DURCHFÜHRUNGSBESCHLUSS (EU) 2016/650 DER KOMMISSION

vom 25. April 2016

zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 [1], insbesondere auf Artikel 30 Absatz 3 und Artikel 39 Absatz 2,

in Erwägung nachstehender Gründe:

(1) In Anhang II der Verordnung (EU) Nr. 910/2014 sind die Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten und qualifizierte elektronische Siegelerstellungseinheiten festgelegt.

(2) Die Aufgabe der Ausarbeitung der technischen Spezifikationen, die für die Herstellung und das Inverkehrbringen von Produkten, die dem derzeitigen Stand der Technik entsprechen, erforderlich sind, wird von den für die Normung zuständigen Gremien wahrgenommen.

(3) Die Internationale Organisation für Normung (ISO) und die Internationale Elektrotechnische Kommission (IEC) legen die allgemeinen Konzepte und Grundsätze der IT-Sicherheit fest und bestimmen das allgemeine Bewertungsmodell, das der Bewertung der Sicherheitseigenschaften von IT-Produkten zugrunde liegt.

(4) Im Rahmen des durch die Kommission erteilten Normungsauftrags M/460 hat das Europäische Komitee für Normung (CEN) Normen für qualifizierte elektronische Signatur- und Siegelerstellungseinheiten ausgearbeitet, bei denen sich die elektronischen Signatur- bzw. Siegelerstellungsdaten vollständig, aber nicht notwendigerweise ausschließlich in der Umgebung des Nutzers befinden. Diese Normen gelten als geeignet, um die Konformität solcher Einheiten mit den einschlägigen Anforderungen gemäß Anhang II der Verordnung (EU) Nr. 910/2014 zu bewerten.

(5) Gemäß Anhang II der Verordnung (EU) Nr. 910/2014 darf nur ein qualifizierter Vertrauensdiensteanbieter elektronische Signaturerstellungsdaten im Namen eines Unterzeichners verwalten. Andere Sicherheitsanforderungen und entsprechende Zulassungsspezifikationen gelten, wenn der Unterzeichner im physischen Besitz eines Produktes ist und wenn ein qualifizierter Vertrauensdiensteanbieter im Namen des Unterzeichners tätig ist. Um beide Fälle zu erfassen und außerdem die laufende Entwicklung von Produkten und Bewertungsnormen, die besonderen Bedürfnissen entsprechen, zu fördern, sollten im Anhang dieses Beschlusses Normen für beide Fälle aufgeführt werden.

(6) Zum Zeitpunkt der Annahme dieses Beschlusses bieten bereits mehrere Vertrauensdiensteanbieter Lösungen für die Verwaltung elektronischer Signaturerstellungsdaten im Namen ihrer Kunden an. Die Zertifizierung von Produkten beschränkt sich derzeit auf die Hardware-Sicherheitsmodule, die zwar nach verschiedenen Normen, jedoch nicht nach den Anforderungen an qualifizierte Signatur- und Siegelerstellungseinheiten zertifiziert sind. Dennoch wurden bisher noch keine Normen, wie z. B. EN 419 211 (für elektronische Signaturen, die vollständig, aber nicht notwendigerweise ausschließlich in der Umgebung des Nutzers erstellt werden), für den ebenso wichtigen Markt für zertifizierte Fernsignaturen veröffentlicht. Da sich für derartige Zwecke möglicherweise geeignete Normen derzeit in der Entwicklung befinden, wird die Kommission den vorliegenden Beschluss ergänzen, sobald derartige Normen verfügbar sind und bewertungsgemäß den Anforderungen nach Anhang II der Verordnung (EU) Nr. 910/2014 entsprechen. Bis zur Aufstellung des Verzeichnisses solcher Normen wird unter den in Artikel 30 Absatz 3 Buchstabe b der Verordnung (EU) Nr. 910/2014 genannten Bedingungen ein alternatives Verfahren für die Bewertung der Konformität solcher Produkte verwendet.

(7) Im Anhang ist die Norm EN 419 211 aufgeführt, die aus mehreren, verschiedene Fälle erfassenden Teilen (1 bis 6) besteht. Die Normen EN 419 211 Teil 5 und EN 419 211 Teil 6 enthalten Erweiterungen im

[1] ABl. L 257 vom 28.8.2014, S. 73.

