

DIN EN 419241-1

ICS 35.030

Entwurf

Einsprüche bis 2017-06-07
 Vorgesehen als Ersatz für
 DIN CEN/TS 419241
 (DIN SPEC 91126):2014-06

**Vertrauenswürdige Systeme, die Serversignaturen unterstützen –
 Teil 1: Allgemeine Systemsicherheitsanforderungen;
 Deutsche und Englische Fassung prEN 419241-1:2017**

Trustworthy Systems Supporting Server Signing –
 Part 1: General System Security Requirements;
 German and English version prEN 419241-1:2017

Systèmes fiables de Serveur de Signature électronique –
 Partie 1: Exigences de sécurité générales du système;
 Version allemande et anglaise prEN 419241-1:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-04-07 wird der Öffentlichkeit zur Prüfung und
 Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
 besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-
 Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
 sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
 Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
 Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

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

Gesamtumfang 71 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales 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 (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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der prEN 419241-1 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm- Entwurfes gelten gleichermaßen auch für den englischen Text.

Änderungen

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

- a) Überführung des DIN CEN/TS 419241 (DIN SPEC 91126) in eine DIN EN 419241-1 und DIN EN 419241-2;
- b) Aufnahme von Anforderungen aus EU Verordnung 910/2014 „eIDAS“, u.a. zum Thema Siegel;
- c) Erweiterung des Konzepts zur „alleinigen Kontrolle“;
- d) Definition eines Schutzprofils in Teil 2;
- e) der Text wurde redaktionell überarbeitet.

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

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm

Dokument-Untertyp:

Dokument-Stage: CEN-Umfrage

Dokument-Sprache: D

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

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

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 [6] 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 [6] Verordnung definierten Vertrauensdienste abzudecken.

Als Teil der europäischen Normenreihe ist dieses Dokument darauf ausgelegt, die Anforderungen der eIDAS [6] 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 [6] 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.

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).

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 [6] 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

1 Anwendungsbereich

1.1 Allgemeines

Diese Norm 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 Fernbedienung erweitert ist. Sie wird von einem Signatur-Aktivierungsmodul (en: Signature Activation Module, SAM) bereitgestellt, das in einer eingriffsgeschützten 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 fernkontrolliert der berechtigte Unterzeichner den Signierschlüssel mit einer hohen Vertrauensstufe, 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 liegend angesehen:

- andere vertrauenswürdige Dienste, die zusammen mit diesem Dienst benutzt werden dürfen, wie z. B. Zertifikatausstellung, Signaturprüfungsdienst, Zeitstempelungsdienst 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, die in dieser Norm teilweise oder als Ganzes zitiert werden, sind für ihre Anwendung erforderlich. 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 (Teile 1 bis 3): *Information technology — Security techniques — Evaluation criteria for IT security*

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

3 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe.

3.1

Authentifizierung

Zuverlässigkeitsgewähr bezüglich der Identität einer Einheit

[QUELLE: ISO/IEC 18014-2]

3.2

Authentifizierungsfaktor

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

[QUELLE: ISO/IEC 19790]

3.3

zu signierende Daten oder deren eindeutige Darstellung

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

3.4

digitale Signatur

an Daten angehängte Daten oder die verschlüsselte Umwandlung von Daten, die es dem Empfänger der Daten ermöglicht, sich der Quelle und der Integrität der Daten zu vergewissern, und die gegen Betrug z. B. durch den Empfänger schützen

[QUELLE: ETSI TR 119 001]

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. Sie garantiert mit einer hohen Vertrauensstufe, dass die Signierschlüssel unter der alleinigen Kontrolle des Unterzeichners benutzt werden.

3.7

Unterzeichner

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

[QUELLE: ETSI TR 119 001]

3.8

Interaktionskomponente des Unterzeichners

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

3.9

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).

3.10

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.

