ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 419241-1:2018

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen

Systèmes fiables de serveur de signature électronique - Partie 1: Exigences de sécurité générales du système

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

07/2018

Nationales Vorwort

Diese Europäische Norm EN 419241-1:2018 wurde als luxemburgische Norm ILNAS-EN 419241-1:2018 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

DIESES WERK IST URHEBERRECHTLICH GESCHÜTZT
Kein Teil dieser Veröffentlichung darf ohne schriftliche Einwilligung weder vervielfältigt noch in sonstiger Weise genutzt werden - sei es elektronisch, mechanisch, durch Fotokopien oder auf andere Art!

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

ENTWURF
prEN 419241-1

März 2017

ICS 35.030

Vorgesehen als Ersatz für CEN/TS 419241:2014

Deutsche Fassung

Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemsicherheitsanforderungen

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Systèmes fiables de Serveur de Signature électronique - Partie 1: Exigences de sécurité générales du système

Dieser Europäische Norm-Entwurf wird den CEN-Mitgliedern zur Umfrage vorgelegt. Er wurde vom Technischen Komitee CEN/TC 224 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CEN-Mitglieder gehalten, die CEN-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Dieser Europäische Norm-Entwurf wurde vom CEN in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Warnvermerk : Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäischen Norm in Bezug genommen werden.

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

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

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

© 2017 CEN Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den nationalen Mitgliedern von CEN vorbehalten.

Inhalt

Seite

Europäisches Vorwort ... **4**

Einleitung ... **6**

1 Anwendungsbereich ... **7**
1.1 Allgemeines ... **7**
1.2 Außerhalb des Anwendungsbereichs ... **7**
1.3 Zielgruppe ... **8**

2 Normative Verweisungen ... **8**

3 Begriffe ... **8**

4 Symbole und Abkürzungen ... **10**

5 Beschreibung vertrauenswürdiger Systeme, die Serversignaturen unterstützen ... **11**
5.1 Allgemeines ... **11**
5.2 Ziele der Signaturerstellung und der Serversignatur ... **11**
5.3 An eine natürliche Person gebundene Signatur oder an eine juristische Person gebundenes Siegel ... **11**
5.4 Alleinige Kontrolle Sicherheitsniveaus ... **11**
5.5 Serversignaturen im Stapel ... **12**
5.6 Signierschlüssel und Verschlüsselungsmodul ... **12**
5.7 Authentifizierung des Unterzeichners ... **12**
5.7.1 Elektronische Identifizierungsmittel ... **12**
5.7.2 Authentifizierungsmechanismus ... **13**
5.7.3 Authentifizierungsziel ... **13**
5.7.4 Authentifizierungsübertragung an eine externe Partei ... **13**
5.8 Signatur-Aktivierungsdaten ... **14**
5.9 Signatur-Aktivierungsprotokoll ... **14**
5.10 Interaktionskomponente des Unterzeichners ... **15**
5.11 Signatur-Aktivierungsmodul ... **15**
5.12 Umgebungen ... **15**
5.12.1 Eingriffsgeschützte Umgebung ... **15**
5.12.2 TSP-geschützte Umgebung ... **16**
5.12.3 Umgebung des Unterzeichners ... **16**
5.13 Funktionsmodell ... **16**
5.13.1 Allgemeines ... **16**
5.13.2 Anwendungsbereich der Anforderungen ... **17**
5.13.3 Signatur-Aktivierungsmechanismus ... **18**
5.13.4 TW4S-Komponenten ... **20**

6 Sicherheitsanforderungen ... **20**
6.1 Allgemeines ... **20**
6.2 Allgemeine Sicherheitsanforderungen (SRG) ... **21**
6.2.1 Verwaltung (SRG_M) ... **21**
6.2.2 Systeme und Betriebsabläufe (SRG_SO) ... **22**
6.2.3 Identifizierung und Authentifizierung (SRG_IA) ... **22**
6.2.4 System-Zugriffskontrolle (SRG_SA) ... **23**
6.2.5 Schlüsselverwaltung (SRG_KM) ... **24**
6.2.6 Abrechnung und Prüfung (SRG_AA) ... **27**
6.2.7 Archivierung (SRG_AR) ... **28**

