TECHNISCHE SPEZIFIKATION

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

CEN/TS 419261

März 2015

ICS 03.120.20; 35.040; 35.240.30

Deutsche Fassung

Sicherheitsanforderungen für vertrauenswürdige Systeme zur Verwaltung von Zertifikaten für elektronische Signaturen und Zeitstempel

Security requirements for trustworthy systems managing certificates and time-stamps

Exigences de sécurité pour systèmes de confiance gérant des certificats et des horodatages

Diese Technische Spezifikation (CEN/TS) wurde vom CEN am 18. November 2014 als eine künftige Norm zur vorläufigen Anwendung angenommen.

Die Gültigkeitsdauer dieser CEN/TS ist zunächst auf drei Jahre begrenzt. Nach zwei Jahren werden die Mitglieder des CEN gebeten, ihre Stellungnahmen abzugeben, insbesondere über die Frage, ob die CEN/TS in eine Europäische Norm umgewandelt werden kann.

Die CEN Mitglieder sind verpflichtet, das Vorhandensein dieser CEN/TS in der gleichen Weise wie bei einer EN anzukündigen und die CEN/TS verfügbar zu machen. Es ist zulässig, entgegenstehende nationale Normen bis zur Entscheidung über eine mögliche Umwandlung der CEN/TS in eine EN (parallel zur CEN/TS) beizubehalten.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Ref. Nr. CEN/TS 419261:2015 D

Inhalt

Seite

Vorwort 4
Einleitung 7
1 Anwendungsbereich 9
1.1 Allgemeines 9
1.2 Spezifisch für die Europäische Verordnung 9
2 Normative Verweisungen 10
3 Begriffe, Symbole und Abkürzungen 11
3.1 Begriffe 11
3.2 Symbole und Abkürzungen 15
4 Beschreibung eines Systems von Vertrauensdiensteanbietern 17
4.1 Allgemeines 17
4.2 TSP-Kerndienste für die Zertifikatverwaltung 17
4.3 Ergänzende TSP-Dienste für die Zertifikatverwaltung 18
4.4 TSP Kerndienste für die elektronische Zeitstempelverwaltung 19
4.5 Gesamtarchitektur 20
5 Sicherheitsanforderungen 21
5.1 Zusammenhang zwischen Sicherheitsanforderungen und -empfehlungen 21
5.2 Allgemeine Sicherheitsanforderungen 22
5.2.1 Verwaltung 22
5.2.2 Systeme und Betriebsvorgänge 23
5.2.3 Identifizierung und Authentifizierung 24
5.2.4 System-Zugriffskontrolle 26
5.2.5 Schlüsselmanagement 26
5.2.6 Zurechenbarkeit und Audit 32
5.2.7 Archivierung 34
5.2.8 Datensicherung und Wiederherstellung 34
5.2.9 Anforderungen an die Netzwerksicherheit für die Betriebsumgebung 35
5.2.10 Physikalische Sicherheitsanforderungen an die Betriebsumgebung 36
5.3 Sicherheitsanforderungen an Kerndienste für TSP zur Verwaltung von Zertifikaten 36
5.3.1 Allgemeines 36
5.3.2 Registrierungsdienst 36
5.3.3 Zertifikatausstellungsdienst 38
5.3.4 Ausgabedienst 41
5.3.5 Zertifikat-Sperrdienst 41
5.3.6 Zertifikat-Sperrstatusdienst 44
5.4 Sicherheitsanforderungen an die ergänzenden Dienste 45
5.4.1 Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber 45
5.5 Sicherheitsanforderungen an die Kerndienste für TWS zur Verwaltung von elektronischen Zeitstempeln 48
5.5.1 Zeitstempeldienst 48

Anhang A (informativ) **Physikalische Sicherheitsanforderungen an die Betriebsumgebung** **51**
A.1 Allgemeines **51**
A.2 P1 Eindringsicherer Sicherheitsperimeter **51**
A.3 P2 Zutrittskontrollsystem **52**
A.4 P3 Einbruchalarmsystem **53**
A.5 P4 Brandschutz und Brandverhütung **53**
A.6 P5 Stromversorgung **54**
A.7 P6 Klimatisierung und Lüftung **54**

Anhang B (informativ) **Netzwerksicherheitsbezogene Anforderungen an die Betriebsumgebung** **56**
B.1 Allgemeines **56**
B.2 NET1 Geschützte TWS-Architektur **56**
B.3 NET2 Protokollierung **57**
B.4 NET3 Überwachung und Alarmierung **57**

Literaturhinweise **58**

Vorwort

Dieses Dokument (CEN/TS 419261:2015) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Dieses Dokument wurde unter einem Mandat erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben.

