DECISÕES

DECISÃO DO BANCO CENTRAL EUROPEU

de 11 de janeiro de 2013

que estabelece o quadro jurídico da infraestrutura de chave pública para o Sistema Europeu de Bancos Centrais

(BCE/2013/1)

(2013/132/UE)

O CONSELHO DO BANCO CENTRAL EUROPEU,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o seu artigo 127.º,

Tendo em conta os Estatutos do Sistema Europeu de Bancos Centrais e do Banco Central Europeu (a seguir «Estatutos do SEBC»), nomeadamente o seu artigo 12.º-1, conjugado com os artigos 3.º-1, 5.º, 12.º-3 e artigos 16.º a 24.º dos citados Estatutos;

Considerando o seguinte:

(1) De acordo com o artigo 12.º-1 dos Estatutos do SEBC, o Conselho adota as orientações e toma as decisões necessárias para assegurar o desempenho das atribuições cometidas ao Sistema Europeu de Bancos Centrais (SEBC) e ao Eurosistema pelo Tratado e pelos Estatutos do SEBC. Nestas inclui-se o poder de decidir sobre a organização de atividades auxiliares que sejam necessárias para a execução de tais atribuições, tais como a emissão e gestão de certificados eletrónicos para proteção da informação armazenada e processada nas aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema, assim como da comunicação de dados para, ou a partir, dos mesmos.

(2) De acordo com o artigo 12.º-3 dos Estatutos do SEBC, o Conselho também tem o poder de determinar a organização interna do Banco Central Europeu (BCE) e dos seus órgãos de decisão. Consequentemente, o Conselho tem o poder de deliberar sobre a utilização, pelo BCE, de certificados eletrónicos emitidos pela infraestrutura de chave pública própria do Eurosistema.

(3) Está a aumentar o número de utilizadores que acedem a um número crescente de serviços, sistemas, plataformas e aplicações eletrónicas, em constante evolução, do SEBC e do Eurosistema. O Conselho considerou ser necessários serviços avançados de segurança informática, tais como meios seguros de autenticação, assinatura eletrónica e encriptação por meio da utilização de certificados eletrónicos.

(4) Poucos bancos centrais do SEBC possuem uma infraestrutura de chave pública própria, e muitos utilizadores de entidades terceiras, que trabalham em conjunto com os bancos centrais do SEBC, não dispõem de acesso fácil a uma autoridade certificadora admitida pelo SEBC em conformidade com o seu quadro de aceitação de certificados.

(5) É necessário que o Eurosistema crie uma infraestrutura de chave pública própria que possa emitir todos os tipos de certificados eletrónicos, como por exemplo certificados pessoais e técnicos, a utilizadores do SEBC e fora do SEBC, e que seja suficientemente flexível para se adaptar aos desenvolvimentos das aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema. Esta infraestrutura de chave pública (a seguir «ESCB-PKI») deveria complementar os serviços fornecidos por outras autoridades certificadoras admitidas pelo SEBC, em conformidade com o quadro de aceitação de certificados, ou por autoridades certificadoras admitidas pelo SEBC para o TARGET2 e TARGET2 Securities, em relação a essas duas aplicações.

(6) Em 29 de setembro de 2010, o Conselho decidiu lançar o projeto ESCB-PKI para organizar e implementar o ESCB-PKI e fornecer os recursos necessários para a sua conclusão. Foi decidido que o ESCB-PKI será desenvolvido, instalado e operado pelo Banco de España.

(7) O ESCB-PKI apoia indiretamente o desempenho das atribuições do SEBC e do Eurosistema. Baseia-se em três níveis de governação: Nível 1, que consiste no Conselho do BCE e na Comissão Executiva; Nível 2, que consiste nos bancos centrais do Eurosistema; e Nível 3, que consiste no banco central fornecedor.

(8) No Nível 1, o Conselho do BCE é responsável pela direção, gestão e controlo das atividades e produtos a fornecer necessários para desenvolver e operar o ESCB-PKI. O mesmo é também responsável pelo processo de decisão relativamente ao ESCB-PKI, e decide sobre a repartição das tarefas que não tenham sido especificamente atribuídas aos Níveis 2 e 3.