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

6.2.8 Backup und Wiederherstellung (SRG_BK) 29
6.3 Kernkomponenten-Sicherheitsanforderungen (SRC) 29
6.3.1 Signierschlüssel-Einrichtung (SRC_SKS) 29
6.3.2 Unterzeichner-Authentifizierung (SRC_SA) 30
6.3.3 Erstellung der digitalen Signatur (SRC_DSC) 30
6.4 Zusätzliche Sicherheitsanforderungen für SCAL2 (SRA) 31
6.4.1 Allgemeines 31
6.4.2 Signatur-Aktivierungsprotokoll und Signatur-Aktivierungsdaten (SRA_SAP) 31
6.4.3 Signierschlüsselverwaltung (SRA_SKM) 33

Literaturhinweise 35

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

Europäisches Vorwort

Dieses Dokument (prEN 419241-1:2017) 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 ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird CEN/TS 419241:2014 ersetzen.

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

Die erfolgreiche Umsetzung der Europäischen Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (in diesem Dokument als eIDAS [4] Verordnung bezeichnet) erfordert Standards für Dienste, Prozesse, Systeme und Produkte im Zusammenhang mit Vertrauensdiensten sowie eine Anleitung für die Konformitätsbewertung solcher Dienste, Prozesse, Systeme und Produkte.

Im Einklang mit dem Normungsmandat 460, das die Kommission CEN, CENELEC und ETSI für die Aktualisierung der existierenden eSignatur-Normungsprodukte erteilt hat, haben CEN und ETSI die eSignatur-Koordinierungsgruppe eingerichtet, um die für das Mandat 460 erreichten Aktivitäten zu koordinieren. Eine der ersten Arbeitsaufgaben war die Erstellung eines rationalisierten Rahmenwerks. In der zweiten Phase wurde eine Normenreihe bereitgestellt, um die in der eIDAS [4] Verordnung definierten Vertrauensdienste abzudecken.

Als Teil der europäischen Normenreihe ist dieses Dokument darauf ausgelegt, die Anforderungen der eIDAS [4] Verordnung an die Fernbenutzung einer Signaturerstellungseinheit zu erfüllen. Dies wird durch Sicherheitsanforderungen an ein serverseitiges System erreicht, das von einem Vertrauensdiensteanbieter verwaltete, private Signierschlüssel verwendet, um digitale Signaturen zu erstellen.

Der Zweck des vertrauenswürdigen Systems ist die Erstellung einer digitalen Signatur unter der alleinigen Kontrolle einer natürlichen Person oder unter der Kontrolle einer juristischen Person, die gemäß der Definition in der eIDAS [4] Verordnung in eine elektronische Signatur oder ein elektronisches Siegel integriert werden kann.

Diese Norm wird als EN 419 241-1 bezeichnet. Ein komplettes Rahmenwerk für die Normierung von Signaturen steht in TR 119 000.

Diese europäische Normenreihe umfasst die folgenden Teile:

— Teil 1: Allgemeine Systemsicherheitsanforderungen;

— Teil 2: QSCD-Schutzprofil für Serversignaturen.

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

Überarbeitungen

ÜBERARBEITUNG VOR DER FREIGABE, NUR FÜR DIE REDAKTIONELLE VERFOLGUNG. VOR DER FINALISIERUNG ENTFERNEN.

