

BESCHLÜSSE

BESCHLUSS DER EUROPÄISCHEN ZENTRALBANK

vom 11. Januar 2013

über die Festlegung eines Rahmens für eine Public-Key-Infrastruktur (PKI) für das Europäische System der Zentralbanken

(EZB/2013/1)

(2013/132/EU)

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 (nachfolgend die „ESZB-Satzung“), insbesondere auf Artikel 12.1 in Verbindung mit Artikel 3.1, Artikel 5, Artikel 12.3 und Artikel 16 bis 24,

in Erwägung nachstehender Gründe:

- (1) Gemäß Artikel 12.1 der ESZB-Satzung erlässt der EZB-Rat die Leitlinien und fasst die Beschlüsse, die erforderlich sind, um die Erfüllung der dem Europäischen System der Zentralbanken (ESZB) und dem Eurosystem nach dem Vertrag und der ESZB-Satzung übertragenen Aufgaben zu gewährleisten. Dies umfasst die Entscheidungsbefugnis über die Organisation von für die Erfüllung dieser Aufgaben erforderlichen Nebentätigkeiten, wie etwa die Ausstellung und Verwaltung von elektronischen Zertifikaten, um Informationen, die über elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems gespeichert und verarbeitet werden, zu schützen, und für die Datenkommunikation zu und von ihnen.
- (2) Gemäß Artikel 12.3 der ESZB-Satzung hat der EZB-Rat auch die Entscheidungsbefugnis, die interne Organisation der Europäischen Zentralbank (EZB) und ihrer Beschlussorgane zu regeln. Der EZB-Rat ist dementsprechend ermächtigt, zu entscheiden, dass die EZB von der eigenen Public-Key-Infrastruktur des Eurosystems ausgestellte elektronische Zertifikate nutzt.
- (3) Der Kreis der auf eine wachsende Anzahl sich ständig weiterentwickelnder elektronischer Anwendungen, Systemen, Plattformen und Dienstleistungen des ESZB und des zugreifenden Nutzer wächst. Der EZB-Rat hat einen Bedarf an fortschrittlichen Diensten zur Informationssicherheit, z. B. die strenge Authentifizierung, elektronische Signatur und Verschlüsselung durch die Nutzung elektronischer Zertifikate festgestellt.
- (4) Wenige Zentralbanken des ESZB haben ihre eigene Public-Key-Infrastruktur; viele Drittnutzer, die mit den Zentralbanken des ESZB zusammenarbeiten, haben nur schwer Zugang zu einer vom ESZB im Einklang mit seinem Rahmen für die Anerkennung von Zertifikaten akzeptierten Zertifizierungsstelle.
- (5) Das Eurosystem muss seine eigene Public-Key-Infrastruktur schaffen, die alle Arten von elektronischen Zertifikaten wie Personenzertifikate und technische Zertifikate für Nutzer des ESZB und außerhalb des ESZB ausstellen kann und flexibel genug ist, sich an Entwicklungen der elektronischen Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems anzupassen. Diese Public-Key-Infrastruktur (nachfolgend die „ESZB-PKI“) sollte die Dienstleistungen der vom ESZB im Einklang mit dem ESZB-Rahmen für die Anerkennung von Zertifikaten akzeptierten sonstigen Zertifizierungsstellen oder der vom ESZB für TARGET2 und TARGET2-Securities akzeptierten Zertifizierungsstellen für diese beiden Anwendungen ergänzen.
- (6) Am 29. September 2010 hat der EZB-Rat beschlossen, das ESZB-PKI-Projekt zu starten, um die ESZB-PKI aufzubauen und umzusetzen und die zu ihrer Umsetzung erforderlichen Ressourcen zur Verfügung zu stellen. Er hat beschlossen, dass die ESZB-PKI von der Banco de España entwickelt, bei ihr angesiedelt und von ihr betrieben wird.
- (7) Die ESZB-PKI unterstützt indirekt die Erfüllung der Aufgaben des ESZB und des Eurosystems. Sie basiert auf drei Steuerungsebenen: Die Ebene 1 besteht aus dem EZB-Rat und dem Direktorium, die Ebene 2 aus den Zentralbanken des Eurosystems und die Ebene 3 aus der liefernden Zentralbank.
- (8) Auf der Ebene 1 ist der EZB-Rat für die Leitung, das Management und die Kontrolle der für die Entwicklung und den Betrieb der ESZB-PKI erforderlichen Tätigkeiten und Leistungen zuständig. Er ist auch für die Entscheidungen in Bezug auf die ESZB-PKI verantwortlich und entscheidet über die Verteilung der Aufgaben, die nicht spezifisch den Ebenen 2 und 3 zugeordnet sind.
- (9) Die Zentralbanken des Eurosystems sind innerhalb des durch den EZB-Rat festgelegten allgemeinen Rahmens für die Aufgaben der Ebene 2 zuständig. Sie haben Befugnisse in Bezug auf die technische Umsetzung der ESZB-PKI.

