

DIN EN 419241-1



ICS 35.030

Ersatz für
DIN CEN/TS 419241
(DIN SPEC 91126):2014-06

**Vertrauenswürdige Systeme, die Serversignaturen unterstützen –
Teil 1: Allgemeine Systemsicherheitsanforderungen;
Deutsche Fassung EN 419241-1:2018**

Trustworthy Systems Supporting Server Signing –
Part 1: General System Security Requirements;
German version EN 419241-1:2018

Systèmes fiables de Serveur de Signature électronique –
Partie 1: Exigences de sécurité générales du système;
Version allemande EN 419241-1:2018

Gesamtumfang 45 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419241-1:2018) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitsausschuss NA 043-01-17-04 UA „Austauschprotokolle bei Chip-Karten“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Änderungen

Gegenüber DIN CEN/TS 419241 (DIN SPEC 91126):2014-06 wurden folgende Änderungen vorgenommen:

- a) Überführung von DIN CEN/TS 419241 (DIN SPEC 91126) in eine DIN EN 419241-1;
- b) Aufnahme von Anforderungen aus Verordnung (EU) 910/2014 „eIDAS“, u. a. zum Thema Siegel;
- c) Erweiterung des Konzepts zur „alleinigen Kontrolle“;
- d) der Text wurde redaktionell überarbeitet.

Frühere Ausgaben

DIN CEN/TS 419241 (DIN SPEC 91126): 2014-06

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

Diese Europäische Norm wurde vom CEN am 30. April 2018 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-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. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem 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.



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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

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	13
5.7.1 Elektronische Identifizierungsmittel	13
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	16
5.12.1 Eingriffsgeschützte Umgebung	16
5.12.2 TSP-geschützte Umgebung	16
5.12.3 Umgebung des Unterzeichners	16
5.13 Funktionsmodell	17
5.13.1 Allgemeines.....	17
5.13.2 Anwendungsbereich der Anforderungen.....	17
5.13.3 Signatur-Aktivierungsmechanismus	18
5.13.4 TW4S-Komponenten	20
6 Sicherheitsanforderungen	21
6.1 Allgemeines.....	21
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)	23
6.2.4 System-Zugriffskontrolle (SRG_SA)	24
6.2.5 Schlüsselverwaltung (SRG_KM)	24
6.2.6 Prüfung (SRG_AA).....	27
6.2.7 Archivierung (SRG_AR).....	28

6.2.8	Backup und Wiederherstellung (SRG_BK)	29
6.3	Kernkomponenten-Sicherheitsanforderungen (SRC)	29
6.3.1	Signierschlüssel-Einrichtung (SRC_SKS) - Kryptografischer Schlüssel (SRC_SKS.1)	29
6.3.2	Unterzeichner-Authentifizierung (SRC_SA)	30
6.3.3	Erstellung der digitalen Signatur (SRC_DSC) - Verschlüsselungsvorgang (SRC_DSC.1)	30
6.4	Zusätzliche Sicherheitsanforderungen für SCAL2 (SRA)	30
6.4.1	Allgemeines	30
6.4.2	Signatur-Aktivierungsprotokoll und Signatur-Aktivierungsdaten (SRA_SAP)	31
6.4.3	Signierschlüsselverwaltung (SRA_SKM)	32
Anhang A (normativ) Anforderungen an elektronische Identifizierungsmittel, Merkmale und		
	Ausführung	34
A.1	Registrierung	34
A.1.1	Beantragung und Eintragung	34
A.1.2	Nachweis und Verifizierung der Identität (natürliche Person)	34
A.1.3	Nachweis und Verifizierung der Identität (juristische Person)	37
A.1.4	Verknüpfung von elektronischen Identifizierungsmitteln von natürlichen und juristischen Personen	39
A.2	Elektronische Identifizierungsmittel und Authentifizierung	40
A.2.1	Merkmale und Ausführung elektronischer Identifizierungsmittel	40
A.2.2	Authentifizierungsmechanismus	40
Literaturhinweise		42

Europäisches Vorwort

Dieses Dokument (EN 419241-1:2018) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2019, und etwaige entgegenstehende nationale Normen müssen bis Januar 2019 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt CEN/TS 419241:2014.

