

DECISIONES

DECISIÓN 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

(BCE/2013/1)

(2013/132/UE)

EL CONSEJO DE GOBIERNO DEL BANCO CENTRAL EUROPEO,

(4) Son pocos los bancos centrales del SEBC que poseen su propia infraestructura de clave pública, y muchos usuarios de terceros que trabajan con bancos centrales del SEBC carecen de un acceso ágil a una autoridad certificadora aceptada por el SEBC de acuerdo con su marco de aceptación de certificados.

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

Vistos los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo (en adelante, «los Estatutos del SEBC»), en particular, el artículo 12.1 en relación con los artículos 3.1, 5, 12.3 y 16 a 24,

(5) Es preciso que el Eurosistema cree una infraestructura de clave pública propia capaz de emitir todo tipo de certificados electrónicos, tales como certificados personales y técnicos para usuarios del SEBC o ajenos al SEBC, y lo bastante flexible como para adaptarse a la evolución de las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema. Esta infraestructura de clave pública (en adelante, «la ESCB-PKI») debe complementar los servicios que prestan otras autoridades certificadoras aceptadas por el SEBC de acuerdo con su marco de aceptación de certificados o las autoridades certificadoras aceptadas por el SEBC a los efectos de TARGET2 y TARGET2 Securities.

Considerando lo siguiente:

(1) Conforme al artículo 12.1 de los Estatutos del SEBC, el Consejo de Gobierno adopta las orientaciones y decisiones necesarias para garantizar el cumplimiento de las funciones asignadas al Sistema Europeo de Bancos Centrales (SEBC) y al Eurosistema con arreglo al Tratado y a los Estatutos del SEBC. Ello incluye la facultad de decidir acerca de la organización de las actividades auxiliares necesarias para el cumplimiento de esas funciones, tales como la emisión y gestión de certificados electrónicos para proteger la información almacenada y tratada en las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema, y para la transmisión de datos desde y hacia estos.

(6) El 29 de septiembre de 2010 el Consejo de Gobierno decidió poner en marcha el proyecto ESCB-PKI a fin de crear la ESCB-PKI y aportar los recursos necesarios para implantarla. El Consejo de Gobierno decidió que el Banco de España fuera el encargado de crear, albergar y gestionar la ESCB-PKI.

(2) Conforme al artículo 12.3 de los Estatutos del SEBC, el Consejo de Gobierno tiene la facultad igualmente de decidir acerca de la organización interna del Banco Central Europeo (BCE) y sus órganos rectores. Consecuentemente, el Consejo de Gobierno tiene la facultad de decidir que el BCE utilice certificados electrónicos emitidos por la infraestructura de clave pública propia del Eurosistema.

(7) La ESCB-PKI apoya indirectamente la ejecución de las tareas del SEBC y del Eurosistema. Se basa en tres niveles de gobierno: el nivel 1 lo forman el Consejo de Gobierno y el Comité Ejecutivo; el nivel 2, los bancos centrales del Eurosistema, y, el nivel 3, el banco central proveedor.

(3) Va en aumento el número de usuarios que acceden a un número cada vez mayor de aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema en constante evolución. El Consejo de Gobierno ha determinado la necesidad de dotarse de servicios de seguridad de la información avanzados, tales como autenticación fuerte, firmas electrónicas y encriptado, mediante el uso de certificados electrónicos.

(8) En el nivel 1, el Consejo de Gobierno se encarga de la dirección, administración y control de las actividades y productos necesarios para la creación y gestión de la ESCB-PKI. Se encarga también de la toma de decisiones en relación con la ESCB-PKI, incluida la asignación de funciones no encomendadas expresamente a los niveles 2 o 3.

(9) Los bancos centrales del Eurosistema se encargan de las funciones asignadas al nivel 2, dentro del marco general establecido por el Consejo de Gobierno, y tienen competencias relacionadas con los medios técnicos necesarios para implantar la ESCB-PKI.