Die erfolgreiche Umsetzung der Europäischen Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen ([RL 1999/93/EG]) und der Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [Reg. 910/2014/EU] erfordert Normen zu Diensten, Prozessen, Systemen und Produkten im Zusammenhang mit elektronischen Signaturen sowie eine Anleitung zur Konformitätsbeurteilung für diese Dienste, Prozesse, Systeme und Produkte.

ANMERKUNG Nach Artikel 50 der Verordnung 910/2014/EU wird die Richtlinie 1999/93/EG zum 01. Juli 2016 aufgehoben und Verweise auf die aufgehobene Richtlinie müssen als Verweise auf die Verordnung interpretiert werden.

Im Jahre 1999 startete das Europäische Normungsgremium für Informations- und Kommunikations–technologie (en: European Information and Communications Technologies Standards Board) mit Unterstützung der Europäischen Kommission eine Initiative, die die Industrie und die Behörden sowie Fachleute und weitere Marktteilnehmer mit der Absicht zusammenführte, die Europäische Initiative zur Normung elektronischer Signaturen (EESSI, en: European Electronic Signature Standardisation Initiative) ins Leben zu rufen.

In diesem Rahmen wurden das Comité Européen de Normalisation/Information Society Standardisation System (CEN/ISSS, Normungssystem für die Informationsgesellschaft im CEN) und das European Telecommunications Standards Institute/Electronic Signatures and Infrastructures (ETSI/ESI, Europäisches Institut für Telekommunikationsnormen/Elektronische Signaturen und Infrastrukturen) mit der Ausführung eines Arbeitsprogramms zur Erarbeitung allgemein anerkannter Normen zur Unterstützung der Umsetzung der [RL 1999/93/EG] und der Entwicklung einer Europäischen Infrastruktur für elektronische Signaturen beauftragt.

Der CEN/ISSS-Workshop zu elektronischen Signaturen (WS/E-SIGN) führte zu einer Reihe von Ergebnissen, CEN Workshop Agreements (CWA), die einen Beitrag zu diesen allgemein anerkannten Normen leisteten.

Im Jahre 2011 unterzeichnete die Europäische Kommission (EU-Kommission) mit Unterstützung der Europäischen Freihandelsassoziation eine spezifische Zuwendungsvereinbarung mit dem Europäischen Komitee für Normung (CEN) hinsichtlich der Aktualisierung der bestehenden CEN Workshop Agreements (CWA) zur europäischen elektronischen Signatur im Rahmen von Phase 1 des Mandats M/460. Das vorliegende Dokument stellt eine derartiges CEN Workshop Agreement dar, das anfangs als CWA erarbeitet und dann zu einer Technischen Spezifikation (TS) aktualisiert wurde.

Der Zweck dieser TS besteht in der Beschreibung der Sicherheitsanforderungen an vertrauenswürdige Systeme, die Zertifikate für elektronische Signaturen verwalten, sowie in der Definition von Sicherheitsanforderungen an das Gesamtsystem, während EN 419221 Sicherheitsanforderungen an kryptographische Einheiten festlegt. Die Anforderungen beruhen teilweise auf den Common Criteria [CC], Teil 2, die TS weist jedoch keine Übereinstimmung mit den [CC] auf, wie z. B. EN 419221. Folglich kann diese TS nicht für die Durchführung der Common-Criteria-Zertifizierung von Produkten angewendet werden.

Die vorliegende TS ist für die Anwendung durch Planer und Entwickler von Systemen zur Verwaltung von Zertifikaten und Zeitstempeln sowie die Anwender derartiger Systeme (Kunden) vorgesehen.

Kurzfassung

Diese TS legt Sicherheitsanforderungen an Produkte und technische Komponenten fest, die von Vertrauensdiensteanbietern (TSP, en: Trust Service Providers) benutzt werden, um Zertifikate und elektronische Zeitstempel im Sinne der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [Reg.910/2014/EU], auszugeben und zu verwalten.

