BESCHLÜSSE

BESCHLUSS (EU) 2016/187 DER EUROPÄISCHEN ZENTRALBANK

vom 11. Dezember 2015

zur Änderung des Beschlusses EZB/2013/1 über die Festlegung eines Rahmens für eine Public-Key-Infrastruktur (PKI) für das Europäische System der Zentralbanken (EZB/2015/46)

DER EZB-RAT —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 127,

gestützt auf die Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank, insbesondere auf die Artikel 12.1 in Verbindung mit Artikel 3.1, Artikel 5, Artikel 12.3 und den Artikeln 16 bis 24 und 34,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([1]) wurde durch die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates ([2]) mit Wirkung vom 1. Juli 2016 aufgehoben. Demzufolge ist es angemessen, auf die Verordnung (EU) Nr. 910/2014 im Beschluss EZB/2013/1 ([3]) zu verweisen.

(2) Informationen über die ESZB-PKI-Zertifizierungsstelle, einschließlich ihrer Identität sowie ihrer technischen Komponenten, wie sie im Anhang dieses Beschlusses EZB/2013/1 festgelegt sind, bedürfen der Aktualisierung.

(3) Der Beschluss EZB/2013/1 sollte daher entsprechend geändert werden —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Änderungen

Der Beschluss EZB/2013/1 wird wie folgt geändert:

1. Artikel 1 Nummer 10 erhält folgende Fassung:

„10. ‚ESZB-PKI-Zertifizierungsstelle': die das Vertrauen der Nutzer genießende Stelle, die gemäß dem Rahmen des ESZB/SSM für die Anerkennung von Zertifikaten ESZB-PKI-Zertifikate ausstellt, verwaltet, widerruft und erneuert;".

2. Artikel 4 Absatz 4 erhält folgende Fassung:

„(4) Das Sicherheits- und Zertifizierungskonzept der ESZB-PKI ist ein Regelwerk, das den Lebenszyklus von elektronischen Zertifikaten vom ersten Antrag bis zum Ende der Nutzung oder Widerruf sowie die Beziehungen zwischen dem Zertifikatsantragsteller oder -nehmer, der Zertifizierungsstelle der ESZB-PKI und den vertrauenden Dritten bestimmt. Es umfasst Zertifikate, die in den Anwendungsbereich der Richtlinie 1999/93/EG und Verordnung

([1]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

([2]) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000, S. 12).

([3]) Beschluss EZB/2013/1 der Europäischen Zentralbank vom 11. Januar 2013 über die Festlegung eines Rahmens für eine Public-Key-Infrastruktur (PKI) für das Europäische System der Zentralbanken (ABl. L 74 vom 16.3.2013, S. 30).

(EU) Nr. 910/2014 des Europäischen Parlaments und des Rates (*) fallen sowie Zertifikate, die nicht in deren Anwendungsbereich fallen. Es legt auch die Aufgaben und Zuständigkeiten aller Parteien und die Verfahren in Bezug auf die Ausstellung und Verwaltung der Zertifikate fest. Es ist der Level 2 — Level 3-Vereinbarung beigefügt.

(*) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).“

3. In Artikel 10 Absatz 1 erhalten der einleitende Satz und Buchstabe a folgende Fassung:

„(1) Sofern sie nicht nachweisen, dass sie nicht fahrlässig gehandelt haben, haften die Zentralbanken des Eurosystems gemäß ihren Aufgaben und Zuständigkeiten im Rahmen der ESZB-PKI in Bezug auf Schäden gegenüber einem Nutzer, der vernünftigerweise auf das qualifizierte Zertifikat vertraut, im Sinne der Richtlinie 1999/93/EG und der Verordnung (EU) Nr. 910/2014, im Hinblick auf:

a) die Korrektheit aller Informationen in einem qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung, und die Vollständigkeit der für ein qualifiziertes Zertifikat vorgeschriebenen Angaben im Sinne der Richtlinie 1999/93/EG und der Verordnung (EU) Nr. 910/2014 im Zertifikat;“.