- (10) El Comité de Tecnología Informática (ITC) del SEBC dirige la creación de la ESCB-PKI. Orienta, evalúa, controla y aprueba los productos del proyecto con arreglo a los criterios de aceptación acordes con el marco de aceptación de certificados del SEBC y el ámbito de aplicación y el calendario aprobados por el Consejo de Gobierno.
- (11) En el nivel 3, se ha nombrado al Banco de España banco central proveedor, encargado de realizar las funciones que se le asignan en el marco general que establezca el Consejo de Gobierno. El banco central proveedor ha puesto en marcha la infraestructura técnica y los dispositivos y servicios seguros necesarios para crear y utilizar una infraestructura de clave pública de acuerdo con: a) en la medida aplicable, la ley nacional que implementa la 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 ⁽¹⁾; b) en la medida aplicable, la ley nacional que implementa la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ⁽²⁾, y c) el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ⁽³⁾.
- (12) Puesto que los certificados electrónicos son elementos de utilización esencial en las aplicaciones electrónicas tanto como mecanismo de autenticación para implantar las firmas electrónicas como para el encriptado basado en claves públicas, la ESCB-PKI tendrá en cuenta las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema ya existentes y los proyectos del SEBC actualmente en marcha a fin de garantizar que sus necesidades queden cubiertas.
- (13) Los bancos centrales nacionales (BCN) no pertenecientes a la zona del euro pueden optar por utilizar los certificados y servicios que facilite la ESCB-PKI.
- 2) «aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema», las aplicaciones, sistemas, plataformas y servicios electrónicos que utilizan el SEBC o el Eurosistema o ambos al ejecutar las funciones que les corresponden de acuerdo con el Tratado y los Estatutos del SEBC;
- 3) «infraestructura de clave pública» o «PKI», el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para la prestación de servicios de autenticación, encriptado, integridad y no repudio por medio de criptografía de claves públicas y privadas y certificados electrónicos;
- 4) «usuario», un firmante de certificado o un aceptante de certificado, o ambos;
- 5) «autenticación», el proceso de comprobación de la identidad de un solicitante de certificado o de un firmante de certificado;
- 6) «banco central del SEBC», un banco central tanto del Eurosistema como no perteneciente a la zona del euro;
- 7) «banco central del Eurosistema», un BCN de un Estado miembro cuya moneda es el euro, incluido el banco central proveedor, o el BCE;
- 8) «banco central proveedor», el BCN al que el Consejo de Gobierno ha encargado crear la ESCB-PKI y prestar los servicios de ESCB-PKI en nombre de los bancos centrales del Eurosistema y en su beneficio;
- 9) «BCN no perteneciente a la zona del euro», un BCN de un Estado miembro cuya moneda no es el euro;
- 10) «autoridad certificadora de la ESCB-PKI», la entidad en que confían los usuarios para que emita, gestione, revoque y renueve certificados en nombre de los bancos centrales del SEBC o de los bancos centrales del Eurosistema de acuerdo con el marco de aceptación de certificados del SEBC;
- 11) «autoridad validadora de la ESCB-PKI», la entidad en que confían los usuarios para que proporcione información sobre la validez de los certificados emitidos por la autoridad certificadora de la ESCB-PKI;
- 12) «firmante de certificado», bien una persona a la que se refiere un certificado electrónico y para quien se ha emitido, bien un gestor de componentes técnicos que ha aceptado un certificado electrónico emitido por la autoridad certificadora de la ESCB-PKI respecto de un componente técnico, o ambos;
- 13) «marco de aceptación de certificados del SEBC», los criterios establecidos por el ITC del SEBC para determinar las autoridades certificadoras, internas del SEBC o externas a él, en

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Definiciones

A los efectos de la presente Decisión, se entenderá por:

- 1) «certificado» o «certificado electrónico», un archivo electrónico, emitido por una autoridad certificadora, que asocia una clave pública a una identidad de firmante de certificado y que se utiliza para todas o algunas de las siguientes finalidades: a) para comprobar que una clave pública pertenece a un firmante de certificado; b) para autenticar a un firmante de certificado; c) para comprobar la firma del firmante de un certificado; d) para encriptar un mensaje dirigido a un firmante de certificado, y e) para comprobar los derechos de acceso de un firmante de certificado a las

⁽¹⁾ DO L 13 de 19.1.2000, p. 12.

⁽²⁾ DO L 281 de 23.11.1995, p. 31.

⁽³⁾ DO L 8 de 12.1.2001, p. 1.

las que se puede confiar a los efectos de las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema;

- 14) «autoridad de registro», una entidad en que confían los usuarios para comprobar la identidad de los solicitantes de certificados antes de que estos sean emitidos por la autoridad certificadora de la ESBC-PKI;
- 15) «aceptante de certificado», una persona o entidad distinta del firmante de certificado que acepta un certificado y confía en él;
- 16) «política de auditoría», la política de auditoría del SEBC establecida el 7 de octubre de 1998 por el Consejo de Gobierno y publicada en la dirección del BCE en internet ⁽¹⁾;
- 17) «solicitante de certificado», una persona que solicita la emisión de un certificado para sí o para un componente técnico;
- 18) «componente técnico», cualquier componente físico o lógico que pueda identificarse mediante el uso de certificados electrónicos.