Die Benennung TSP umfasst Zertifizierungsdiensteanbieter (CSP, en: certification service provider), die qualifizierte Zertifikate (QC, en: qualified certificates) entsprechend der Definition in der Richtlinie „RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ [RL 1999/93/EG] ausgeben. Diese Zertifikate werden im Zusammenhang mit elektronischen Signaturen und fortgeschrittenen elektronischen Signaturen nach [RL 1999/93/EG] eingesetzt. Darüber hinaus bieten durch einen TSP ausgegebene elektronische Zeitstempel einen Nachweis dafür, dass die gestempelten Daten zu einem bestimmten Zeitpunkt vorlagen.

Diese Technische Spezifikation umfasst dieselben Anforderungen an vertrauenswürdige Systeme, die von CSPs nach [RL 1999/93/EG] verwendet werden und an vertrauenswürdige Systeme, die von TSPs nach [Verordnung 910/2014/EU] verwendet werden. Jedoch erlaubt [Verordnung 910/2014/EU] den TSPs die Verwaltung von elektronischen Zeitstempeln, ohne Zertifikate zu verwalten. Dies dürfen CSPs nach [RL 1999/93/EG] nicht. Daher unterscheidet diese technische Spezifikation falls notwendig auf Basis der zur Verfügung stehenden Dienste zwischen CSPs und TSPs.

TSP müssen vertrauenswürdige Systeme (TWS, en: trustworthy systems) benutzen, um die folgenden in dieser TS definierten Dienste auf sichere Weise anbieten zu können:

a) Registrierungsdienst — zur Überprüfung der Identität und gegebenenfalls jeglicher spezifischer Attribute eines Zertifikatinhabers;

b) Zertifikatausstellungsdienst — zur Erstellung von Zertifikaten;

c) Ausgabedienst — zur Bereitstellung von Zertifikaten und Richtlinieninformationen an Zertifikatinhaber und vertrauende Parteien;

d) Sperrdienst — zur Bearbeitung von Sperranfragen;

e) Sperrstatusdienst — zur Bereitstellung von Informationen zum Zertifikatsperrstatus an vertrauende Parteien;

f) Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber — zur Herstellung und Bereitstellung von Signaturerstellungseinheiten (SCDev, en: Signature Creation Devices) an Zertifikatinhaber. Dies umfasst die Bereitstellung qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten (QSCD, en: Qualifed electronic Signature and Seal Creation Device);

g) Zeitstempeldienst — zur Bereitstellung eines Zeitstempeldienstes, der zu Zwecken der Signaturüberprüfung erforderlich sein kann.

Der TSP muss Folgendes erfüllen:

h) die in 5.2 festgelegten „Allgemeinen Sicherheitsanforderungen“, die für alle zuvor erwähnten Dienste gelten;

i) die in 5.3, 5.4 und 5.5 festgelegten Sicherheitsanforderungen, die für einige der zuvor erwähnten Dienste gelten.

Entsprechend [RL 1999/93/EG] müssen CSP die für die Ausgabe und Verwaltung qualifizierter Zertifikate relevanten ersten fünf Kerndienste (Registrierungsdienst, Zertifikatausstellungsdienst, Ausgabedienst, Sperrdienst und Sperrstatusdienst) entwickeln und anwenden. Die anderen beiden Dienste (Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber und Zeitstempeldienst) sind optional und müssen nicht durch die CSP zur Verfügung gestellt und unterhalten werden, da sie in [RL 1999/93/EG] nicht spezifisch erwähnt sind.

TSPs zum Verwalten von Zertifikaten, die nach Verordnung (EU) Nr. 910/2014 [Verordnung 910/2014/EU] arbeiten, müssen die für die Ausgabe und Verwaltung qualifizierter Zertifikate relevanten ersten fünf Kerndienste (Registrierungsdienst, Zertifikatausstellungsdienst, Ausgabedienst, Sperrdienst und Sperrstatusdienst) entwickeln und anwenden. Der Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber ist ein optionaler Dienst für diese TSP. TSP zum Verwalten elektronischer Zeitstempel müssen den für die Ausgabe und Verwaltung elektronischer Zeitstempel relevanten Zeitstempeldienst entwickeln und anwenden.

TSP, die Folgendes ausgeben:

j) Zertifikate nach ETSI/TS 119 411-1 oder TS 119 411-2 (oder entsprechender Europäischer Normen die zu einem späteren Zeitpunkt veröffentlicht werden) und/oder

k) Zeitstempel nach ETSI TS 119 421 (oder entsprechender Europäischer Normen die zu einem späteren Zeitpunkt veröffentlicht werden),

dürfen TWS nutzen, die unabhängig gegen die relevanten Sicherheitsanforderungen nach dieser TS beurteilt wurden und für die die Übereinstimmung mit diesen Anforderungen erklärt wurde. In diesem Fall kann der TSP den Aufwand zum Erreichen der Übereinstimmung ihrer Richtlinien mit den relevanten Normen sowie die Erfüllung der Anforderungen nach [RL 1999/93/EG] und/oder [Verordnung 910/2014/EU] reduzieren.