(9) Os bancos centrais do Eurosistema são responsáveis pelas tarefas atribuídas ao Nível 2, no âmbito do quadro geral definido pelo Conselho do BCE. Têm competências relativamente aos meios técnicos de implementação do ESCB-PKI.

(10) O Comité de Tecnologias de Informação do SEBC (ESCB-ITC) tem um papel de controlo no desenvolvimento do ESCB-PKI. Este Comité orienta, avalia, controla e aprova os resultados do projeto face aos critérios de aceitação previstos no quadro de aceitação de certificados do SEBC, ao âmbito de aplicação e ao calendário aprovado pelo Conselho do BCE.

(11) No Nível 3, o Banco de España foi designado como o banco central fornecedor para levar a cabo as tarefas que lhe foram atribuídas no âmbito do quadro geral definido pelo Conselho do BCE. O banco central fornecedor instalou a infraestrutura técnica e os dispositivos e serviços seguros necessários para criar e usar uma infraestrutura de chave pública de acordo com: a) a legislação nacional que transpôs a Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas ([1]), conforme aplicável; com b) a legislação nacional que transpôs a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ([2]), conforme aplicável; e com c) o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho de, 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados ([3]).

(12) Considerando que os certificados eletrónicos são elementos essenciais utilizados nas aplicações eletrónicas, tanto como mecanismo de autenticação de assinaturas eletrónicas como para a encriptação com chave pública, o ESCB-PKI irá tomar em conta as aplicações eletrónicas, sistemas, plataformas e serviços do SEBC existentes e os atuais projetos do SEBC por forma a garantir a cobertura das respetivas necessidades.

(13) Os bancos centrais nacionais (BCN) não participantes na área do euro podem decidir utilizar os certificados e serviços fornecidos pelo ESCB-PKI,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Definições

Para efeitos da presente decisão, entende-se por:

1) «certificado» ou «certificado eletrónico»: o ficheiro eletrónico, emitido por uma autoridade certificadora, que associa uma chave pública à identidade do subscritor do certificado e que é utilizado para todos ou alguns dos seguintes efeitos: a) verificar se a chave pública pertence ao subscritor do certificado; b) autenticar um certificado do subscritor; c) verificar a assinatura do subscritor do certificado; d) encriptar uma mensagem dirigida a um subscritor do certificado; e e) verificar os direitos de acesso do subscritor do certificado às aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema. Toda e qualquer referência, na presente decisão, a um certificado ou certificado eletrónico inclui a referência a dispositivos portadores de dados onde o certificado ou o certificado eletrónico possa ser armazenado;

2) «aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema»: aplicações eletrónicas, sistemas, plataformas e serviços que o SEBC e/ou o Eurosistema utilizam quando desempenham as atribuições que lhe foram conferidas pelo Tratado e pelos Estatutos do SEBC;

3) «infraestrutura de chave pública»: conjunto de indivíduos, políticas, procedimentos, e sistemas informáticos necessários para fornecer autenticação, encriptação, integridade e serviços de não repúdio através de encriptação de chave pública e privada e certificados eletrónicos;

4) «utilizador»: o subscritor do certificado ou a parte que confia no certificado, ou ambos;

5) «autenticação»: o processo de verificação da identidade do requerente do certificado ou do subscritor do certificado;

6) «banco central do SEBC»: o banco central do Eurosistema ou um BCN não participante na área do euro;

7) «banco central do Eurosistema»: o BCN de um Estado-Membro cuja moeda seja o euro, incluindo o banco central fornecedor, ou o BCE;

8) «banco central fornecedor»: o BCN designado pelo Conselho para desenvolver o ESCB-PKI e fornecer serviços ESCB-PKI em nome do Eurosistema, e para benefício deste;

9) «BCN não pertencente à área do euro»: o BCN de um Estado-Membro cuja moeda não seja o euro;

10) «autoridade certificadora ESCB-PKI»: entidade, na qual os utilizadores depositem confiança, que emite, gere, revogue e renove certificados em nome dos bancos centrais do SEBC ou dos bancos centrais do Eurosistema em conformidade com o quadro de aceitação de certificados do SEBC;

11) «autoridade de validação ESCB-PKI»: entidade, na qual os utilizadores depositem confiança, que fornece informação sobre a validade dos certificados emitidos pela autoridade certificadora ESCB- PKI;