Artículo 2

Ámbito de aplicación

1. La presente Decisión establece el marco de la ESCB-PKI. La ESCB-PKI es la infraestructura de clave pública propia del Eurosistema creada por el banco central proveedor en nombre de los bancos centrales del Eurosistema y en su beneficio, que emite, gestiona, revoca y renueva certificados de acuerdo con el marco de aceptación de certificados del SEBC.
2. Dado que los servicios de ESCB-PKI pueden afectar a los aceptantes de certificados, en la presente Decisión se establecen además las condiciones en que dichos aceptantes pueden confiar en los certificados de ESCB-PKI.

Artículo 3

Alcance y objetivos de la ESCB-PKI

1. Únicamente podrán acceder a las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema de nivel crítico medio o superior a medio, y utilizarlos, los usuarios que hayan sido autenticados mediante un certificado electrónico emitido y gestionado por autoridades certificadoras aceptadas por el SEBC de acuerdo con el marco de aceptación de certificados del SEBC, incluida la autoridad certificadora de la ESBC-PKI, o por autoridades certificadoras aceptadas por el SEBC a los efectos de TARGET2 y TARGET2 Securities.
2. La autoridad certificadora de la ESBC-PKI emitirá certificados electrónicos y prestará otros servicios de certificación electrónica a los firmantes de certificados de los bancos centrales del SEBC y de terceros que trabajen con estos a fin de permitirles un acceso y utilización seguros de las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema.

3. La ESCB-PKI prestará los siguientes servicios de certificación:

- a) emisión, renovación y revocación de certificados, y confirmación de validez de certificados en relación con diferentes tipos de certificados;
- b) emisión de certificados de autenticación, firma electrónica y encriptado en relación con usuarios del SEBC y externos al SEBC, y emisión de certificados técnicos;
- c) recuperación de claves privadas para asegurar la recuperación de información encriptada basada en claves públicas en caso de pérdida de certificados;
- d) entrega y gestión de dispositivos criptográficos para los firmantes de certificados en caso necesario;
- e) suministro de información acerca de los procedimientos de gestión de certificados de ESCB-PKI, y apoyo técnico a los jefes de proyecto del SEBC a fin de ayudarles a integrar los certificados de ESCB-PKI en sus aplicaciones.

En el futuro podrán añadirse otros servicios según lo requieran las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema.

Artículo 4

Marco de la ESCB-PKI

1. Con sujeción a lo establecido en la presente Decisión, los deberes y funciones del banco central proveedor y de los demás bancos centrales del Eurosistema en relación con la implantación, funcionamiento y uso de la ESCB-PKI se establecerán mediante un acuerdo entre el nivel 2 y el nivel 3 y se detallarán en las políticas de certificados de ESCB-PKI y en la declaración de prácticas de certificación de ESCB-PKI.
2. El acuerdo entre el nivel 2 y el nivel 3, que incluye el acuerdo de nivel de servicio, contiene el acuerdo negociado entre el banco central proveedor y los bancos centrales del Eurosistema en cuanto a los deberes y funciones respectivos. El acuerdo se someterá a la aprobación del Consejo de Gobierno antes de su firma por el banco central proveedor y los bancos centrales del Eurosistema.
3. El acuerdo de nivel de servicio establece el nivel de los servicios que debe prestar el banco central proveedor al Eurosistema y el nivel de los servicios que debe prestar el Eurosistema a los BCN no pertenecientes a la zona del euro y a terceros en relación con la ESCB-PKI.
4. La declaración de prácticas de certificación de 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 ESBC-PKI y los aceptantes de certificados. Comprende tanto los certificados electrónicos que pertenecen al ámbito de aplicación de la Directiva 1999/93/CE como los que se encuentran fuera de 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 nivel 3.

⁽¹⁾ www.ecb.europa.eu.

5. Una política de certificados de ESCB-PKI es un conjunto de normas aplicables a cada tipo de certificado que se emite. Cada política detalla la aplicación de la declaración de prácticas de certificación de ESCB-PKI de cada tipo de certificado emitido. Las políticas de certificados de ESCB-PKI se adjuntan como anexos al acuerdo entre el nivel 2 y el nivel 3.

6. Las políticas de certificados de ESCB-PKI y la declaración de prácticas de certificación de ESCB-PKI se publicarán en la dirección de la ESCB-PKI en internet ⁽¹⁾.