Dieses Dokument wurde unter einem Mandat erarbeitet, das 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 Normen 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 Mandat 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 Normung von Signaturen steht in ETSI TR 119 000.

Diese europäische Normenreihe besteht unter dem allgemeinen Titel „*Vertrauenswürdige Systeme, die Serversignaturen unterstützen*“ aus den folgenden Teilen:

- Teil 1: *Allgemeine Systemsicherheitsanforderungen*
- Teil 2: *Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung*

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: 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, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die Europäische Verordnung eIDAS schafft den Rechtsrahmen von 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, dass 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 sicherzustellen, dass die obigen Anforderungen erfüllt werden.

Diese Norm beabsichtigt nicht, 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:

Editor: Franck Leroy

E-Mail: franck.leroy@docapost.fr

1 Anwendungsbereich

1.1 Allgemeines

Dieses Dokument legt Sicherheitsanforderungen und Empfehlungen für Vertrauenswürdige Systeme, die Serversignaturen unterstützen (TW4S) und digitale Signaturen generieren, fest.

Das TW4S besteht aus mindestens einer Serversignaturanwendung (en: Server Signing Application, SSA) und einer Signaturerstellungseinheit (en: Signature Creation Device, SCDev) oder einer Fern-Signaturerstellungseinheit.

Eine Fern-SCDev ist eine SCDev, die um eine Fernsteuerung erweitert ist. Sie wird von einem Signatur-Aktivierungsmodul (en: Signature Activation Module, SAM) bereitgestellt, das in einer manipulationsgeschützten Umgebung ausgeführt wird. Dieses Modul benutzt die über ein Signatur-Aktivierungsprotokoll (en: Signature Activation Protocol, SAP) erfassten Signatur-Aktivierungsdaten (en: Signature Activation Data, SAD), um mit einer hohen Vertrauensstufe zu garantieren, dass die Signierschlüssel unter der alleinigen Kontrolle des Unterzeichners benutzt werden.

Die SSA benutzt eine SCDev oder eine Fern-SCDev, um die Signierschlüssel unter der alleinigen Kontrolle ihres berechtigten Unterzeichners zu generieren, zu halten und zu benutzen. Der Signierschlüsselimport aus den CAs liegt außerhalb des Anwendungsbereichs.

Deshalb kontrolliert der berechtigte Unterzeichner den Signierschlüssel mit einer hohen Vertrauensstufe aus der Ferne, wenn die SSA eine Fern-SCDev benutzt.

Ein TW4S soll dem Unterzeichner oder einer anderen Anwendung eine digitale Signatur liefern, die auf Grundlage der zu signierenden Daten erstellt wurde.

Diese Norm:

- enthält allgemein anerkannte Funktionsmodelle des TW4S;
- legt allgemeine Anforderungen fest, die für alle in den Funktionsmodellen identifizierten Dienste gelten;
- legt Sicherheitsanforderungen für alle im TW4S identifizierten Dienste fest;
- legt Sicherheitsanforderungen für vertrauliche Systemkomponenten fest, die vom TW4S benutzt werden können.

Diese Norm ist technologie- und protokollneutral und konzentriert sich auf Sicherheitsanforderungen.

1.2 Außerhalb des Anwendungsbereichs

Die folgenden Aspekte werden als außerhalb des Anwendungsbereichs dieses Dokuments liegend angesehen:

- andere vertrauenswürdige Dienste, die zusammen mit diesem Dienst benutzt werden dürfen, wie z. B. Zertifikatausstellung, Signaturprüfdienst, Zeitstempeldienst und Informationserhaltungsdienst;
- Anwendungen oder Systeme außerhalb des TW4S (insbesondere die Signaturerstellungsanwendung einschließlich der Erstellung fortgeschrittener Signaturformate);
- Signierschlüssel- und Signierzertifikat-Import aus den CAs;
- die rechtliche Auslegung der Signaturform (z. B. elektronische Signatur, elektronisches Siegel, qualifiziert oder nicht).