12) «subscritor do certificado»: significa quer o indivíduo que seja objeto de um certificado eletrónico e ao qual foi emitido um certificado eletrónico, quer um gestor de componente técnica que tenha aceite um certificado eletrónico emitido pela autoridade certificadora ESCB-PKI para um componente técnico, quer ambos;

13) «quadro de aceitação de certificados do SEBC»: critérios estabelecidos pelo ESCB-ITC para identificar as autoridades certificadoras, tanto internas como externas ao SEBC, nas

([1]) JO L 13, de 19.1.2000, p. 12.
([2]) JO L 281, de 23.11.1995, p. 31.
([3]) JO L 8, de 12.1.2001, p. 1.

quais se pode depositar confiança relativamente às aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema.

14) «autoridade de registo»: entidade, na qual os utilizadores depositem confiança, que verifica a identidade de um requerente do certificado antes da emissão do certificado pelo ESCB-PKI;

15) «parte que confia no certificado»: indivíduo ou entidade, que não seja o subscritor do certificado, que aceita e confia num certificado;

16) «política de auditoria»: política de inspeções definida pelo Conselho em 7 de outubro de 1998, conforme publicação disponível no sítio do BCE ([1]);

17) «requerente do certificado»: indivíduo que requer a emissão do certificado para si ou para um componente técnico;

18) «componente técnico»: qualquer equipamento de *software* ou *hardware* que possa ser identificado através da utilização de certificados eletrónicos.

Artigo 2.º

Âmbito de aplicação

1. A presente decisão estabelece o enquadramento jurídico do ESCB-PKI. O ESCB-PKI é a infraestrutura de chave pública do Eurosistema desenvolvida pelo banco central fornecedor, em nome e para benefício dos bancos centrais do Eurosistema, que emite, gere, revoga e renova certificados, de acordo com o quadro de aceitação de certificados do SEBC.

2. Tendo em conta que os serviços ESCB-PKI podem afetar as partes que aceitem um certificado, esta decisão também estabelece as condições em que as partes que aceitam os certificados podem confiar nos certificados do ESCB-PKI.

Artigo 3.º

Âmbito de aplicação e objetivos do ESCB-PKI

1. As aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema que apresentem um grau de importância crítica médio ou elevado apenas podem ser acedidos e utilizados se o utilizador tiver sido autenticado através de certificado eletrónico emitido e gerido por uma autoridade certificadora admitida pelo SEBC em conformidade com o quadro de aceitação de certificados do SEBC, nomeadamente pela autoridade certificadora ESCB-PKI, ou por autoridades certificadoras admitidas pelo SEBC para o TARGET2 e TARGET2 Securities, em relação a essas duas aplicações.

2. A autoridade certificadora ESCB-PKI emite certificados eletrónicos e fornece outros serviços de certificação eletrónica aos subscritores certificados dos bancos centrais do SEBC e de partes terceiras que com eles trabalhem, de forma a permitir-lhes aceder e utilizar com segurança as aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema.

([1]) www.ecb.europa.eu

3. O ESCB-PKI fornece os serviços de certificação seguintes:

a) Emissão, renovação e revogação do certificado, e ainda confirmação da validade do certificado relativamente aos diferentes tipos de certificados;

b) Emissão de certificados para autenticação, assinatura eletrónica e encriptação relativamente a utilizadores do SEBC e fora do SEBC, e certificados técnicos;

c) Recuperação de chave privada para assegurar a recuperação de informação baseada na chave pública encriptada, em caso de perda do certificado;

d) Entrega e gestão de *tokens* de chave criptográfica aos subscritores do certificado, quando necessário;

e) Prestação de informações sobre os procedimentos de gestão de certificados do ESCB-PKI e apoio técnico aos gestores de projeto do SEBC para auxílio na integração de certificados ESCB-PKI nas suas aplicações.

Outros serviços poderão ser adicionados no futuro, se tal for necessário para as aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema.

Artigo 4.º

Quadro do ESCB-PKI

1. Nos termos da presente decisão, as responsabilidades e funções do banco central fornecedor e de outros bancos centrais do Eurosistema, no que respeita à implementação, funcionamento e utilização do ESCB-PKI devem ser estabelecidas num Acordo de Nível 2-Nível 3 e ser objeto de mais pormenorização nas políticas de certificado do ESCB-PKI e na declaração de práticas de certificação do ESCB-PKI.

