AFGØRELSER

DEN EUROPÆISKE CENTRALBANKS AFGØRELSE (EU) 2016/187

af 11. december 2015

om ændring af afgørelse ECB/2013/1 om fastlæggelse af rammerne for en public key-infrastruktur for Det Europæiske System af Centralbanker (ECB/2015/46)

STYRELSESRÅDET FOR DEN EUROPÆISKE CENTRALBANK HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 127,

under henvisning til statutten for Det Europæiske System af Centralbanker og Den Europæiske Centralbank, særlig artikel 12.1 sammenholdt med artikel 3.1, artikel 5, artikel 12.3 samt artikel 16 til 24 og artikel 34, og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([1]) har ophævet Europa-Parlamentets og Rådets direktiv 1999/93/EF ([2]) med virkning fra 1. juli 2016. Det er derfor hensigtsmæssigt at henvise til forordning (EU) nr. 910/2014 i Den Europæiske Centralbanks afgørelse ECB/2013/1 ([3]).

(2) Oplysningerne om ESCB-PKI certificeringsmyndigheden, herunder dens identitet og tekniske komponenter, som fastsat i bilaget til afgørelse ECB/2013/1, bør opdateres.

(3) Afgørelse ECB/2013/1 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Ændringer

Afgørelse ECB/2013/1 ændres som følger:

1) Artikel 1, nr. 10, affattes således:

»10. »ESCB-PKI certificeringsmyndighed«: den enhed, som brugerne har tillid til, der udsteder, administrerer, tilbagekalder og fornyer ESCB-PKI certifikater i overensstemmelse med ESCB/SSM's rammer for godkendelse af certifikater«.

2) Artikel 4, stk. 4, affattes således:

»4. Erklæringen om certificeringspraksis for ESCB-PKI er et regelsæt, der dækker elektroniske certifikaters livscyklus fra den indledende anmodning til ophør af anvendelse eller tilbagekaldelse, samt forholdet mellem certifikatansøgeren eller -indehaveren, ESCB-PKI certificeringsmyndigheden og modtagerparterne. Det dækker både certifikater, der er omfattet af anvendelsesområdet for direktiv 1999/93/EF og Europa-Parlamentets og Rådets

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

([2]) Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12).

([3]) Den Europæiske Centralbanks afgørelse ECB/2013/1 af 11. januar 2013 om fastlæggelse af rammerne for en public key-infrastruktur for Det Europæiske System af Centralbanker (EUT L 74 af 16.3.2013, s. 30).

forordning (EU) nr. 910/2014 (*), og certifikater, som ikke er omfattet af anvendelsesområdet for disse. Det fastsætter også alle parters roller og ansvar og fastlægger procedurerne for udstedelse og administration af certifikater. Det indgår som bilag til niveau 2-niveau 3-aftalen.

(*) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).«

3) Artikel 10, stk. 1, indledningen og litra a), affattes således:

»1. Medmindre de godtgør, at de ikke har handlet uagtsomt, ifalder centralbankerne i Eurosystemet erstatningsansvar i overensstemmelse med deres opgaver og ansvar i ESCB-PKI for ethvert tab, der påføres en bruger, som med rimelighed forlader sig på et kvalificeret certifikat, som defineret i direktiv 1999/93/EF og forordning (EU) nr. 910/2014, for så vidt angår:

a) korrektheden af alle oplysningerne i det kvalificerede certifikat på udstedelsestidspunktet og spørgsmålet om, hvorvidt certifikatet indeholder alle de for et kvalificeret certifikat foreskrevne angivelser, som defineret i direktiv 1999/93/EF og forordning (EU) nr. 910/2014«.

4) Bilaget erstattes af bilaget til denne afgørelse.

Artikel 2

Ikrafttrædelse

Denne afgørelse træder i kraft på tredjedagen efter dens offentliggørelse i *Den Europæiske Unions Tidende*.

Udfærdiget i Frankfurt am Main, den 11. december 2015.

Mario DRAGHI

Formand for ECB

BILAG

»BILAG

Oplysninger om ESCB-PKI certificeringsmyndigheden, herunder dens identitet og tekniske komponenter

ESCB-PKI certificeringsmyndigheden identificeres i dets certifikat som udsteder, og dets private nøgle anvendes til at signere certifikater. ESCB-PKI certificeringsmyndigheden er ansvarlig for:

i) udstedelsen af private og offentlige nøglecertifikater

ii) udstedelsen af tilbagekaldelseslister

iii) genereringen af nøglepar knyttet til specifikke certifikater, f.eks. certifikater, der kræver nøglegenskabelse

iv) det overordnede ansvar for ESCB-PKI og sikring af, at alle krav, der er nødvendige for driften, er opfyldt.

ESCB-PKI certificeringsmyndigheden omfatter alle individer, politikker, procedurer og computersystemer, der har til opgave at udstede elektroniske certifikater og at tildele disse til certifikatindehaverne.

ESCB-PKI certificeringsmyndigheden har to tekniske komponenter:

— **ESCB-PKI rodcertificeringsmyndigheden**: Denne certificeringsmyndighed på første niveau udsteder kun certifikater til sig selv og til dets underordnede certificeringsmyndigheder. Den er kun i drift, når den udfører sine egne snævert definerede opgaver. Følgende data udgør dens væsentligste data:

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

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

b) SHA-256 certifikat:

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

([1]) Dette certifikat vil kun blive benyttet i systemer, der ikke understøtter højere algoritmer.

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

— **ESCB-PKI onlinecertificeringsmyndigheden**: Denne certificeringsmyndighed på andet niveau er underordnet ESCB-PKI rodcertificeringsmyndigheden. Den har ansvaret for udstedelsen af ESCB-PKI certifikater til brugerne. Følgende data udgør dens væsentligste data:

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

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

b) SHA-256 certifikat:

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

([1]) Dette certifikat vil kun blive benyttet i systemer, der ikke understøtter højere algoritmer.