1.3 Zielgruppe

Diese Norm legt Sicherheitsanforderungen fest, die befolgt werden sollen von:

- Anbietern von TW4S-Systemen;
- Vertrauensdiensteanbieter (TSP), die einen Signaturerstellungsdienst anbieten.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 15408 (alle Teile), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

FIPS PUB 140-2, *Security requirements for cryptographic modules*

3 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe.

ISO und IEC verwalten Begriffsdatenbanken für die Verwendung in der Normung unter folgenden Adressen:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

Authentifizierung

Zuverlässigkeitsgewähr bezüglich der Identität einer Einheit

[QUELLE: ISO/IEC 18014-2:2009]

3.2

Authentifizierungsfaktor

Information und/oder Prozess zum Authentifizieren oder Überprüfen der Identität einer Einheit

[QUELLE: ISO/IEC 19790:2012]

3.3

zu signierende Daten oder deren eindeutige Darstellung

formatierte Daten, mit denen der Wert der digitalen Signatur berechnet wird (z. B. Hashwert)

[QUELLE: ETSI/TR 119 001:2016]

3.4

digitale Signatur

an eine Dateneinheit angefügte Daten oder eine kryptografische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung z. B. durch den Empfänger bietet

[QUELLE: ETSI TR 119 001:2016]

3.5**eIDAS Verordnung**

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

3.6**Fern-Signaturerstellungseinheit**

aus der Perspektive des Unterzeichners fernbenutzte Signaturerstellungseinheit, welche das Signatur-Aktivierungsprotokoll anwendet, um Kontrolle über den Signiervorgang in ihrem Auftrag zu haben und mit einer hohen Vertrauensstufe garantiert, dass die Signierschlüssel unter der alleinigen Kontrolle des Unterzeichners benutzt werden

3.7**Signatur-Aktivierungsdaten**

vom SAP erfasster Datensatz, mit dem mit hoher Vertrauensstufe ein bestimmter Signaturvorgang kontrolliert wird, der im Auftrag des Unterzeichners von einem Verschlüsselungsmodul durchgeführt wird, das unter alleiniger Kontrolle des Unterzeichners steht

Anmerkung 1 zum Begriff: Die SAD können das Ergebnis von Verschlüsselungsvorgängen sein (siehe Details in 5.8).

3.8**Signatur-Aktivierungsmodul**

konfigurierte Software, die die SAD benutzt, um mit einer hohen Vertrauensstufe zu garantieren, dass die Signierschlüssel unter der alleinigen Kontrolle des Unterzeichners benutzt werden

3.9**Signatur-Aktivierungsprotokoll**

Protokoll, das mithilfe des Signierschlüssels des Unterzeichners die SAD erfasst, mit denen ein Signaturvorgang an einem DTBS/R (Satz) kontrolliert wird

3.10**Signaturerstellungsanwendung**

Anwendung, die mit der von einer SCDev generierten digitalen Signatur ein signiertes Dokument erstellt

3.11**Signaturerstellungseinheit**

konfiguriertes Software- und/oder Hardware-Verschlüsselungsmodul zum Erstellen einer digitalen Signatur

3.12**Signaturpolitik**

Signaturerstellungspolitik, Signaturerhöhungspolitik, Signaturprüfpolitik oder eine Kombination daraus, die auf dieselbe Signatur oder denselben Signatursatz anwendbar ist

[QUELLE: ETSI/TS 119 001:2016]

3.13**Unterzeichner**

Einheit (natürliche oder juristische Person), die der Erzeuger einer digitalen Signatur ist

[QUELLE: ETSI/TR 119 001:2016]

3.14**Interaktionskomponente des Unterzeichners**

Software- und/oder Hardware-Komponente, mit der der Unterzeichner das SAP unterstützt