2. O Acordo Nível 2-Nível 3, que inclui o Acordo de Nível de Serviço, contém o acordo celebrado entre o banco central fornecedor e os bancos centrais do Eurosistema no tocante às responsabilidades e funções do banco central fornecedor e dos bancos centrais do Eurosistema. O acordo de Nível 2-Nível 3 deve ser enviado para aprovação pelo Conselho e, em seguida, assinado pelo banco central fornecedor e pelos bancos centrais do Eurosistema.

3. O Acordo de Nível de Serviço constitui tanto o acordo que define o nível de serviços a prestar pelo banco central fornecedor ao Eurosistema, como o acordo que define o nível dos serviços relacionados com o ESCB-PKI a prestar pelo Eurosistema aos BCN não participantes da área do euro e a terceiros.

4. A declaração de práticas de certificação do ESCB-PKI é um conjunto de regras que regulam o ciclo de vida dos certificados eletrónicos, desde o pedido inicial até ao fim da assinatura ou revogação, assim como as relações entre o requerente do certificado ou subscritor, a autoridade de certificação do ESCB-PKI e as partes que aceitam os certificados. Abrange os certificados eletrónicos abrangidos pelo âmbito de aplicação da Diretiva 1999/93/CE e os certificados eletrónicos fora do seu âmbito de aplicação. Também estabelece as atribuições e responsabilidades de todas as partes e os procedimentos de emissão e gestão de certificados. Encontra-se anexada ao Acordo de Nível 2-Nível 3.

5. Uma política de certificado do ESCB-PKI traduz-se num conjunto de regras aplicáveis a cada tipo de certificado emitido. Cada conjunto de regras fornece detalhes de implementação relacionados com a declaração de práticas de certificação do ESCB-PKI relativamente a cada tipo de certificado emitido. As políticas de certificado do ESCB-PKI encontram-se anexadas ao Acordo de Nível 2-Nível 3.

6. As políticas de certificado do ESCB-PKI e a declaração de práticas de certificação do ESCB-PKI são publicadas no sítio do ESCB-PKI ([1]).

7. A informação respeitante à autoridade de certificação do ESCB-PKI, incluindo a sua identidade e os seus componentes técnicos, consta do anexo à presente decisão.

Artigo 5.º

Responsabilidades e atribuições do banco central fornecedor

1. O banco central fornecedor é responsável pela operação e manutenção do ESCB-PKI em benefício dos bancos centrais do Eurosistema, incluindo a instalação, operação e gestão efetuada em conformidade com o Acordo de Nível 2-Nível 3. Deve, em particular, fornecer certificados e serviços do ESCB-PKI de acordo com os requisitos do negócio e com as especificações técnicas, como sejam o quadro de aceitação de certificado do SEBC e os requisitos e as especificações definidas no Acordo de Nível 2-Nível 3.

2. O banco central fornecedor instala a infraestrutura organizacional necessária para criar, emitir e gerir os certificados e deve assegurar que a manutenção dessa infraestrutura. Para esse efeito o banco central fornecedor pode adotar, em consulta com o Comité de Tecnologias de Informação, regras respeitantes à sua organização e administração interna.

3. O banco central fornecedor atua como autoridade de certificação do ESCB-PKI e como autoridade de validação do ESCB-PKI.

4. O Acordo de Nível 2-Nível 3 estabelece o regime de responsabilidade aplicável ao banco central fornecedor.

Artigo 6.º

Responsabilidades e atribuições dos bancos centrais do Eurosistema

1. Cada banco central do Eurosistema é responsável pela identificação dos seus subscritores de certificados. Para executar esta tarefa deve designar um oficial de registo autorizado a registar terceiros utilizadores.

2. Cada banco central do Eurosistema atua como uma parte que confia no certificado em relação aos certificados para encriptação e assinatura eletrónica emitidos pelo ESCB-PKI a outros bancos centrais do Eurosistema ou terceiros utilizadores subscritores de certificados ou.

3. Cada banco central do Eurosistema que utilize os serviços do ESCB-PKI deve atua como uma autoridade de registo em relação aos seus requerentes do certificado e garante que esses requerentes aceitam e aplicam os termos e condições de utilização constantes do formulário de aplicação para os serviços da autoridade de certificação do ESCB-PKI.

