka ESB/2013/1 Europske središnje banke od 11. siječnja 2013. o utvrđivanju okvira za infrastrukturu javnog ključa za Europski sustav središnjih banaka (SL L 74, 16.3.2013., str. 30.).

Direktive 1999/93/EZ i Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća (*) i certifikate koji ne pripadaju području njezine primjene. Njome se također utvrđuju uloge i odgovornosti svih stranaka i određuju postupci povezani s izdavanjem certifikata i upravljanjem njima. Ona se prilaže sporazumu između razine 2 i razine 3.

(*) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).";

3. u članku 10., uvodna izjava i točka (a) zamjenjuju se sljedećim:

„1. Osim ako dokažu da nisu djelovale nemarno, u skladu sa svojim funkcijama i odgovornostima u infrastrukturi javnog ključa ESSB-a, središnje banke Eurosustava odgovorne su za sve štete nastale korisniku koji se razumno pouzdao u kvalificirani certifikat kako je određeno u Direktivi 1999/93/EZ i Uredbi (EU) br. 910/2014 u pogledu:

(a) točnosti svih informacija navedenih u kvalificiranom certifikatu u trenutku izdavanja te pitanja sadržava li certifikat sve pojedinosti propisane za kvalificirani certifikat kako je određeno u Direktivi 1999/93/EZ i Uredbi (EU) br. 910/2014;";

4. Prilog se zamjenjuje Prilogom ovoj Odluci.

Članak 2.

Stupanje na snagu

Ova Odluka stupa na snagu trećeg dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u Frankfurtu na Majni 11. prosinca 2015.

Predsjednik ESB-a

Mario DRAGHI

PRILOG

„PRILOG

Informacije o tijelu za certificiranje infrastrukture javnog ključa ESSB-a, uključujući njegov identitet i njegove tehničke komponente

Tijelo za certificiranje infrastrukture javnog ključa ESSB-a utvrđuje se u njegovu certifikatu kao izdavatelj te se njegov tajni ključ upotrebljava za potpisivanje certifikata. Tijelo za certificiranje infrastrukture javnog ključa ESSB-a nadležno je za:

i. izdavanje certifikata tajnog i javnog ključa;

ii. izdavanje popisa opoziva;

iii. generiranje parova ključeva povezanih s određenim certifikatima, npr. onima za koje je potreban oporavak ključa;

iv. ukupnu odgovornost za infrastrukturu javnog ključa ESSB-a i osiguravanje ispunjavanja svih zahtjeva potrebnih za njezin rad.

Tijelo za certificiranje infrastrukture javnog ključa ESSB-a uključuje sve osobe, politike, postupke i računalne sustave kojima je povjereno izdavanje elektroničkih certifikata i njihovo dodjeljivanje imateljima certifikata.

Tijelo za certificiranje infrastrukture javnog ključa ESSB-a uključuje dvije tehničke komponente:

— **Osnovno tijelo za certificiranje infrastrukture javnog ključa ESSB-a**: Ovo tijelo za certificiranje na prvoj razini izdaje certifikate samo sebi i svojim podređenim tijelima za certificiranje. Ono radi samo kada obavlja svoje usko određene odgovornosti. Njegovi su najznačajniji podaci:

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

Distinguished name (razlikovno ime)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (serijski broj	596F AC4C 218C 21BC 4E00 6B42 A164 46DD |
Distinguished name of issuer (razlikovno ime izdavatelja)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (razdoblje valjanosti)	od 21-06-2011 11:58:26 do 21-06-2041 11:58:26
Message digest (sažetak poruke) (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest (sažetak poruke) (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Kriptografski algoritmi	SHA-1/RSA 4096

(b) Certifikat SHA-256

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

([1]) Ovaj se certifikat koristi samo u sustavima koji ne podržavaju više algoritme.

Distinguished name of issuer (razlikovno ime izdavatelja)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (razdoblje valjanosti)	od 21-06-2011 12:35:34 do 21-06-2041 12:35:34
Message digest (sažetak poruke) (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (sažetak poruke) (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Kriptografski algoritmi	SHA-256/RSA 4096

— **Mrežno tijelo za certificiranje infrastrukture javnog ključa ESSB-a**: Ovo tijelo za certificiranje na drugoj razini podređeno je osnovnom tijelu za certificiranje infrastrukture javnog ključa ESSB-a. Ono je odgovorno za izdavanje certifikata infrastrukture javnog ključa ESSB-a korisnicima. Njegovi su najznačajniji podaci:

(a) Certifikat SHA-1 ([1])

Distinguished name (razlikovno ime)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (serijski broj)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer (razlikovno ime izdavatelja)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (razdoblje valjanosti)	od 22-07-2011 12:46:35 do 22-07-2026 12:46:35
Message digest (sažetak poruke) (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message digest (sažetak poruke) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Kriptografski algoritmi	SHA-1/RSA 4096

(b) Certifikat SHA-256

Distinguished name (razlikovno ime)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (serijski broj)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of issuer (razlikovno ime izdavatelja)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (razdoblje valjanosti)	od 22-07-2011 12:46:35 do 22-07-2026 12:46:35
Message digest (sažetak poruke) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest (sažetak poruke) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Kriptografski algoritmi	SHA-256/RSA 4096”

([1]) Ovaj se certifikat koristi samo u sustavima koji ne podržavaju više algoritme.