

DÉCISIONS

DÉCISION (UE) 2016/187 DE LA BANQUE CENTRALE EUROPÉENNE

du 11 décembre 2015

modifiant la décision BCE/2013/1 établissant le cadre applicable à une infrastructure à clés publiques pour le Système européen de banques centrales (BCE/2015/46)

LE CONSEIL DES GOUVERNEURS DE LA BANQUE CENTRALE EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, notamment son article 127,

vu les statuts du Système européen de banques centrales et de la Banque centrale européenne, notamment leur article 12.1, en liaison avec leur article 3.1, leur article 5, leur article 12.3, leurs articles 16 à 24 et leur article 34,

considérant ce qui suit:

- (1) Le règlement (UE) n° 910/2014 du Parlement européen et du Conseil ⁽¹⁾ a abrogé la directive 1999/93/CE du Parlement européen et du Conseil ⁽²⁾ avec effet au 1^{er} juillet 2016. Par conséquent, il convient de renvoyer au règlement (UE) n° 910/2014 dans la décision BCE/2013/1 ⁽³⁾.
- (2) Les informations relatives à l'autorité de certification de l'ICP-SEBC, notamment son identité et ses composants techniques, précisées en annexe à la décision ECB/2013/1, doivent être mises à jour.
- (3) Il convient donc de modifier la décision BCE/2013/1 en conséquence,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Modifications

La décision BCE/2013/1 est modifiée comme suit:

1. À l'article 1^{er}, le point 10 est remplacé par le texte suivant:

«10. "autorité de certification de l'ICP-SEBC": l'entité, à laquelle les utilisateurs font confiance, chargée de l'émission, de la gestion, de la révocation et du renouvellement des certificats de l'ICP-SEBC conformément au cadre d'acceptation des certificats du SEBC/MSU;»

2. À l'article 4, le point 4 est remplacé par le texte suivant:

«4. La déclaration des pratiques de certification de l'ICP-SEBC est un ensemble de règles gouvernant le cycle de vie des certificats électroniques, depuis la demande initiale jusqu'à la fin de l'abonnement ou la révocation, ainsi que les relations entre le demandeur de certificat ou l'abonné à un certificat, l'autorité de certification de l'ICP-SEBC et les parties utilisatrices. Elle couvre les certificats relevant du champ d'application de la directive 1999/93/CE et du

⁽¹⁾ Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

⁽²⁾ Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques (JO L 13 du 19.1.2000, p. 12).

⁽³⁾ Décision BCE/2013/1 de la Banque centrale européenne du 11 janvier 2013 établissant le cadre applicable à une infrastructure à clés publiques pour le Système européen de banques centrales (JO L 74 du 16.3.2013, p. 30).

règlement (UE) n° 910/2014 du Parlement européen et du Conseil (*) et les certificats ne relevant pas de leur champ d'application. En outre, elle définit les rôles et les responsabilités de toutes les parties ainsi que les procédures en matière d'émission et de gestion des certificats. Elle est annexée à l'accord de niveau 2 — niveau 3.

(*) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).»

3. À l'article 10, la déclaration introductive et le point a) du paragraphe 1 sont remplacés par le texte suivant:

«1. Sauf si elles prouvent qu'elles n'ont commis aucune négligence, les banques centrales de l'Eurosystème sont tenues responsables, conformément à leurs fonctions et responsabilités dans le cadre de l'ICP-SEBC, de tout préjudice causé à un utilisateur se fiant raisonnablement à un certificat qualifié, tel que défini dans la directive 1999/93/CE et le règlement (UE) n° 910/2014, en ce qui concerne:

a) l'exactitude de toutes les informations contenues dans un certificat qualifié à la date de son émission et la présence, dans le certificat, de toutes les données détaillées exigées pour un certificat qualifié, ainsi que défini dans la directive 1999/93/CE et le règlement n° 910/2014;»

4. l'annexe est remplacée par l'annexe de la présente décision.

Article 2

Entrée en vigueur

La présente décision entre en vigueur le troisième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Francfort-sur-le-Main, le 11 décembre 2015.

Le président de la BCE
Mario DRAGHI

ANNEXE

«ANNEXE

Informations relatives à l'autorité de certification de l'ICP-SEBC, notamment son identité et ses composants techniques

L'autorité de certification de l'ICP-SEBC est identifiée comme l'émetteur, dans son certificat, et sa clé privée est utilisée pour signer les certificats. L'autorité de certification de l'ICP-SEBC est chargée:

- i) d'émettre les certificats à clés privées et à clés publiques,
- ii) d'émettre les listes de certificats révoqués,
- iii) de créer des bi-clés associés à des certificats particuliers, par exemple ceux qui nécessitent le recouvrement d'une clé,
- iv) de conserver la responsabilité générale de l'ICP-SEBC et de garantir que sont réunies toutes les conditions nécessaires à son fonctionnement.

L'autorité de certification de l'ICP-SEBC comprend l'ensemble des personnes, politiques, procédures et systèmes informatiques auxquels sont confiées l'émission de certificats électroniques et l'attribution de ces certificats aux abonnés à un certificat.

L'autorité de certification de l'ICP-SEBC comprend deux composants techniques:

- **L'autorité de certification racine de l'ICP-SEBC:** cette autorité de certification, au premier niveau, émet uniquement des certificats pour elle-même et pour ses autorités de certification intermédiaires. Elle fonctionne uniquement lorsqu'elle s'acquitte de ses propres responsabilités étroitement définies. Ses principales données sont les suivantes:

- a) Certificat SHA-1 ⁽¹⁾:

Distinguished name [nom distinctif]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number [numéro de série]	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer [nom distinctif de l'émetteur]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period [période de validité]	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest [empreinte numérique] (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest [empreinte numérique] (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms [algorithmes cryptographiques]	SHA-1/RSA 4096

- b) Certificat SHA-256:

Distinguished name [nom distinctif]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number [numéro de série]	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

⁽¹⁾ Ce certificat sera utilisé uniquement dans les systèmes qui ne supportent pas les algorithmes plus élevés.

Distinguished name of Issuer [nom distinctif de l'émetteur]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period [période de validité]	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest [empreinte numérique] (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest [empreinte numérique] (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms [algorithmes cryptographiques]	SHA-256/RSA 4096

- **L'autorité de certification en ligne de l'ICP-SEBC:** cette autorité de certification, au deuxième niveau, est subordonnée à l'autorité de certification racine de l'ICP-SEBC. Elle est chargée d'émettre des certificats ICP-SEBC pour les utilisateurs. Ses principales données sont les suivantes:

a) Certificat SHA-1 ⁽¹⁾:

Distinguished name [nom distinctif]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number [numéro de série]	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer [nom distinctif de l'émetteur]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period [période de validité]	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest [empreinte numérique] (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message digest [empreinte numérique] (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms [algorithmes cryptographiques]	SHA-1/RSA 4096

b) Certificat SHA-256:

Distinguished name [nom distinctif]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number [numéro de série]	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of Issuer [nom distinctif de l'émetteur]	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period [période de validité]	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest [empreinte numérique] (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest [empreinte numérique] (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms [algorithmes cryptographiques]	SHA-256/RSA 4096»

⁽¹⁾ Ce certificat sera utilisé uniquement dans les systèmes qui ne supportent pas les algorithmes plus élevés.