([1]) http://pki.escb.eu.

Artigo 7.º

Relações entre os bancos centrais do Eurosistema, partes terceiras e subscritores de certificados

Cada banco central do Eurosistema tomaas medidas necessárias relativamente ao acesso e à utilização segura, por terceiros, das aplicações eletrónicas, sistemas, plataformas e serviços do SEBC e do Eurosistema mediante a utilização de certificados do ESCB-PKI. Estes acordos regem, exclusivamente, a relação entre o banco central do Eurosistema relevante e os terceiros que utilizam certificados do ESCB-PKI. Todos os terceiros devem respeitar as políticas de certificado do ESCB-PKI, a declaração de práticas de certificação do ESCB-PKI e os termos e condições de utilização definidas no formulário de aplicação para os serviços da autoridade de certificação do ESCB-PKI.

Artigo 8.º

Relação entre as partes que confiam no certificado

Um certificado eletrónico, emitido ao abrigo desta decisão, pode ser considerado digno de confiança desde que a parte que confia no certificado:

a) Verifique a validade, suspensão ou revogação do certificado através da informação do estado atual de revogação;

b) Considere quaisquer limitações de utilização específicas do certificado; e

c) Aceite a declaração de práticas de certificação do ESCB-PKI e as políticas do certificado SEBC- PKI.

Artigo 9.º

Direitos para o ESCB-PKI

1. O ESCB-PKI é propriedade plena dos bancos centrais do Eurosistema.

2. Consequentemente, o banco central fornecedor concede aos bancos centrais do Eurosistema, na medida do possível e nos termos da legislação aplicável, todas as licenças em matéria de direitos de propriedade intelectual que sejam necessárias para permitir que os bancos centrais do Eurosistema utilizem o ESCB-PKI, os seus componentes e todos os serviços do ESCB-PKI, presta também serviços ESCB-PKI a terceiros, de acordo com a declaração de práticas de certificação do ESCB-PKI e as políticas de certificado do ESCB-PKI. O banco central fornecedor compensa os bancos centrais do Eurosistema pelo pagamento de quaisquer pedidos de indemnização referentes a violação de direitos de propriedade intelectual apresentados por terceiros.

3. Os detalhes referentes aos direitos dos bancos centrais do Eurosistema sobre o ESCB-PKI serão acordados entre o Nível 2 e o Nível 3, no Acordo de Nível 2-Nível 3.

Artigo 10.º

Responsabilidade dos bancos centrais do Eurosistema perante os utilizadores

1. Excetuando os casos em que demonstrem que não agiram de forma negligente, os bancos centrais do Eurosistema são responsáveis, nos termos das suas funções e responsabilidades

no ESCB-PKI, por qualquer dano causado a um utilizador que confie, de forma razoável, num certificado qualificado, conforme definido na Diretiva 1999/93/CE, quanto ao seguinte:

a) À exatidão, no momento da emissão, de todas as informações contidas num determinado certificado qualificado e à verificação de todos os requisitos exigidos para a qualificação de um certificado como qualificado, conforme definido na Diretiva 1999/93/CE;

b) À garantia de que, no momento de emissão de um determinado certificado qualificado, o subscritor do certificado nele identificado era titular dos dados de criação de assinatura correspondentes aos dados de verificação de assinatura, incluídos ou identificados nesse certificado;

c) À garantia de que o dispositivo de criação de assinaturas e o dispositivo de verificação de assinaturas funcionam em conjunto, de forma complementar, nos casos em que ambos sejam gerados pelo ESCB-PKI;

d) A qualquer falha do registo na revogação de um certificado qualificado.

2. Os bancos centrais do Eurosistema não assumem qualquer compromisso, não oferecem quaisquer garantias e não aceitam qualquer responsabilidade perante os utilizadores, exceto se expressamente indicado na presente decisão e na declaração de práticas de certificação do ESCB-PKI.

Artigo 11.º

Participação dos BCN não participantes na área do euro no ESCB-PKI

1. Um BCN não participante na área do euro pode atuar como autoridade de registo tanto em relação aos seus utilizadores internos como para os terceiros utilizadores, podendo designar um oficial de registo para executar essa tarefa.