- (10) Der Ausschuss für Informationstechnologie des ESZB (ITC) wirkt steuernd auf die Entwicklung der ESZB-PKI ein. Er leitet, bewertet, kontrolliert und genehmigt die Projektleistungen nach Maßgabe der Anerkennungskriterien im Einklang mit dem vom EZB-Rat genehmigten ESZB-Rahmen für die Anerkennung von Zertifikaten, Anwendungsbereich und Zeitplan.
- (11) Auf der Ebene 3 wurde die Banco de España als liefernde Zentralbank ernannt, um die ihr innerhalb des durch den EZB-Rat festgelegten allgemeinen Rahmens übertragenen Aufgaben durchzuführen. Die liefernde Zentralbank hat die technische Infrastruktur und Sicherheitstools und Dienstleistungen zur Schaffung und Nutzung einer Public-Key-Infrastruktur gemäß a) den für sie maßgebenden innerstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ⁽¹⁾, b) den für sie maßgebenden innerstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ⁽²⁾ und c) der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ⁽³⁾ eingerichtet.
- (12) Elektronische Zertifikate sind wesentliche Elemente in elektronischen Anwendungen sowohl für den Authentifizierungsmechanismus für elektronische Signaturen als auch für die Public-Key-basierte Verschlüsselung; deshalb wird die ESZB-PKI die vorhandenen elektronischen Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems sowie aktuelle Projekte des ESZB einbeziehen, um zu gewährleisten, dass ihre Bedürfnisse abgedeckt werden.
- (13) Nationale Zentralbanken (NZBen) außerhalb des Euro-Währungsgebiets können beschließen, von der ESZB-PKI zur Verfügung gestellte Zertifikate und Dienstleistungen zu nutzen —
- zur Überprüfung der Zugriffsrechte des Zertifikatnehmers auf elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems. In diesem Beschluss sind Bezugnahmen auf ein Zertifikat oder elektronisches Zertifikat als Bezugnahmen auf die Datenträger, auf denen das Zertifikat oder elektronische Zertifikat gespeichert ist, zu verstehen;
2. „elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems“: elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen, die das ESZB bzw. das Eurosystem nutzen, wenn sie die nach dem Vertrag und der ESZB-Satzung übertragenen Aufgaben ausüben;
 3. „Public-Key-Infrastruktur“: natürliche Personen, Maßnahmen, Verfahren und Computersysteme, die erforderlich sind, um Dienstleistungen der Authentifizierung, Verschlüsselung, Integrität und Nachprüfbarkeit durch Public- und Private-Key-Kryptographie und elektronische Zertifikate zu erbringen;
 4. „Nutzer“: ein Zertifikatnehmer oder ein vertrauender Dritter oder beide;
 5. „Authentifizierung“: Verfahren zur Überprüfung der Identität des Zertifikatsantragstellers oder Zertifikatnehmers;
 6. „Zentralbank des ESZB“: eine Zentralbank des Eurosystems oder eine NZB außerhalb des Euro-Währungsgebiets;
 7. „Zentralbank des Eurosystems“: eine NZB eines Mitgliedstaats, dessen Währung der Euro ist, einschließlich der liefernden Zentralbank, oder die EZB;
 8. „liefernde Zentralbank“: die vom EZB-Rat zur Entwicklung der ESZB-PKI und zur Erbringung von Dienstleistungen der ESZB-PKI im Namen und zugunsten der Zentralbanken des Eurosystems ernannte NZB;
 9. „NZB außerhalb des Euro-Währungsgebiets“: eine NZB eines Mitgliedstaats, dessen Währung nicht der Euro ist;
 10. „ESZB-PKI-Zertifizierungsstelle“: die das Vertrauen der Nutzer genießende Stelle, die im Namen der Zentralbanken des ESZB oder der Zentralbanken des Eurosystems gemäß dem ESZB-Rahmen für die Anerkennung von Zertifikaten Zertifikate ausstellt, verwaltet, widerruft und erneuert;
 11. „ESZB-PKI-Validierungsstelle“: die das Vertrauen der Nutzer genießende Stelle, die Informationen über die Gültigkeit der von der ESZB-PKI-Zertifizierungsstelle ausgestellten Zertifikate zur Verfügung stellt;
 12. „Zertifikatnehmer“: eine natürliche Person, die Gegenstand eines elektronischen Zertifikats ist und der ein elektronisches Zertifikat ausgestellt wurde, oder ein technischer Komponentenmanager, der ein von der ESZB-PKI-Zertifizierungsstelle ausgestelltes elektronisches Zertifikat für eine technische Komponente akzeptiert hat, oder beide;
 13. „ESZB-Rahmen für die Anerkennung von Zertifikaten“: die vom ITC des ESZB festgelegten Kriterien zur Identifizierung der Zertifizierungsstellen innerhalb und außerhalb des ESZB,