Zusammenhang mit der Umgebung der qualifizierten Signaturerstellungseinheit, beispielsweise für die Kommunikation mit vertrauenswürdigen Signaturerstellungsanwendungen. Produktherstellern steht es frei, diese Erweiterungen zu verwenden. Gemäß Erwägungsgrund 56 der Verordnung (EU) Nr. 910/2014 erstreckt sich der Anwendungsbereich der Zertifizierung nach den Artikeln 30 und 39 dieser Verordnung nur auf den Schutz der Signaturerstellungsdaten, wogegen Signaturerstellungsanwendungen davon ausgeschlossen sind.

(8) Damit die durch eine qualifizierte Signatur- oder Siegelerstellungseinheit erzeugten elektronischen Signaturen oder Siegel im Sinne des Anhangs II der Verordnung (EU) Nr. 910/2014 verlässlich gegen Fälschung geschützt sind, sind geeignete kryptografische Algorithmen, Schlüssellängen und Hash-Funktionen Voraussetzung für die Sicherheit des zertifizierten Produkts. Da der Bereich der elektronischen Signaturen und Siegel nicht auf europäischer Ebene harmonisiert ist, sollten die Mitgliedstaaten zusammenarbeiten, um sich auf die zu verwendenden kryptografischen Algorithmen, Schlüssellängen und Hash-Funktionen in diesem Bereich zu einigen.

(9) Mit Annahme des vorliegenden Beschlusses wird die Entscheidung 2003/511/EG der Kommission [1] hinfällig. Sie ist daher aufzuheben.

(10) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des in Artikel 48 der Verordnung (EU) Nr. 910/2014 genannten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Die Normen für die Sicherheitsbewertung informationstechnischer Produkte, die gemäß Artikel 30 Absatz 3 Buchstabe a bzw. Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 für die Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten bzw. qualifizierter elektronischer Siegelerstellungseinheiten gelten, wenn sich die elektronischen Signatur- bzw. Siegelerstellungsdaten vollständig, aber nicht notwendigerweise ausschließlich in der Umgebung des Nutzers befinden, sind im Anhang des vorliegenden Beschlusses aufgeführt.

(2) Bis die Kommission ein Verzeichnis der Normen für die Sicherheitsbewertung informationstechnischer Produkte erstellt hat, die für die Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten oder qualifizierter elektronischer Siegelerstellungseinheiten gelten, wenn ein qualifizierter Vertrauensdiensteanbieter die elektronischen Signatur- bzw. Siegelerstellungsdaten im Namen eines Unterzeichners oder eines Siegelerstellers verwaltet, erfolgt die Zertifizierung solcher Produkte auf der Grundlage eines Verfahrens gemäß Artikel 30 Absatz 3 Buchstabe b, bei dem gleichwertige Sicherheitsniveaus gemäß Artikel 30 Absatz 3 Buchstabe a angewendet werden und das die in Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014 genannte öffentliche oder private Stelle der Kommission mitteilt.

Artikel 2

Die Entscheidung 2003/511/EG wird aufgehoben.

Artikel 3

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

Brüssel, den 25. April 2016

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

[1] Entscheidung 2003/511/EG der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates(ABl. L 175 vom 15.7.2003, S. 45).

ANHANG

VERZEICHNIS DER NORMEN GEMÄSS ARTIKEL 1 ABSATZ 1

— ISO/IEC 15408 — Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit, Teile 1 bis 3, wie folgt:

  — ISO/IEC 15408-1:2009 — Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1. ISO, 2009

  — ISO/IEC 15408-2:2008 — Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2. ISO, 2008

  — ISO/IEC 15408-3:2008 — Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3. ISO, 2008

  und

— ISO/IEC 18045:2008 — Informationstechnik — IT-Sicherheitsverfahren — Methode für die Bewertung der IT-Sicherheit,

  und

— EN 419 211 — Schutzprofile für sichere Signaturerstellungseinheiten, Teile 1 bis 6 — soweit zutreffend — wie folgt:

  — EN 419211-1:2014 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick

  — EN 419211-2:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Einheiten mit Schlüsselerzeugung

  — EN 419211-3:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsselimport

  — EN 419211-4:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Zertifikaterzeugungsanwendung

  — EN 419211-5:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung

  — EN 419211-6:2014 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung.