2024/2683

15.10.2024

BESCHLUSS (EU) 2024/2683 DER EUROPÄISCHEN ZENTRALBANK

vom 8. Oktober 2024

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/2024/26)*

DER EZB-RAT —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 127 und Artikel 132 Absatz 1,

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

in Erwägung nachstehender Gründe:

(1) Mit dem Beschluss EZB/2013/1 der Europäischen Zentralbank ([1]) wurde ein Rahmen für die Public-Key-Infrastruktur des Eurosystems (nachfolgend die „ESZB-PKI“) geschaffen, um die Ausstellung und Verwaltung elektronischer Zertifikate zu regeln, die für den Zugriff auf elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems mit mittlerer oder höherer Kritikalität sowie deren Nutzung erforderlich sind.

(2) Die von der ESZB-PKI verwendete Technologie hat das Ende ihrer Lebensdauer erreicht. Es ist daher notwendig, eine neue ESZB-PKI-Online-Zertifizierungsstelle (nachfolgend die „ESZB-PKI-Online-Zertifizierungsstelle V1.2“) einzurichten, wobei auch berücksichtigt werden sollte, dass Zertifikate mit dreijähriger Gültigkeit, die von einer ESZB-PKI-Online-Zertifizierungsstelle für dem ESZB angehörende und nicht dem ESZB angehörende Nutzer und technische Komponenten ausgestellt werden, nicht später ihre Gültigkeit verlieren können als das Zertifikat dieser ESZB-PKI-Online-Zertifizierungsstelle selbst. Das Zertifikat der bestehenden ESZB-PKI-Online-Zertifizierungsstelle verliert am 22. Juli 2026 seine Gültigkeit und danach wäre die ESZB-PKI-Online-Zertifizierungsstelle V1.2 bis zum Ablauf der Gültigkeit ihres Zertifikats die einzige ESZB-PKI-Online-Zertifizierungsstelle.

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

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Änderung

Der Anhang des Beschlusses EZB/2013/1 wird durch den Anhang dieses Beschlusses ersetzt.

Artikel 2

Inkrafttreten

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

Geschehen zu Frankfurt am Main am 8. Oktober 2024.

Die Präsidentin der EZB
Christine LAGARDE

([1]) 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).

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 umfasst 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 besteht aus drei technischen Komponenten:

1. **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:

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
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

2. **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. Ihr Betrieb wird am 22. Juli 2026 eingestellt. Ihre wichtigsten Daten sind:

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

3. **Die ESZB-PKI-Online-Zertifizierungsstelle V1.2**: Diese Zertifizierungsstelle auf der zweiten Ebene ist der ESZB-PKI-Wurzelzertifizierungsstelle nachgeordnet. Sie ist für die Ausstellung von ESZB-PKI-Zertifikaten für Nutzer zuständig. Nach dem 22. Juli 2026 ist sie bis zur Einstellung ihres Betriebs die einzige ESZB-PKI-Online-Zertifizierungsstelle. Ihre wichtigsten Daten sind:

Distinguished name (Name)	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Seriennummer)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished name of issuer (Name des Ausstellers)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Gültigkeitszeitraum)	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message digest (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms (kryptographische Algorithmen)	SHA-256/RSA 4096“