2. Sujeito à aprovação do Conselho, um BCN não participante na área do euro também pode decidir utilizar os serviços ESCB-PKI em condições idênticas às aplicáveis aos bancos centrais do Eurosistema. Para esse efeito, o BCN não participante na área do euro deve submeter uma declaração ao Conselho confirmando que irá cumprir com as obrigações previstas na presente decisão e no Acordo de Nível 2-Nível 3. Um BCN não participante na área do euro não se torna coproprietário do ESCB-PKI e não é obrigado a contribuir para o envelope financeiro do ESCB-PKI.

Artigo 12.º

Proteção de dados

No desempenho das suas funções relacionadas com o ESCB-PKI, os bancos centrais do Eurosistema devem atuar de acordo com a legislação de proteção de dados aplicável ao seu tratamento de dados pessoais.

Artigo 13.º

Auditoria

As auditorias ao ESCB-PKI são efetuadas em conformidade com os princípios e regras estabelecidos na política de auditoria. Estes não obstam às medidas de controlo e de auditoria interna que se apliquem ou sejam adotadas pelos bancos centrais do Eurosistema.

Artigo 14.º

Quadro financeiro

Os bancos centrais do Eurosistema suportam os custos operacionais e de desenvolvimento do ESCB-PKI conforme especificado no envelope financeiro do ESCB-PKI.

Artigo 15.º

Função da Comissão Executiva

1. De acordo com o artigo 17.º, n.º 3, da Decisão BCE/2004/2, de 19 de fevereiro de 2004, que adota o Regulamento Interno do Banco Central Europeu [1], o Conselho delega os seus poderes normativos na Comissão Executiva para tomar quaisquer medidas para implementar esta decisão que sejam necessárias para a eficiência e segurança do ESCB-PKI, assim como para aprovar alterações relativas aos aspetos técnicos e aos serviços do ESCB-PKI, previstos nos anexos do Acordo de Nível 2-Nível 3, após tomar em consideração o parecer do ITC e, se aplicável, do parecer do Comité Diretor de Tecnologias de Informação do Eurosistema.

2. A Comissão Executiva deve notificar o Conselho, sem demora, de qualquer medida que adote nos termos do n.º 1, e submeter-se a qualquer decisão adotada pelo referido Conselho nesta matéria.

Feito em Frankfurt am Main, em 11 de janeiro de 2013.

O Presidente do BCE

Mario DRAGHI

[1] JO L 80, de 18.3.2004, p. 33.

ANEXO

Informações sobre a autoridade de certificação do ESCB-PKI, incluindo a sua identidade e os seus componentes técnicos

A autoridade de certificação do ESCB-PKI encontra-se identificada no seu certificado como emissor, sendo a sua chave privada utilizada para assinar certificados. A autoridade de certificação do ESCB-PKI é responsável pela:

i) emissão de certificados de chaves públicas e privadas,

ii) emissão de listas de revogação,

iii) criação de pares de chaves associados a certificados específicos, como, por exemplo, certificados que necessitem de recuperação de chave,

iv) responsabilidade global pelo ESCB-PKI e pela garantia de que todos os requisitos operacionais necessários são cumpridos.

A autoridade de certificação do ESCB-PKI inclui todos as pessoas singulares, políticas, procedimentos e sistemas de computador encarregues da emissão de certificados eletrónicos e a atribuição aos respetivos subscritores.

A autoridade de certificação do ESCB-PKI inclui dois componentes técnicos:

— **A autoridade de certificação Root ESCB-PKI:** esta autoridade de certificação, num primeiro nível, apenas emite certificados para si própria e para as suas autoridades de certificação subordinadas. Apenas opera na prossecução das suas responsabilidades estritamente definidas. Os seus dados mais importantes são:

Distinguished name	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period	De 21-06-2011 11:58:26 até 21-06-2041 11:58:26
Message digest (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

— **A autoridade de certificação Online ESCB-PKI:** Esta autoridade de certificação, num segundo nível, está subordinada à autoridade de certificação Root ESCB-PKI. É responsável pela emissão dos certificados do ESCB-PKI para utilizadores. Os seus dados mais importantes são:

Distinguished name	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period	De 22-07-2011 12:46:35 até 22-07-2026 12:46:35
Message digest (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08