BESLUT

EUROPEISKA CENTRALBANKENS BESLUT (EU) 2016/187

av den 11 december 2015

om ändring av beslut ECB/2013/1 om ett ramverk för en infrastruktur för kryptering med öppen nyckel (PKI) för Europeiska centralbankssystemet (ECB/2015/46)

ECB-RÅDET HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 127,

med beaktande av stadgan för Europeiska centralbankssystemet och Europeiska centralbanken, särskilt artikel 12.1 jämförd med artiklarna 3.1, 5, 12.3, 16–24 och 34, och

av följande skäl:

(1) Enligt Europaparlamentets och rådets förordning (EU) nr 910/2014 ([1]) ska Europaparlamentets och rådets direktiv 1999/93/EG ([2]) upphöra att gälla från och med den 1 juli 2016. Därför är det lämpligt att hänvisa till förordning (EU) nr 910/2014 i beslut ECB/2013/1 ([3]).

(2) Informationen om ECBS-PKI-certifikatutfärdaren, inklusive dess identitet och dess tekniska komponenter, som framgår av bilagan till beslut ECB/2013/1 måste uppdateras.

(3) Beslut ECB/2013/1 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar

Beslut ECB/2013/1 ska ändras på följande sätt:

1. I artikel 1 ska punkt 10 ersättas med följande:

”10. *ECBS-PKI-certifikatutfärdare*: den betrodda enhet som utfärdar, hanterar, återkallar och förnyar ECBS-PKI-certifikat i enlighet med ECBS/SSM ramverk för godkännande av certifikat.”

2. I artikel 4 ska punkt 4 ersättas med följande:

”4. ECBS-PKI-riktlinjer för certifiering innehåller regler för ett elektroniskt certifikats livscykel, från första begäran om utfärdande till dess att användningen upphör eller certifikatet återkallas, samt även regler som beskriver förhållandet mellan den som ansöker om ett certifikat eller är certifikatanvändare, ECBS-PKI-certifikatutfärdaren samt accepterande parter. De omfattar certifikat som faller inom tillämpningsområdet för direktiv 1999/93/EG och

([1]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).
([2]) Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12).
([3]) Europeiska centralbankens beslut ECB/2013/1 av den 11 januari 2013 om ett ramverk för en infrastruktur för kryptering med öppen nyckel (PKI) för Europeiska centralbankssystemet (EUT L 74, 16.3.2013, s. 30).

Europaparlamentets och rådets förordning (EU) nr 910/2014 (*) samt certifikat som faller utanför deras tillämpningsområden. De beskriver alla parters roller och ansvar samt reglerar hur certifikat ska utfärdas och hanteras. Riktlinjerna finns som bilaga till nivå 2/nivå 3-avtalet.

(*) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73)."

3. I artikel 10 ska inledningsfrasen och punkt 1 a ersättas med följande:

"1. Centralbankerna i Eurosystemet måste visa att de inte har varit vårdslösa, i annat fall ansvarar de, i enlighet med sitt ansvar och sina funktioner inom ECBS-PKI för all skada som åsamkas en användare som har rimlig anledning att förlita sig på ett kvalificerat certifikat, enligt definitionerna i direktiv 1999/93/EG och förordning (EU) nr 910/2014, för:

a) att all information i det kvalificerade certifikatet är korrekt vid tidpunkten för utfärdandet och att certifikatet innehåller alla de uppgifter som föreskrivs för ett kvalificerat certifikat enligt definitionerna i direktiv 1999/93/EG och förordning (EU) nr 910/2014,"

4. Bilagan ska ersättas av bilagan till det här beslutet.

Artikel 2

Ikraftträdande

Detta beslut träder i kraft den tredje dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Frankfurt am Main den 11 december 2015.

Mario DRAGHI

ECB:s ordförande

BILAGA

"BILAGA

Information om ECBS-PKI-certifikatutfärdaren, inklusive dess identitet och dess tekniska komponenter

ECBS-PKI-certifikatutfärdaren identifieras i sitt certifikat som utgivare och dennes privata nyckel används för att signera certifikat. ECBS-PKI-certifikatutfärdaren ska

i) utfärda certifikat för öppna och privata nycklar,

ii) publicera förteckningar över återkallade certifikat,

iii) generera nyckelpar som är associerade med specifika certifikat, t.ex. sådana som kräver att nycklar återskapas,

iv) ha det övergripande ansvaret för ECBS-PKI och säkerställa att alla kraven för att driva det uppfylls.

ECBS-PKI-certifikatutfärdaren inkluderar alla individer, regler, förfaranden och datorsystem som är betrodda att utfärda elektroniska certifikat och registrera dem på certifikatanvändarna.

ECBS-PKI-certifikatutfärdaren inkluderar två tekniska komponenter:

— **ECBS-PKI-certifikatutfärdaren på rotnivå**: Denna certifikatutfärdare, på den första nivån, utfärdar endast certifikat för sig själv och sina underordnade certifikatutfärdare. Den är endast verksam när den utför sina egna mycket begränsade uppgifter. Dess viktigaste kännetecken är:

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

Systemets unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Utfärdarens unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-06-21, kl. 11:58:26 till 2041-06-21, kl. 11:58:26
Kontrollsumma (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Kontrollsumma (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Krypteringsalgoritm	SHA-1/RSA 4096

b) SHA-256 certifikat:

Systemets unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

([1]) Detta certifikat används endast i system som inte stöder högre algoritmer.

Utfärdarens unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-06-21, kl. 12:35:34 till 2041-06-21, kl. 12:35:34
Kontrollsumma (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Kontrollsumma (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Krypteringsalgoritm	SHA-256/RSA 4096

— **Online ECBS-PKI-certifikatutfärdaren**: Denna certifikatutfärdare, på den andra nivån, är underordnad ECBS-PKI-certifikatutfärdaren på rotnivå. Den ansvarar för utfärdandet av ECBS-PKI-certifikat till användarna. Dess viktigaste kännetecken är:

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

Systemets unika namn	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Utfärdarens unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-07-22, kl. 12:46:35 till 2026-07-22, kl. 12:46:35
Kontrollsumma (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Kontrollsumma (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Krypteringsalgoritm	SHA-1/RSA 4096

b) SHA-256 certifikat:

Systemets unika namn	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Utfärdarens unika namn	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-07-22, kl. 12:46:35 till 2026-07-22, kl. 12:46:35
Kontrollsumma (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Kontrollsumma (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Krypteringsalgoritm	SHA-256/RSA 4096”

([1]) Detta certifikat används endast i system som inte stöder högre algoritmer.