3.15**Signierschlüssel**

privater Schlüssel eines asymmetrischen kryptografischen Schlüsselpaares, mit dem eine digitale Signatur erstellt wird

3.16**Vertrauensdiensteanbieter**

natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste bereitstellt

[QUELLE: ETSI/TS 119 001:2016]

3.17**vertrauenswürdige System, das Serversignaturen unterstützt**

Client-Server-System, das Signierschlüssel unter der Kontrolle des Unterzeichners verwendet, um digitale Signaturen zu erstellen

4 Symbole und Abkürzungen

CA	Zertifizierungsstelle
CC	Common Criteria, ISO/IEC 15408, Evaluationskriterien für IT-Sicherheit
CEN	Europäisches Komitee für Normung
DTBS/R	zu signierende Daten oder deren eindeutige Darstellung
EAL	Vertrauenswürdighkeitsstufe
ETSI	Europäisches Institut für Telekommunikationsnormen
ISO/IEC	Internationale Normungsorganisation/Internationale Elektrotechnische Kommission
ISSS	Normungssystem für die Informationsgesellschaft
QSCD	Einheit zur Erstellung einer qualifizierten elektronischen Signatur (oder eines elektronischen Siegel) wie in der eIDAS Verordnung definiert
RA	Registrierungsstelle
SAD	Signatur-Aktivierungsdaten
SAM	Signatur-Aktivierungsmodul
SAP	Signatur-Aktivierungsprotokoll
SCA	Signaturerstellungsanwendung
SCAL	Alleinige Kontrolle Sicherheitsniveau
SCDev	Signaturerstellungseinheit
SIC	Interaktionskomponente des Unterzeichners
SSA	Serversignaturanwendung
TSP	Vertrauensdiensteanbieter
TW4S	Vertrauenswürdige System, das Serversignaturen unterstützt

5 Beschreibung vertrauenswürdiger Systeme, die Serversignaturen unterstützen

5.1 Allgemeines

Dieser Abschnitt beschreibt die verschiedenen Serversignatur-Konzepte, um zu klären, wie die Sicherheitsanforderungen aus Abschnitt 6 umgesetzt werden sollten.

Alle Anforderungen dieser Norm sind deutlich angegeben und können sein:

- obligatorisch (angegeben durch MUSS [DARF NICHT]);
- optional (angegeben durch SOLLTE [SOLLTE NICHT]);
- zulässig (angegeben durch DARF [NICHT]).

5.2 Ziele der Signaturerstellung und der Serversignatur

Zweck des TW4S ist die Erstellung einer digitalen Signatur unter Unterzeichnerkontrolle mithilfe zu signierender Daten oder deren eindeutiger Darstellung (DTBS/R).

5.3 An eine natürliche Person gebundene Signatur oder an eine juristische Person gebundenes Siegel

Mit der digitalen Signatur kann eine elektronische Signatur oder ein elektronisches Siegel dargestellt werden.

In diesen beiden Fällen ist nicht unbedingt dieselbe Vertrauensstufe bei der Signierschlüsselkontrolle zu erwarten.

Die in Übereinstimmung mit dieser Norm erstellte digitale Signatur kann unter Kontrolle einer natürlichen oder juristischen Person erstellt werden.

Zur besseren Übersichtlichkeit umfasst der Begriff Unterzeichner in dieser Norm sowohl natürliche als auch juristische Personen.

Zur besseren Übersichtlichkeit umfasst der Begriff SCDev in dieser Norm sowohl Signatur- als auch Siegelerstellungseinheiten.

5.4 Alleinige Kontrolle Sicherheitsniveaus

Im vorliegenden Dokument werden zwei Sicherheitsniveaus für die alleinige Kontrolle festgelegt:

- Alleinige Kontrolle Sicherheitsniveau 1 (SCAL1):
 - Die Signierschlüssel werden mit einer niedrigen Vertrauensstufe unter der alleinigen Kontrolle des Unterzeichners benutzt.
 - Dem berechtigten Unterzeichner wird die Benutzung des Schlüssels für die Signatur von der SSA, die den Unterzeichner authentifiziert, aufgezwungen.

