# DECISÕES

## DECISÃO (UE) 2016/187 DO BANCO CENTRAL EUROPEU

**de 11 de dezembro de 2015**

**que altera a Decisão BCE/2013/1 que estabelece o quadro jurídico da infraestrutura de chave pública para o Sistema Europeu de Bancos Centrais (BCE/2015/46)**

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, nomeadamente o seu artigo 12.º-1, conjugado com o artigo 3.º-1, o artigo 5.º, o artigo 12.º, n.º 3 e, ainda, os artigos 16.º a 24.º e 34.º dos citados Estatutos,

Considerando o seguinte:

(1) O Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([1]) revoga, a partir de 1 de julho de 2016, a Diretiva 1999/93/CE do Parlamento Europeu e do Conselho ([2]). Justifica-se, portanto, a menção ao Regulamento (UE) n.º 910/2014 na Decisão BCE/2013/1 ([3]).

(2) A informação respeitante à autoridade de certificação do ESCB-PKI, incluindo a sua identidade e os seus componentes técnicos, constante do anexo à Decisão BCE/2013/1, necessita de ser atualizada.

(3) Havendo, por conseguinte, que alterar em conformidade a Decisão BCE/2013/1,

ADOTOU A PRESENTE DECISÃO:

*Artigo 1.º*

**Alterações**

A Decisão BCE/2013/1 é alterada do seguinte modo:

1) O artigo 1.º, n.º 10 é substituído pelo seguinte:

«10. "autoridade certificadora *ESCB-PKI*": a entidade da confiança dos utilizadores que emite, gere, revoga e renova certificados *ESCB/PKI* em conformidade com o quadro de aceitação de certificados do SEBC/MUS;»;

2) O artigo 4.º, n.º 4, é substituído pelo seguinte:

«4. A declaração de práticas de certificação do *ESCB-PKI* é um conjunto de regras que regem o ciclo de vida dos certificados eletrónicos, desde o pedido inicial até ao fim da assinatura ou à sua revogação, assim como o relacionamento entre o requerente ou subscritor do certificado, a autoridade de certificação do *ESCB-PKI* e as partes que aceitam os certificados. A mesma cobre tanto os certificados no âmbito de aplicação da Diretiva 1999/93/CE e do

([1]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

([2]) 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 (JO L 13 de 19.1.2000, p. 12).

([3]) Decisão BCE/2013/1 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 (JO L 74 de 16.3.2013, p. 30).

Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho (*), como os não abrangidos por estes. Também estabelece as atribuições e responsabilidades de todas as partes, e os procedimentos de emissão e de gestão de certificados. A mesma constitui um anexo do Acordo de Nível 2 — Nível 3.

(*) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73)».

3) No artigo 10.º, a declaração introdutória e o n.º 1, alínea a) são substituídos pelos seguintes:

«1. Salvo se conseguirem demonstrar que não houve negligência da sua parte, os bancos centrais do Eurosistema são responsáveis, nos termos das respetivas funções e responsabilidades no *ESCB-PKI*, por qualquer dano causado a um utilizador que razoavelmente confie num certificado qualificado, conforme definido na Diretiva 1999/93/CE e no Regulamento (UE) n.º 910/2014, quanto:

a) à exatidão, no momento da emissão, de todas as informações contidas no certificado qualificado, e à questão de saber se o certificado contém todos os detalhes exigidos pela Diretiva 1999/93/CE e pelo Regulamento (UE) n.º 910/2014 para um certificado qualificado.»;

4) O presente anexo substitui o anexo da decisão.

*Artigo 2.º*

**Entrada em vigor**

A presente decisão entra em vigor no terceiro dia subsequente ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Frankfurt am Main, em 11 de dezembro de 2015.

*O Presidente do BCE*
Mario DRAGHI

*ANEXO*

*«ANEXO*

**Informação respeitante à autoridade de certificação do *ESCB-PKI*, incluindo a sua identidade e os seus componentes técnicos**

A autoridade de certificação do *ESCB-PKI* está 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 chave pública e privada;

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; e

iv) pelo funcionamento geral do *ESCB-PKI* e pela garantia do cumprimento de todos os requisitos operacionais.

A autoridade de certificação do *ESCB-PKI* inclui todas as pessoas singulares e as políticas, procedimentos e sistemas de computador incumbidas da emissão de certificados eletrónicos e da sua atribuição aos respetivos subscritores.

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

— **Autoridade de certificação Root** ESCB-PKI**:** Esta autoridade de certificação, de primeiro nível, só emite certificados para si própria e para as autoridades de certificação que lhe estão subordinadas. A mesma apenas está em operação quando prossegue responsabilidades próprias, estritamente definidas. Os seus dados mais importantes são:

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

| | |
|---|---|
| **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 |
| **Message digest (SHA-256)** | C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB |
| **Cryptographic algorithms** | SHA-1/RSA 4096 |

b) Certificado SHA-256:

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

([1]) Este certificado apenas será utilizado em sistemas que não suportem algoritmos mais elevados.

| | |
|---|---|
| **Distinguished name of issuer** | CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU |
| **Validity period** | De 21-06-2011 12:35:34 até 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** | SHA-256/RSA 4096 |

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

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

| | |
|---|---|
| **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 |
| **Message digest (SHA-256)** | 4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A |
| **Cryptographic algorithms** | SHA-1/RSA 4096 |

b) Certificado SHA-256:

| | |
|---|---|
| **Distinguished name** | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU |
| **Serial number** | 660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D |
| **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)** | 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** | SHA-256/RSA 4096» |

([1]) Este certificado apenas será utilizado em sistemas que não suportem algoritmos mais elevados.