HAT FOLGENDEN BESCHLUSS GEFASST:

Artikel 1

Begriffsbestimmungen

Im Sinne dieses Beschlusses sind die nachfolgend aufgeführten Begriffe wie folgt zu verstehen:

1. „Zertifikat“ oder „elektronisches Zertifikat“: eine von einer Zertifizierungsstelle ausgestellte elektronische Datei, die einen Public Key mit der Identität eines Zertifikatnehmers verbindet und die für alle oder einige der folgenden Zwecke verwendet wird: a) zur Überprüfung, dass ein Public Key zu einem bestimmten Zertifikatnehmer gehört, b) zur Authentifizierung des Zertifikatnehmers, c) zur Überprüfung einer Signatur dieses Zertifikatnehmers, d) zur Verschlüsselung einer an diesen Zertifikatnehmer gerichteten Nachricht, e)

⁽¹⁾ ABl. L 13 vom 19.1.2000, S. 12.

⁽²⁾ ABl. L 281 vom 23.11.1995, S. 31.

⁽³⁾ ABl. L 8 vom 12.1.2001, S. 1.

denen in Bezug auf elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems vertraut werden kann;

14. „Registrierungsstelle“: eine das Vertrauen der Nutzer genießende Stelle, die die Identität eines Zertifikatsantragstellers überprüft bevor die Zertifizierungsstelle der ESZB-PKI ein Zertifikat ausstellt;
15. „vertrauender Dritter“: eine natürliche oder juristische Person, die kein Zertifikatnehmer ist und ein Zertifikat vor der Ausstellung eines Zertifikats durch die ESZB-Zertifizierungsstelle akzeptiert und hierauf vertraut;
16. „Richtlinien für das Revisionswesen“: die vom EZB-Rat am 7. Oktober 1998 festgelegten Richtlinien für das Revisionswesen des ESZB wie sie auf der Website der EZB veröffentlicht sind ⁽¹⁾;
17. „Zertifikatsantragsteller“: eine natürliche Person, die die Ausstellung eines Zertifikats für sich selbst oder für eine technische Komponente beantragt;
18. „technische Komponente“: jede Software- oder Hardwareausstattung, die durch die Verwendung elektronischer Zertifikate identifiziert werden kann.

