BESLUITEN

BESLUIT (EU) 2016/187 VAN DE EUROPESE CENTRALE BANK

van 11 december 2015

houdende wijziging van Besluit ECB/2013/1 tot vaststelling van het kader voor een publieke sleutelinfrastructuur voor het Europees Stelsel van centrale banken (ECB/2015/46)

DE RAAD VAN BESTUUR VAN DE EUROPESE CENTRALE BANK

Gezien het Verdrag betreffende de werking van de Europese Unie, met name artikel 127,

Gezien de Statuten van het Europees Stelsel van centrale banken en van de Europese Centrale Bank, met name artikel 12.1 in samenhang met artikel 3.1, artikel 5, artikel 12.3 en artikel 16 tot en met 24 en 34,

Overwegende:

(1) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([1]) heeft Richtlijn 1999/93/EG van het Europees Parlement en de Raad ([2]) met ingang van 1 juli 2016 ingetrokken. Het is derhalve aangewezen om in Besluit ECB/2013/1 te verwijzen naar Verordening (EU) nr. 910/2014 ([3]).

(2) Informatie betreffende de ESCB-PKI-certificeringsautoriteit, met inbegrip van haar identiteit, en de technische onderdelen ervan, zoals uiteengezet in de bijlage bij Besluit ECB/2013/1, moet bijgewerkt worden.

(3) Besluit ECB/2013/1 moet derhalve dienovereenkomstig gewijzigd worden,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Wijzigingen

Besluit ECB/2013/1 wordt als volgt gewijzigd:

1) Artikel 1, punt 10 als volgt vervangen:

„10. „ESCB-PKI-certificeringsautoriteit": de door gebruikers vertrouwde entiteit voor de uitgifte, het beheer, de intrekking en vernieuwing van certificaten namens de centrale banken van het ESCB of de centrale banken van het Eurosysteem conform het ESCB-/SSM-kader voor de acceptatie van certificaten;".

2) Artikel 4, lid 4 als volgt vervangen:

„4. De ESCB-PKI-certificatiepraktijkverklaring is een stel regels dat de levenscyclus van elektronische certificaten regelt, vanaf het eerste verzoek tot intekening en/of intrekking, alsook de relaties tussen de aanvrager van of intekenaar op het certificaat, de ESCB-PKI-certificeringsautoriteit en de vertrouwende partijen. De verklaring bestrijkt

([1]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

([2]) Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PB L 13 van 19.1.2000, blz. 12).

([3]) Besluit ECB/2013/1 van de Europese Centrale Bank van 11 januari 2013 tot vaststelling van het kader voor een publieke sleutelinfrastructuur voor het Europees Stelsel van centrale banken (PB L 74 van 16.3.2013, blz. 30).

elektronische certificaten die binnen het toepassingsgebied van Richtlijn 1999/93/EG en Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad (*) vallen, en elektronische certificaten die buiten het toepassingsgebied ervan vallen. De verklaring zet ook de rollen en verantwoordelijkheden van alle partijen uiteen en stelt de procedures vast betreffende de afgifte en het beheer van certificaten. De verklaring wordt als bijlage bij de Niveau 2-Niveau 3-overeenkomst gevoegd.

(*) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).".

3) In artikel 10 worden de inleidende zin en punt a) van lid 1 als volgt vervangen:

„1. Tenzij zij bewijzen niet nalatig te hebben gehandeld, zijn de centrale banken van het Eurosysteem aansprakelijk conform hun functies en verantwoordelijkheden in de ESCB-PKI voor elke schade veroorzaakt aan een gebruiker die in redelijkheid op een gekwalificeerd certificaat heeft vertrouwd zoals gedefinieerd in Richtlijn 1999/93/EG en Verordening (EU) nr. 910/2014, wat betreft:

a) de juistheid, op het tijdstip van uitgifte, van alle gegevens in een gekwalificeerd certificaat en de opneming in het certificaat van alle gegevens voorgeschreven voor een gekwalificeerd certificaat, zoals gedefinieerd in Richtlijn 1999/93/EG en Verordening (EU) nr. 910/2014;".

4) De bijlage wordt vervangen door de bijlage bij dit besluit.

Artikel 2

Inwerkingtreding

Dit besluit treedt in werking op de derde dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Frankfurt am Main, 11 december 2015.

De president van de ECB

Mario DRAGHI

BIJLAGE

„BIJLAGE

Informatie betreffende de ESCB-PKI-certificeringsautoriteit, waaronder de identiteit en technische componenten daarvan

De ESCB-PKI-certificeringsautoriteit wordt in haar certificaat geïdentificeerd als de uitgever en haar privésleutel wordt gebruikt om certificaten te ondertekenen. De ESCB-PKI-certificeringsautoriteit is belast met:

i) het uitgeven van certificaten met geheime sleutels en publieke sleutels;

ii) het publiceren van intrekkingslijsten;

iii) het genereren van sleutelparen verbonden met specifieke certificaten, bijv. waarvoor een sleutel dient te worden achterhaald;

iv) het dragen van de algehele verantwoordelijkheid voor de ESCB-PKI en het verzekeren dat aan alle vereisten is voldaan die nodig zijn voor de exploitatie ervan.

De ESCB-PKI-certificeringsautoriteit omvat alle natuurlijke personen, beleidslijnen, procedures en computersystemen waaraan de uitgifte van elektronische certificaten en de toewijzing daarvan aan de intekenaars op certificaten zijn toevertrouwd.

De ESCB-PKI-certificeringsautoriteit omvat twee technische componenten:

— **De root-ESCB-PKI-certificeringsautoriteit**: deze certificeringsautoriteit, op het hoogste niveau, geeft alleen certificaten uit voor zichzelf en haar ondergeschikte certificeringsautoriteiten. Zij is alleen actief bij het uitvoeren van haar eigen nauwkeurig afgebakende verantwoordelijkheden. Haar belangrijkste gegevens zijn:

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

Distinguished name (Distinguished name)	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 (Distinguished name van de uitgevende instantie)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Geldigheidsperiode)	From 21.6.2011 11:58:26 to 21.6.2041 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 (encryptiealgoritmen)	SHA-1/RSA 4096

b) SHA-256 certificaat:

Distinguished name	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]) Dit certificaat wordt alleen in systemen gebruikt die geen hogere algoritmes ondersteunen.

Distinguished name of issuer (Distinguished name van de uitgevende instantie)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Geldigheidsperiode)	From 21.6.2011 12:35:34 to 21.6.2041 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 (encryptiealgoritmen)	SHA-256/RSA 4096

— **De online ESCB-PKI-certificeringsautoriteit:** Deze certificeringsautoriteit, op het tweede niveau, is ondergeschikt aan de root-ESCB-PKI-certificeringsautoriteit. Zij is verantwoordelijk voor het afgeven van ESCB-PKI-certificaten voor gebruikers. Haar belangrijkste gegevens zijn:

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

Distinguished name (Distinguished name)	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 (Distinguished name van de uitgevende instantie)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Geldigheidsperiode)	From 22.7.2011 12:46:35 to 22.7.2026 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 (encryptiealgoritmen)	SHA-1/RSA 4096

b) SHA-256 certificaat:

Distinguished name (Distinguished name)	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 (Distinguished name van de uitgevende instantie)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Geldigheidsperiode)	From 22.7.2011 12:46:35 to 22.7.2026 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 (encryptiealgoritmen)	SHA-256/RSA 4096”

([1]) Dit certificaat wordt alleen in systemen gebruikt die geen hogere algoritmes ondersteunen.