7. La información relativa a la autoridad certificadora de la ESCB-PKI, incluidos sus datos identificativos y sus componentes técnicos, figura en el anexo a la presente Decisión.

Artículo 5

Deberes y funciones del banco central proveedor

1. El banco central proveedor se encargará, en beneficio de los bancos centrales del Eurosistema, del funcionamiento y mantenimiento de la ESCB-PKI, incluidas las funciones de albergar, operar y gestionar la infraestructura de conformidad con el acuerdo entre el nivel 2 y el nivel 3. En particular, el banco central proveedor entregará los certificados y prestará los servicios de ESCB-PKI de acuerdo con requisitos de negocio y especificaciones técnicas tales como el marco de aceptación de certificados del SEBC y los requisitos y especificaciones establecidos en el acuerdo entre el nivel 2 y el nivel 3.

2. El banco central proveedor se dotará de la infraestructura organizativa necesaria para crear, emitir y gestionar certificados, y garantizará el mantenimiento de dicha infraestructura. A tal fin, en consulta con el ITC, el banco central proveedor podrá adoptar normas sobre su organización y administración internas.

3. El banco central proveedor actuará como la autoridad certificadora de la ESCB-PKI y como la autoridad validadora de la ESCB-PKI.

4. El acuerdo entre el nivel 2 y el nivel 3 establecerá el régimen de responsabilidad aplicable al banco central proveedor.

Artículo 6

Deberes y funciones de los bancos centrales del Eurosistema

1. Cada banco central del Eurosistema se encargará de identificar a sus firmantes de certificados y, para llevar a cabo esta función, creará el puesto de encargado de registro, que será la persona autorizada para registrar a terceros usuarios.

2. Cada banco central del Eurosistema actuará como aceptante de certificado en relación con los certificados para encriptado y firma electrónica emitidos por la ESCB-PKI para los firmantes de certificados de otros bancos centrales del Eurosistema o de terceros usuarios.

3. Cada banco central del Eurosistema que utilice servicios de ESCB-PKI actuará como autoridad de registro para sus solicitantes de certificados, y velará por que estos acepten y apliquen las condiciones para usuarios que constan en el formulario de solicitud de servicios de la autoridad certificadora de la ESCB-PKI.

Artículo 7

Relaciones entre los bancos centrales del Eurosistema, los terceros y los firmantes de certificados

Cada banco central del Eurosistema implantará medidas para el acceso seguro por terceros a las aplicaciones, sistemas, plataformas y servicios electrónicos del SEBC y del Eurosistema, y para el uso seguro por terceros de dichas aplicaciones, sistemas, plataformas y servicios, mediante la utilización de certificados de ESCB-PKI. Estas medidas se aplicarán exclusivamente a la relación entre el correspondiente banco central del Eurosistema y los terceros que utilicen los certificados de ESCB-PKI. Todos los terceros observarán las políticas de certificados de ESCB-PKI, la declaración de prácticas de certificación de ESCB-PKI y las condiciones para usuarios que constan en el formulario de solicitud de servicios de la autoridad certificadora de la ESCB-PKI.

Artículo 8

Relaciones con los aceptantes de certificados

Se podrá confiar en un certificado electrónico emitido de acuerdo con la presente Decisión siempre que su aceptante:

- compruebe la validez, la suspensión o la revocación del certificado utilizando a tal fin información actual sobre el estado de revocación;
- tenga en cuenta cualquier limitación de uso especificada en el certificado, y
- acepte la declaración de prácticas de certificación de ESCB-PKI y las políticas de certificados de ESCB-PKI aplicables.

Artículo 9

Derechos respecto de la ESCB-PKI

1. Los bancos centrales del Eurosistema son plenos propietarios de la ESCB-PKI.

2. En consecuencia, el banco central proveedor concederá a los bancos centrales del Eurosistema, en la medida de lo posible de conformidad con la legislación aplicable, todas las licencias sobre derechos de propiedad intelectual necesarias para que los bancos centrales del Eurosistema puedan utilizar la ESCB-PKI y sus componentes y la totalidad de los servicios de ESCB-PKI, y puedan además prestar los servicios de ESCB-PKI a terceros de acuerdo con la declaración de prácticas de certificación de ESCB-PKI y las políticas de certificados de ESCB-PKI. El banco central proveedor responderá ante los bancos centrales del Eurosistema de toda reclamación de terceros por vulneración de derechos de propiedad intelectual.