Artikel 2

Anwendungsbereich

- (1) Dieser Beschluss legt den Rahmen für die ESZB-PKI fest. Die ESZB-PKI ist die eigene Public-Key-Infrastruktur des Eurosystems, die von der liefernden Zentralbank im Namen und zugunsten der Zentralbanken des Eurosystems entwickelt wurde, die gemäß dem ESZB-Rahmen für die Aufnahme von Zertifikaten Zertifikate ausstellt, verwaltet, widerruft und erneuert.
- (2) Da Dienstleistungen der ESZB-PKI vertrauende Dritte betreffen können, legt dieser Beschluss auch die Bedingungen fest, unter denen diese Dritten auf Zertifikate der ESZB-PKI vertrauen können.

Artikel 3

Anwendungsbereich und Ziele der ESZB-PKI

- (1) Elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems mit mittlerer oder höherer Kritikalität dürfen nur genutzt werden, wenn ein Nutzer durch ein elektronisches Zertifikat authentifiziert wurde, das von einer durch das ESZB gemäß dem ESZB-Rahmen für die Anerkennung von Zertifikaten akzeptierten Zertifizierungsstelle, einschließlich der ESZB-PKI-Zertifizierungsstelle oder der vom ESZB für TARGET2 und TARGET2-Securities für diese beiden Anwendungen akzeptierten Zertifizierungsstellen, ausgestellt und verwaltet wurde.
- (2) Die ESZB-PKI-Zertifizierungsstelle stellt elektronische Zertifikate aus und erbringt weitere elektronische Zertifizierungsdienstleistungen für Zertifikatnehmer der Zentralbanken des ESZB und mit ihnen zusammenarbeitender Dritter, damit diese sicher auf elektronische Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und Eurosystems zugreifen und diese nutzen können.

(3) Die ESZB-PKI erbringt die folgenden Zertifizierungsdienstleistungen:

- a) Zertifikatsausstellung, -erneuerung und -widerruf und Bestätigung der Gültigkeit eines Zertifikats in Bezug auf verschiedene Zertifikatsarten;
- b) Ausstellung von Zertifikaten zur Authentifizierung, elektronischen Signatur und Verschlüsselung in Bezug auf dem ESZB angehörende und nicht dem ESZB angehörende Nutzer sowie technische Zertifikate;
- c) Wiederherstellung privater Schlüssel, um die Wiederherstellung von Public-Key-basierten verschlüsselten Informationen bei einem Zertifikatsverlust sicherzustellen;
- d) Bereitstellung und Verwaltung von kryptographischen Token für Zertifikatnehmer soweit erforderlich;
- e) Bereitstellung von Informationen über Verfahren der ESZB-PKI zur Zertifikatsverwaltung, und technische Unterstützung für Projektmanager des ESZB, um ihnen bei der Integration der ESZB-PKI-Zertifikate in ihre Anwendungen zu helfen.

Weitere Dienstleistungen können in Zukunft gemäß den Anforderungen der elektronischen Anwendungen, Systemen, Plattformen und Dienstleistungen des ESZB und Eurosystems hinzugefügt werden.

Artikel 4

ESZB-PKI-Rahmen

- (1) Nach diesem Beschluss werden die Zuständigkeiten und Aufgaben der liefernden Zentralbank und der anderen Zentralbanken des Eurosystems in Bezug auf die Umsetzung, den Betrieb und die Nutzung der ESZB-PKI in einer Level 2-Level 3-Vereinbarung festgelegt und in den ESZB-PKI-Zertifizierungsrichtlinien und dem ESZB-PKI-Sicherheits- und Zertifizierungskonzept näher bestimmt.
- (2) Die Level 2-Level 3-Vereinbarung einschließlich der Service-Level-Vereinbarung enthält die zwischen der liefernden Zentralbank und den Zentralbanken des Eurosystems in Bezug auf die Zuständigkeiten und Aufgaben der liefernden Zentralbank und der Zentralbanken des Eurosystems ausgehandelte Vereinbarung. Sie wird dem EZB-Rat zur Billigung vorgelegt und anschließend von der liefernden Zentralbank und den Zentralbanken des Eurosystems unterzeichnet.
- (3) Die Service-Level-Vereinbarung ist eine Vereinbarung, die sowohl das Niveau der dem Eurosystem von der liefernden Zentralbank in Bezug auf die ESZB-PKI zu erbringenden Dienstleistungen, als auch das Niveau der den NZBen außerhalb des Euro-Währungsgebiets und Dritten vom Eurosystem in Bezug auf die ESZB-PKI zu erbringenden Dienstleistungen bestimmt.
- (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 elektronische Zertifikate, die in den Anwendungsbereich der Richtlinie 1999/93/EG fallen, sowie elektronische Zertifikate, die nicht in ihren 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 beigelegt.