ANMERKUNG 1 Es wird nicht erwartet, dass solche Implementierungen die Anforderungen der alleinigen Kontrolle erfüllen, so wie dies von einer Stand-Alone-QSCD, wie in der eIDAS [4] Verordnung definiert, erwartet wird.

- Alleinige Kontrolle Sicherheitsniveau 2 (SCAL2):
 - Die Signierschlüssel werden mit einer hohen Vertrauensstufe unter der alleinigen Kontrolle des Unterzeichners benutzt.
 - Dem berechtigten Unterzeichner wird die Benutzung des Schlüssels für die Signatur vom SAM mithilfe der SAD aufgezwungen, die der Unterzeichner durch die Benutzung des SAP bereitstellt, um die Benutzung des entsprechenden Signierschlüssels zu ermöglichen.

ANMERKUNG 2 Das Protokoll soll dasselbe Alleinige Kontrolle Sicherheitsniveau erreichen, das mit einer Stand-Alone-QSCD, wie in der eIDAS [4] Verordnung definiert, erreicht werden würde.

Die Entscheidung, ob das Alleinige Kontrolle Sicherheitsniveau 1 oder 2 verwendet werden soll, hängt von der Signaturpolitik und den anwendbaren gesetzlichen Bestimmungen ab.

5.5 Serversignaturen im Stapel

In einigen EU-Mitgliedstaaten kann ein Dokumentenstapel signiert werden, ohne dass der Unterzeichner jedes Dokument prüfen und ausdrücklich genehmigen muss, oder eine Gelegenheit zur Prüfung dieser vor dem Signieren hat, zum Beispiel durch Verknüpfungen zu den Dokumenten im Stapel, anstatt jedes Dokument für die Prüfung und Genehmigung zu übergeben.

Dies bedeutet, dass der Unterzeichner nur alleinige Kontrollen auf den Signierprozess eines Stapels anzuwenden braucht, und nicht auf jedes einzelne Dokument.

Einige EU-Mitgliedstaaten lassen Stapelsignaturen nicht zu. In diesem Fall ist sicherzustellen, ob dieses Verbot uneingeschränkt für alle Arten fortgeschrittener elektronischer Signaturen gilt, oder nur für qualifizierte.

Da die rechtliche Zulässigkeit von Stapelsignaturen von der Rechts- und Anwendungsumgebung abhängt, SOLLTE das TW4S Konfigurationsprofile haben, welche digitale Signaturen im Stapel zulassen bzw. nicht zulassen.

5.6 Signierschlüssel und Verschlüsselungsmodul

Zum Generieren einer digitalen Signatur auf SCAL1 und zum Garantieren hoher Flexibilität muss der Signierschlüssel (z. B. privater Schlüssel eines asymmetrischen Schlüsselpaares) nicht unbedingt in einem Verschlüsselungsmodul (z. B. Hardware-Sicherheitseinheit oder Smartcard) generiert, gespeichert und verwendet werden. Der Signierschlüssel könnte auch in einer Datei gespeichert werden, und die SCDev kann Software sein, die diese Datei benutzt.

Beim Benutzen von Dateien SOLLTEN zusätzlich zum Schutz der Dateien selbst vor Eingriffen (Löschung, Änderung) spezielle externe Sicherheitsmaßnahmen implementiert werden.

Dennoch empfiehlt diese Norm, dass das TW4S durch eine eingriffsgeschützte Umgebung geschützte Signierschlüssel benutzt, um digitale Signaturen zu erstellen. Das heißt, die SCDev SOLLTE ein Verschlüsselungsmodul sein (z. B. Hardware-Sicherheitseinheiten nach Normenreihe EN 419211 oder Normenreihe CEN/TS 419221).