3. Los detalles acerca de los derechos de los bancos centrales del Eurosistema respecto de la ESCB-PKI se acordarán entre el nivel 2 y el nivel 3 y figurarán en el acuerdo entre el nivel 2 y el nivel 3.

Artículo 10

Responsabilidad de los bancos centrales del Eurosistema frente a los usuarios

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

⁽¹⁾ <http://pki.escb.eu>.

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, 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;
- b) la garantía de que, en el momento de la emisión del certificado reconocido, el firmante de certificado identificado en el mismo estaba en posesión de los datos de creación de firma correspondientes a los datos de verificación de firma facilitados o identificados en el certificado;
- c) la garantía de que el dispositivo de creación de firma y el dispositivo de verificación de firma funcionan juntos de manera complementaria en los casos en que la ESCB-PKI genere ambos;
- d) la ausencia de registro de la revocación de un certificado reconocido.

2. Los bancos centrales del Eurosistema no asumen compromisos, garantías o responsabilidades frente a los usuarios que no se hayan establecido expresamente en la presente Decisión y en la declaración de prácticas de certificación de ESCB-PKI.

Artículo 11

Participación en la ESCB-PKI de los BCN no pertenecientes a la zona del euro

1. Un BCN no perteneciente a la zona del euro podrá actuar como autoridad de registro respecto de sus usuarios internos y de terceros usuarios, y podrá crear el puesto de encargado de registro para desempeñar esta función.

2. Si lo autoriza el Consejo de Gobierno, un BCN no perteneciente a la zona del euro podrá igualmente optar por utilizar los servicios de ESCB-PKI en las mismas condiciones que las aplicables a los bancos centrales del Eurosistema. A tal fin, el BCN no perteneciente a la zona del euro presentará una declaración al Consejo de Gobierno en la que confirme que cumplirá las obligaciones establecidas en la presente Decisión y en el acuerdo entre el nivel 2 y el nivel 3. Los BCN no pertenecientes a la zona del euro no se convertirán en copropietarios de la ESCB-PKI ni estarán obligados a contribuir a su sobre financie-

Artículo 12

Protección de datos

Los bancos centrales del Eurosistema observarán la legislación de protección de datos aplicable al tratamiento de datos personales que lleven a cabo en el desempeño de sus funciones relativas a la ESCB-PKI.

Artículo 13

Auditoría

Las auditorías de la ESCB-PKI se llevarán a cabo de acuerdo con los principios y disposiciones de la política de auditoría. Estas auditorías se entenderán sin perjuicio de los controles internos y las normas de auditoría que se apliquen a los bancos centrales del Eurosistema o que estos adopten.

Artículo 14

Disposiciones financieras

Los bancos centrales del Eurosistema correrán con los gastos de creación y funcionamiento de la ESCB-PKI conforme se especifique en el sobre financiero.

Artículo 15

Función del Comité Ejecutivo

1. De acuerdo con el artículo 17.3 de la Decisión BCE/2004/2, de 19 de febrero de 2004, por la que se adopta el Reglamento interno del Banco Central Europeo ⁽¹⁾, el Consejo de Gobierno delega sus poderes normativos en el Comité Ejecutivo para que adopte las medidas de aplicación de la presente Decisión que sean necesarias para la eficiencia y seguridad de la ESCB-PKI, así como las modificaciones relativas a los aspectos técnicos de la ESCB-PKI y sus servicios previstos en los anexos del acuerdo entre el nivel 2 y el nivel 3, una vez obtenido el asesoramiento del ITC y, en su caso, del Comité Directivo de Tecnologías de la Información del Eurosistema.

2. El Comité Ejecutivo notificará al Consejo de Gobierno sin demoras injustificadas toda medida que adopte en virtud del apartado 1, y acatará toda decisión del Consejo de Gobierno al respecto.

Hecho en Fráncfort del Meno, el 11 de enero de 2013.

El Presidente del BCE

Mario DRAGHI

⁽¹⁾ DO L 80 de 18.3.2004, p. 33.

ANEXO

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

La autoridad certificadora de la ESBC-PKI se identifica en su certificado como emisor, y su clave privada se utiliza para firmar certificados. La autoridad certificadora de la ESBC-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 ESBC-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 ESBC-PKI incluye dos componentes técnicos:

- **Autoridad certificadora raíz de la ESBC-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:

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 de 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
--	---

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

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 4E29 550B B5A3 F59C
--	---

Distinguished name of issuer (Nombre distinguido de 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
--	---