⁽¹⁾ www.ecb.europa.eu.

(5) Eine ESZB-PKI-Zertifizierungsrichtlinie ist ein Regelwerk, das auf alle ausgestellten Zertifikatsarten anwendbar ist. Jede Regel sieht Einzelheiten der Umsetzung in Bezug auf das ESZB-PKI-Sicherheits- und Zertifizierungskonzept für alle ausgestellten Zertifikatsarten vor. Die ESZB-PKI-Zertifizierungsrichtlinien sind der Level 2-Level 3-Vereinbarung beigefügt.

(6) Die ESZB-PKI-Zertifizierungsrichtlinien und das ESZB-PKI-Sicherheits- und Zertifizierungskonzept werden auf der Website der ESZB-PKI veröffentlicht ⁽¹⁾.

(7) Informationen über die ESZB-PKI-Zertifizierungsstelle, einschließlich ihrer Identität sowie ihrer technischen Komponenten, sind im Anhang dieses Beschlusses festgelegt.

Artikel 5

Zuständigkeiten und Aufgaben der liefernden Zentralbank

(1) Die liefernde Zentralbank ist für den Betrieb und die Instandhaltung der ESZB-PKI zugunsten der Zentralbanken des Eurosystems zuständig, einschließlich der Einrichtung, dem Betrieb und der Verwaltung gemäß der Level 2-Level 3-Vereinbarung. Insbesondere stellt sie Zertifikate und ESZB-PKI-Dienstleistungen im Einklang mit Betriebsanforderungen und technischen Spezifikationen, z. B. dem ESZB-Rahmen für die Anerkennung von Zertifikaten und den in der Level 2-Level 3-Vereinbarung festgelegten Anforderungen und Spezifikationen, zur Verfügung.

(2) Die liefernde Zentralbank schafft die erforderliche organisatorische Infrastruktur zur Erzeugung, Ausstellung und Verwaltung von Zertifikaten und stellt sicher, dass die Infrastruktur bestehen bleibt. Zu diesem Zweck kann die liefernde Zentralbank in Absprache mit dem ITC Vorschriften über ihre interne Organisation und Verwaltung verabschieden.

(3) Die liefernde Zentralbank handelt als ESZB-PKI-Zertifizierungsstelle und als ESZB-PKI-Validierungsstelle.

(4) Die Level 2-Level 3-Vereinbarung legt das für die liefernde Zentralbank geltende Haftungsregime fest.

Artikel 6

Zuständigkeiten und Aufgaben der Zentralbanken des Eurosystems

(1) Jede Zentralbank des Eurosystems ist für die Identifizierung ihrer Zertifikatnehmer zuständig. Sie ernennt zur Erfüllung dieser Aufgabe einen Registrierungsverantwortlichen ein, der befugt sein soll, Drittnutzer zu registrieren.

(2) Jede Zentralbank des Eurosystems handelt als vertrauender Dritter hinsichtlich der von der ESZB-PKI für andere Zentralbanken des Eurosystems oder Zertifikatnehmer der Drittnutzer ausgestellten Zertifikate zur Verschlüsselung und elektronischen Signatur.

