DECISIONES

DECISIÓN (UE) 2016/187 DEL BANCO CENTRAL EUROPEO

de 11 de diciembre de 2015

que modifica la Decisión BCE/2013/1 por la que se establece el marco de una infraestructura de clave pública para el Sistema Europeo de Bancos Centrales (BCE/2015/46)

EL CONSEJO DE GOBIERNO DEL BANCO CENTRAL EUROPEO,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, el artículo 127,

Vistos los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo y, en particular, el artículo 12.1 en relación con los artículos 3.1, 5, 12.3, 16 a 24 y 34,

Considerando lo siguiente:

(1) El Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([1]) ha derogado la Directiva 1999/93/CE del Parlamento Europeo y del Consejo ([2]) con efectos a partir del 1 de julio de 2016. Por tanto, procede remitir al Reglamento (UE) n.º 910/2014 en la Decisión BCE/2013/1 ([3]).

(2) Debe actualizarse la información relativa a la autoridad certificadora de la ESCB-PKI, inclusive su identidad y sus componentes técnicos, como se establece en el anexo de la Decisión BCE/2013/1.

(3) Debe modificarse en consecuencia la Decisión BCE/2013/1.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Modificaciones

La Decisión BCE/2013/1 se modifica como sigue:

1) En el artículo 1, el punto 10 se sustituye por el siguiente:

«10) "autoridad certificadora de la ESCB-PKI", la entidad en que confían los usuarios para que emita, gestione, revoque y renueve los certificados de la ESCB-PKI de acuerdo con el marco de aceptación de certificados del SEBC/MUS;».

2) En el artículo 4, el apartado 4 se sustituye por el siguiente:

«4. La declaración de prácticas de certificación de la ESCB-PKI es el conjunto de normas que rigen el ciclo de vida de los certificados electrónicos, desde su solicitud inicial hasta el final o la revocación de la suscripción, así como las relaciones entre el solicitante o firmante del certificado, la autoridad certificadora de la ESCB-PKI y los aceptantes de certificados. Comprende tanto los certificados incluidos en el ámbito de aplicación de la Directiva 1999/93/CE y del

([1]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

([2]) Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (DO L 13 de 19.1.2000, p. 12).

([3]) Decisión BCE/2013/1 del Banco Central Europeo, de 11 de enero de 2013, por la que se establece el marco de una infraestructura de clave pública para el Sistema Europeo de Bancos Centrales (DO L 74 de 16.3.2013, p. 30).

Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo (*) como los no incluidos en dicho ámbito. Además, expone los deberes y funciones de todas las partes y establece los procedimientos relativos a la emisión y gestión de los certificados. Se adjunta como anexo al acuerdo entre el nivel 2 y el 3.

(*) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).».

3) En el artículo 10, la frase introductoria y la letra a) del apartado 1 se sustituyen por las siguientes:

«1. Salvo que demuestren que no han actuado de manera negligente, los bancos centrales del Eurosistema responderán, de acuerdo con sus deberes y funciones en la ESCB-PKI, de los daños que causen a los usuarios que hayan confiado razonablemente en un certificado reconocido conforme a la definición de la Directiva 1999/93/CE y del Reglamento (UE) n.º 910/2014, en lo referente a:

a) la veracidad, en el momento de su emisión, de toda la información contenida en el certificado reconocido, y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos conforme se definen en la Directiva 1999/93/CE y el Reglamento (UE) n.º 910/2014;».

4) El anexo se sustituye por el anexo de la presente decisión.

Artículo 2

Entrada en vigor

La presente decisión entrará en vigor el tercer día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Fráncfort del Meno, el 11 de diciembre de 2015.

El presidente del BCE
Mario DRAGHI

ANEXO

«ANEXO

Información relativa a la autoridad certificadora de la ESCB-PKI, inclusive su identidad y sus componentes técnicos

La autoridad certificadora de la ESCB-PKI se identifica en su certificado como emisor, y su clave privada se utiliza para firmar certificados. La autoridad certificadora de la ESCB-PKI se encarga de:

i) emitir certificados de clave privada y pública;

ii) emitir listas de revocación;

iii) generar pares de claves asociados a certificados específicos, por ejemplo los que precisan de recuperación de clave;

iv) responder en general de la ESCB-PKI y velar por que se cumplan todos los requisitos necesarios para su funcionamiento.

La autoridad certificadora de la ESCB-PKI la componen todas las personas, políticas, procedimientos y sistemas informáticos a los que se confía la emisión de certificados electrónicos y su asignación a los firmantes de certificados.

La autoridad certificadora de la ESCB-PKI incluye dos componentes técnicos:

— **Autoridad certificadora raíz de la ESCB-PKI**: Esta autoridad certificadora de primer nivel únicamente emite certificados para sí misma y para sus autoridades certificadoras subordinadas. Funciona exclusivamente para el desempeño de sus propias funciones estrictamente definidas. Sus datos más relevantes son los siguientes:

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

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

b) Certificado SHA-256:

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

([1]) Este certificado se utilizará únicamente en sistemas que no admitan algoritmos más altos.

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

— **Autoridad certificadora en línea de la ESCB-PKI**: Esta autoridad certificadora de segundo nivel está subordinada a la autoridad certificadora raíz de la ESCB-PKI. Se encarga de emitir los certificados de la ESCB-PKI para usuarios. Sus datos más relevantes son los siguientes:

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

Distinguished name (Nombre distinguido)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Número de serie)	2C13 E18F FDB5 91CE 4E9 550B B5A3 F59C
Distinguished name of issuer (Nombre distinguido del emisor)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Período de validez)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (digesto de mensaje) (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message Digest (Digesto de mensaje) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (Algoritmos criptográficos)	SHA-1/RSA 4096

b) Certificado SHA-256:

Distinguished name (Nombre distinguido)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Número de serie)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of Issuer (Nombre distinguido del emisor)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Período de validez)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (digesto de mensaje) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message Digest (Digesto de mensaje) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (Algoritmos criptográficos)	SHA-256/RSA 4096»

([1]) Este certificado se utilizará únicamente en sistemas que no admitan algoritmos más altos.