v0.0.0.a	23.04.14	Erstentwurf basierend auf CEN/TS 419241:2014
v0.0.0.b	18.06.14	zusätzliche Anforderungen an die Authentifizierung des Unterzeichners ausgerichtet auf ISO/IEC 29115:2013
v0.0.0.c	17.11.14	Arbeitsversion zur Definition von SAD und SAP
v0.0.0.d	16.12.14	ISO/IEC 29115:2013 entfernt, Einführung neuer PPs (PP-SAD, PP-TSCM).
v0.0.0.e/f	07.07.15	Ausarbeitung der Anforderungen nach SAD- und SAP-Definitionen.
v0.0.0.g	12.10.15	Arbeitsversion unter Berücksichtigung der Besprechung in La Ciotat.
v0.0.0.h	23.11.2015	Arbeitsversion unter Berücksichtigung der Kommentartabellen.
v0.0.0.i	11.12.2015	Arbeitsversion unter Berücksichtigung der Besprechung in Kochel.
v0.0.0.j	05.02.2016	Arbeitsversion unter Berücksichtigung der Kommentartabellen.
v0.0.0.k	17.02.2016	Arbeitsversion unter Berücksichtigung der Besprechung am 09.02.2016.
v0.0.0.l	23.03.2016	Arbeitsversion unter Berücksichtigung der Besprechung in Urbs.
v0.0.0.m	09.05.2016	Arbeitsversion unter Berücksichtigung der Audio-Besprechung im April.
v0.0.0.n	17.06.16	stabiler Entwurf von der Besprechung in Paris.
v0.0.0.o	25.10.16	Update von der Besprechung in Kopenhagen.
v0.0.0.p	09.11.16	Abstimmung mit (EU) 2015/1502.
v0.0.0.q	05.12.16	Anordnung von Kommentaren.
v0.0.0.r	08.12.16	Update von der Besprechung in Essen (Absendung zur CEN-Umfrage von WG17 genehmigt).

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop

Einleitung

Die Europäische Verordnung eIDAS schafft den Rechtsrahmen der Anforderungen für elektronische Signaturen. Diese Verordnung führt auch den Begriff der mit einer Fern-Signaturerstellungseinheit erstellten elektronischen Signaturen ein, um deren Verwendung angesichts ihrer zahlreichen wirtschaftlichen Vorteile und der leichten Bedienung zu steigern. Die eIDAS [4] Verordnung führt auch das Konzept des elektronischen Siegels ein, das ähnliche technische Eigenschaften wie die elektronischen Signaturen hat, aber mit einem geringeren Grad alleiniger Kontrolle. Sowohl die elektronischen Signaturen als auch die elektronischen Siegel nutzen auf asymmetrischer Kryptographie basierende Technologie, die gemeinhin als digitale Signatur bezeichnet wird.

Damit aber solche fernerstellten digitalen Signaturen genauso rechtlich anerkannt werden, wie in einer vollkommen benutzerverwalteten Umgebung erstellte digitale Signaturen (z. B. mit Smartcards), sollten Fernsignatur-Dienstleistungsanbieter besondere Management- und Verwaltungssicherheitsverfahren anwenden und zuverlässige Systeme und Produkte einschließlich sicherer elektronischer Kommunikationskanäle verwenden, um zu garantieren, dass die Serversignatur-Umgebung zuverlässig ist und die Signierschlüssel mit einer hohen Vertrauensstufe unter der alleinigen Kontrolle des Unterzeichners verwendet werden.

Das Hauptziel dieser Norm ist die Definition von Anforderungen und Empfehlungen für einen vernetzten Signaturserver, der von natürlichen oder juristischen Personen verwendete Signierschlüssel für die Erstellung von digitalen Signaturen verwalten kann.

Dieser Teil der europäischen Normenreihe legt die allgemeinen Anforderungen an Systeme für Serversignaturen fest. Es dürfen zusätzliche Spezifikationen (z. B. Schutzprofile) ausgegeben werden, die detailliertere Anforderungen für besondere Komponenten des Systems enthalten.

Es wird angenommen, dass der Signaturerstellungsdienste anbietende Vertrauensdiensteanbieter (en: Trust Service Provider, TSP) das vertrauenswürdige System in einer Umgebung betreibt, für die eine Sicherheitspolitik mit allgemeinen physischen, persönlichen, prozeduralen und dokumentarischen Sicherheitsanforderungen an die TSPs gilt, die Signaturerstellungsdienste anbieten.

Es wird empfohlen, z. B. ETSI EN 319 401 zu befolgen, um zu gewährleisten, dass die obigen Anforderungen erfüllt werden.

Es ist nicht die Absicht dieser Norm, die rechtliche Form der erstellten Signatur, ob elektronische Signatur oder elektronisches Siegel, ob qualifiziert oder nicht, zu begrenzen.

Korrespondenz und Kommentare zu diesen Sicherheitsanforderungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen, sollten gerichtet werden an:

Herausgeber: Franck Leroy

E-Mail: franck.leroy@docapost.fr

ILNAS-EN 419241-1:2018 - Preview only Copy via ILNAS e-Shop