(3) Jede Zentralbank des Eurosystems, die Dienstleistungen der ESZB-PKI nutzt, handelt als Registrierungsstelle für ihre Zertifikatsantragsteller und stellt sicher, dass ihre Zertifikatsantragsteller die im Antragsformular der ESZB-PKI-Zertifizierungsstelle für ihre Dienstleistungen festgelegten Nutzerbedingungen akzeptieren und anwenden.

Artikel 7

Beziehungen zwischen den Zentralbanken des Eurosystems, Dritten und Zertifikatnehmern

Jede Zentralbank des Eurosystems trifft Regelungen in Bezug auf einen sicheren Zugriff und eine sichere Nutzung durch Dritte der elektronischen Anwendungen, Systeme, Plattformen und Dienstleistungen des ESZB und des Eurosystems durch die Nutzung von ESZB-PKI-Zertifikaten. Die Beziehung zwischen der betreffenden Zentralbank des Eurosystems und den Dritten, die ESZB-PKI-Zertifikate nutzen, unterliegt ausschließlich diesen Regelungen. Die Dritten sind verpflichtet, die Zertifizierungsrichtlinien der ESZB-PKI, das ESZB-PKI-Sicherheits- und Zertifizierungskonzept und die im Antragsformular der ESZB-PKI-Zertifizierungsstelle für ihre Dienstleistungen festgelegten Nutzerbedingungen einzuhalten.

Artikel 8

Beziehungen zu vertrauenden Dritten

Auf ein nach diesem Beschluss ausgestelltes elektronisches Zertifikat kann vertraut werden, sofern ein vertrauender Dritter:

- a) die Gültigkeit, Aussetzung oder den Widerruf des Zertifikats unter Verwendung aktueller Widerrufsstatusinformationen überprüft;
- b) alle bezüglich des Zertifikats bestehenden Einschränkungen beachtet und
- c) das ESZB-PKI-Sicherheits- und Zertifizierungskonzept und die geltenden ESZB-PKI-Zertifizierungsrichtlinien akzeptiert.

Artikel 9

Rechte an der ESZB-PKI

(1) Die ESZB-PKI steht vollständig im Eigentum der Zentralbanken des Eurosystems.

(2) Angesichts dessen gewährt die liefernde Zentralbank den Zentralbanken des Eurosystems, soweit es nach den geltenden Rechtsvorschriften möglich ist, alle Lizenzen hinsichtlich der Rechte des geistigen Eigentums, die erforderlich sind, damit die Zentralbanken des Eurosystems die ESZB-PKI und ihre Komponenten und die volle Bandbreite der ESZB-PKI-Dienstleistungen nutzen und auch Dritten nach dem ESZB-PKI-Sicherheits- und Zertifizierungskonzept und den ESZB-PKI-Zertifizierungsrichtlinien ESZB-PKI-Dienstleistungen erbringen können. Die liefernde Zentralbank stellt die Zentralbanken des Eurosystems von allen Ansprüchen frei, die von Dritten in Bezug auf Verstöße im Zusammenhang mit diesen geistigen Eigentumsrechten erhoben werden.

(3) Die Rechte der Zentralbanken des Eurosystems an der ESZB-PKI werden im Einzelnen zwischen der Ebene 2 und Ebene 3 in der Level 2-Level 3-Vereinbarung vereinbart.

Artikel 10

Haftung der Zentralbanken des Eurosystems gegenüber Nutzern

(1) Sofern sie nicht nachweisen, dass sie nicht fahrlässig gehandelt haben, haften die Zentralbanken des Eurosystems gemäß ihren Aufgaben und Zuständigkeiten im Rahmen der

⁽¹⁾ <http://pki.escb.eu>.

ESZB-PKI in Bezug auf Schäden gegenüber einem Nutzer, der vernünftigerweise auf das qualifizierte Zertifikat vertraut, im Sinne der Richtlinie 1999/93/EG, 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 im Zertifikat;
- b) die Zusicherung, dass der in dem qualifizierten Zertifikat angegebene Unterzeichner zum Zeitpunkt der Ausstellung des Zertifikats im Besitz der Signaturstellungsdaten war, die den im Zertifikat angegebenen bzw. identifizierten Signaturprüfdaten entsprechen;
- c) die Zusicherung, dass in Fällen, in denen die ESZB-PKI sowohl die Signaturstellungsdaten als auch die Signaturprüfdaten erzeugt, beide Komponenten in komplementärer Weise genutzt werden können;
- d) die Nichtregistrierung des Widerrufs des qualifizierten Zertifikats.