Eine Anleitung zur Konformitätsbeurteilung in Bezug auf die Sicherheitsanforderungen nach dieser TS ist in CWA 14172-3 enthalten.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Technische Spezifikation anzukündigen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die Europäische Richtlinie [RL 1999/93/EG] und die Verordnung (EU) Nr. 910/2014 [Verordnung 910/2014/EU] legen einen Anforderungsrahmen für die Anwendung elektronischer Signaturen fest, die rechtlich gleichwertig zu handschriftlich verfassten Unterschriften sind. Dies gilt für „fortgeschrittene elektronische Signaturen“, die auf einem „qualifizierten Zertifikat“ beruhen und von einer „sicheren Signaturerstellungseinheit“ nach Artikel 5.1 der [RL 1999/93/EG] erstellt werden und qualifizierte Signaturen nach Artikel 25.2 der [Verordnung 910/2014/EU].

Die durch die TSP bei der Ausgabe qualifizierter Zertifikate (QC) und TSP bei der Bereitstellung qualifizierter Vertrauensdienste zu erfüllenden Anforderungen sind insbesondere in [RL 1999/93/EG], Anhang II und [Verordnung 910/2014/EU], Artikel 24.2 €, angegeben. Im Speziellen müssen sie:

— vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische Sicherheit der von ihnen unterstützten Verfahren gewährleisten.

Die vorliegende TS definiert Sicherheitsanforderungen an TWS innerhalb des Bereichs von Diensten, die ein TSP anbieten muss. Es ist davon auszugehen, dass TWS, die die relevanten Sicherheitsanforderungen dieser TS erfüllen, durch TSPs genutzt werden dürfen, um die für die Anwendung von Systemen in Übereinstimmung mit [RL 1999/93/EG] und/oder [Verordnung 910/2014/EU] erforderlichen Anstrengungen zu verringern. Dieser Ansatz sollte eine Hilfestellung für die Industrie bei der Entwicklung von Systemen bieten, die die Anforderungen nach [RL 1999/93/EG], Anhang II (f) und [Verordnung 910/2014/EU], Artikel 24.2 (e), erfüllen.

ETSI/TS 119 411-1, 119 411-2 und 119 421 wurden als Verweisungen berücksichtigt. Als Folge daraus sind für TWS, die die relevanten Sicherheitsanforderungen dieser TS bereits erfüllen, nur geringfügiger Konfigurationsaufwand seitens der sie nutzenden TSP erforderlich, um die in ETSI/TS 119 411-1, 119 411-2 und 119 421 (oder entsprechender Europäischer Normen die zu einem späteren Zeitpunkt veröffentlicht werden) definierten Sicherheitsanforderungen an TWS zu erfüllen. Darüber hinaus dürfen konforme TWS ohne Erfordernis einer wiederholten Konformitätsbeurteilung durch verschiedene TSP angewendet werden.

Um die TSP bei der Bereitstellung der folgenden Kerndienste zu unterstützen, müssen TWS für TSPs zum Verwalten von Zertifikaten die Sicherheitsanforderungen nach 5.2 und 5.3 erfüllen:

a) Registrierung von Zertifikatinhaberinformationen (Registrierungsdienst);

b) Ausstellung von Zertifikaten (Zertifikatausstellungsdienst);

c) Ausgabe von Zertifikaten (Ausgabedienst):

d) Zertifikatsperrverwaltung (Sperrdienst);

e) Bereitstellung des Zertifikatsperrsstatus (Sperrstatusdienst).

TWS für TSPs zum Verwalten von Zertifikaten dürfen die weiteren Sicherheitsanforderungen nach 5.4 und 5.5 erfüllen, um die TSP bei der Bereitstellung der folgenden ergänzenden Dienste zu unterstützen:

f) Herstellung von Signaturerstellungseinheiten / qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten (Bereitstellungsdienst für Signaturerstellungseinheiten für Zertifikatinhaber);

g) Zeitstempelfunktionen (Zeitstempeldienst).