4. Der Anhang wird ersetzt durch den Anhang dieses Beschlusses.

Artikel 2

Inkrafttreten

Dieser Beschluss tritt am dritten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Geschehen zu Frankfurt am Main am 11. Dezember 2015.

Der Präsident der EZB
Mario DRAGHI

ANHANG

„ANHANG

Informationen in Bezug auf die ESZB-PKI-Zertifizierungsstelle, einschließlich ihrer Identität, und ihre technischen Komponenten

Die ESZB-PKI-Zertifizierungsstelle wird in ihrem Zertifikat als Ausstellerin bestimmt und ihr privater Schlüssel wird zum Signieren von Zertifikaten verwendet. Die ESZB-PKI-Zertifizierungsstelle ist zuständig für:

i) die Ausstellung von privaten und Public-Key-Zertifikaten;

ii) die Ausstellung von Widerrufslisten;

iii) die Erzeugung von Schlüsselpaaren im Zusammenhang mit spezifischen Zertifikaten, z. B. solche, die eine Schlüsselwiederherstellung erfordern;

iv) die Beibehaltung der Gesamtverantwortung für die ESZB-PKI und Sicherstellung, dass alle für ihren Betrieb erforderlichen Voraussetzungen erfüllt sind.

Die ESZB-PKI-Zertifizierungsstelle schließt alle natürlichen Personen, Richtlinien, Verfahren und Computersysteme ein, die mit der Ausstellung elektronischer Zertifikate und ihrer Zuordnung an die Zertifikatnehmer betraut sind.

Die ESZB-PKI-Zertifizierungsstelle schließt zwei technische Komponenten ein:

— **Die ESZB-PKI-Wurzelzertifizierungsstelle**: Diese Zertifizierungsstelle auf der ersten Ebene stellt nur Zertifikate für sich selbst und für ihre nachgeordneten Zertifizierungsstellen aus. Sie ist nur in Betrieb, wenn sie ihre eigenen eng definierten Aufgaben wahrnimmt. Ihre wichtigsten Daten sind:

a) SHA-1 certificate (SHA-1-Zertifikat) ([1]):

Distinguished Name (Name)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Seriennummer)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished Name of issuer (Name des Ausstellers)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Gültigkeitszeitraum)	From 21-06-2011 11:58:26 to 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 (kryptographische Algorithmen)	SHA-1/RSA 4096

b) SHA-256 certificate (SHA-56-Zertifikat):

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

([1]) Dieses Zertifikat wird nur in Systemen verwendet, die die Verwendung höherer Algorithmen nicht unterstützen.

Distinguished Name of issuer (Name des Ausstellers)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Gültigkeitszeitraum)	From 21-06-2011 12:35:34 to 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 (kryptographische Algorithmen)	SHA-256/RSA 4096

— **Die ESZB-PKI-Online-Zertifizierungsstelle**: Diese Zertifizierungsstelle auf der zweiten Ebene ist der ESZB-PKI-Wurzelzertifizierungsstelle nachgeordnet. Sie ist für die Ausstellung von ESZB-PKI-Zertifikaten für Nutzer zuständig. Ihre wichtigsten Daten sind:

a) SHA-1 certificate (SHA-1-Zertifikat) ([1]):

Distinguished Name (Name)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Seriennummer)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished Name of issuer (Name des Ausstellers)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Gültigkeitszeitraum)	From 22-07-2011 12:46:35 to 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 (kryptographische Algorithmen)	SHA-1/RSA 4096

b) SHA-256 certificate (SHA-256-Zertifikat):

Distinguished Name (Name)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Seriennummer)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished Name of issuer (Name des Ausstellers)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Gültigkeitszeitraum)	From 22-07-2011 12:46:35 to 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 (kryptographische Algorithmen)	SHA-256/RSA 4096“

([1]) Dieses Zertifikat wird nur in Systemen verwendet, die die Verwendung höherer Algorithmen nicht unterstützen.