(2) Die Zentralbanken des Eurosystems gehen keine Verpflichtungen ein, geben keine Garantien ab und übernehmen keine Haftung gegenüber Nutzern, sofern es nicht ausdrücklich in diesem Beschluss und im ESZB-PKI-Sicherheits- und Zertifizierungskonzept vorgesehen ist.

Artikel 11

Teilnahme der NZBen außerhalb des Euro-Währungsgebiets an der ESZB-PKI

(1) Eine NZB außerhalb des Euro-Währungsgebiets kann für ihre internen Nutzer sowie für Drittnutzer als Registrierungsstelle handeln und das Amt des Registrierungsverantwortlichen einrichten, um diese Aufgabe zu erfüllen.

(2) Vorbehaltlich der Genehmigung des EZB-Rates kann eine NZB außerhalb des Euro-Währungsgebiets auch beschließen, die ESZB-PKI-Dienstleistungen unter denselben Bedingungen zu nutzen, die auch für Zentralbanken des Eurosystems gelten. Zu diesem Zweck gibt die NZB außerhalb des Euro-Währungsgebiets eine Erklärung beim EZB-Rat ab, in der sie bestätigt, die Pflichten des vorliegenden Beschlusses und der Level 2-Level 3-Vereinbarung einzuhalten. Eine NZB außerhalb des Euro-Währungsgebiets wird nicht Miteigentümerin der ESZB-PKI und ist nicht verpflichtet, zum Finanzrahmen der ESZB-PKI beizutragen.

Artikel 12

Datenschutz

Die Zentralbanken des Eurosystems sind verpflichtet, bei der Ausübung ihrer Aufgaben in Bezug auf die ESZB-PKI die Datenschutzvorschriften für ihre Verarbeitung personenbezogener Daten einzuhalten.

Artikel 13

Interne Revision

Prüfungen der ESZB-PKI werden im Einklang mit den in den Richtlinien für das Revisionswesen festgelegten Grundsätzen und Regelungen ausgeführt. Sie ergehen unbeschadet der internen Kontrollen und Rechnungslegungsvorschriften, die von den Zentralbanken des Eurosystems erlassen werden oder für sie gelten.

Artikel 14

Finanzregelungen

Die Zentralbanken des Eurosystems tragen die Kosten der Entwicklung und des Betriebs der ESZB-PKI gemäß den ausführlichen Bestimmungen im ESZB-PKI-Finanzrahmen.

Artikel 15

Rolle des Direktoriums

(1) Gemäß Artikel 17.3 des Beschlusses EZB/2004/2 vom 19. Februar 2004 zur Verabschiedung der Geschäftsordnung der Europäischen Zentralbank⁽¹⁾ überträgt der EZB-Rat seine normativen Befugnisse auf das Direktorium, um alle Maßnahmen zur Durchführung dieses Beschlusses zu ergreifen, die für die Effizienz und Sicherheit der ESZB-PKI erforderlich sind, und um Änderungen der technischen Aspekte der ESZB-PKI und der in den Anhängen der Level 2-Level 3-Vereinbarung vorgesehenen ESZB-PKI-Dienstleistungen unter Berücksichtigung der Stellungnahme des ITC und gegebenenfalls des IT-Lenkungsausschusses des Eurosystems vorzunehmen.

(2) Das Direktorium teilt dem EZB-Rat unverzüglich jede Maßnahme mit, die es gemäß Absatz 1 ergreift, und befolgt alle diesbezüglichen Entscheidungen des EZB-Rates.

Geschehen zu Frankfurt am Main am 11. Januar 2013.

Der Präsident der EZB

Mario DRAGHI

⁽¹⁾ ABl. L 80 vom 18.3.2004, S. 33.

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:

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

- **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:

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