3.11

Signatur-Aktivierungsprotokoll

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

3.12

Signaturerstellungsanwendung

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

3.13

Signierschlüssel

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

3.14

Signaturerstellungseinheit

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

3.15

Signaturpolitik

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

[QUELLE: ETSI TS 119 001]

3.16

Vertrauensdiensteanbieter

natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste bereitstellt

[QUELLE: ETSI TS 119 001]

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

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	Vertrauenswürdigkeitsstufe
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 Anforderungen des nächsten Abschnitts 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 (DARF oder BRAUCHT [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 auferlegt, die den Unterzeichner authentifiziert.

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 [6] 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 auferlegt, 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 [6] 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-Mitgliedsstaaten kann ein Dokumentenstapel signiert werden, ohne dass der Unterzeichner jedes Dokument prüfen und ausdrücklich genehmigen muss, oder er bekommt eine Gelegenheit zur Prüfung vor dem Signieren zum Beispiel durch Verknüpfungen zu den Dokumenten im Stapel.

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

Einige EU-Mitgliedsstaaten 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 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 zu 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 EN 419211 oder EN 419221).

5.7 Authentifizierung des Unterzeichners

5.7.1 Elektronische Identifizierungsmittel

5.7.1.1 SCAL1

Die Registrierung des Unterzeichners sowie die Merkmale und Anforderungen an die Ausführung der elektronischen Identifizierungsmittel werden in **SRC_SA.1.1** definiert.

5.7.1.2 SCAL2

Die Registrierung des Unterzeichners sowie die Merkmale und Anforderungen an die Ausführung der elektronischen Identifizierungsmittel werden in **SRA_SAP.1.1** definiert.

5.7.2 Authentifizierungsmechanismus

5.7.2.1 SCAL1

Die Anforderungen an den Authentifizierungsmechanismus werden in **SRC_SA.1.1** definiert.

5.7.2.2 SCAL2

Die Anforderungen an den Authentifizierungsmechanismus werden in **SRA_SAP.1.1** definiert.

5.7.3 Authentifizierungsziel

5.7.3.1 SCAL1

- Der Unterzeichner MUSS erfolgreich in der SSA authentifiziert werden, damit er Zugriff auf den Signaturvorgang bekommt, und
- Der Signierschlüssel des Unterzeichners MUSS durch die SSA mit dem Authentifizierungsfaktor des Unterzeichners verknüpft werden.

5.7.3.2 SCAL2

- Die SAD MÜSSEN eingerichtet oder berechnet werden oder das Ergebnis einer abgesicherten Interaktion zwischen dem SAM und der SIC über die SSA sein, um den Signiervorgang in der SCDev zu genehmigen, und
- Die SAD MÜSSEN über die SSA an das SAM übertragen werden, um den Signiervorgang in der SCDev für einen eigenen DTBS/R zu genehmigen.

5.7.4 Authentifizierungsübertragung an eine externe Partei

Der TSP DARF den Authentifizierungsprozess an eine externe Partei übertragen (z. B. an einen Identitätsanbieter).

5.7.4.1 SCAL1

Der TSP MUSS sicherstellen, dass der an die externe Partei übertragene Authentifizierungsprozess die Anforderungen nach **SRC_SA.1.1** erfüllt.

ANMERKUNG Wenn die externe Partei elektronische Identifizierungsmittel benutzt, welche nach einer angemeldeten Regelung ausgestellt wurden, die in der von der Kommission nach Artikel 9 der eIDAS [6] Verordnung veröffentlichten Liste stehen, braucht die Konformität mit der erforderlichen Stufe nicht nachgewiesen zu werden. Die Konformität mit den gesetzlichen Vorschriften kann angenommen werden.

5.7.4.2 SCAL2

Der TSP MUSS sicherstellen, dass der an die externe Partei übertragene Authentifizierungsprozess die Anforderungen nach **SRA_SAP.1.1** erfüllt.

Der TSP MUSS sicherstellen, dass;

- die externe Partei alle relevanten Anforderungen dieser Norm und die Anforderungen für die Registrierung nach der eIDAS [6] Verordnung erfüllt oder
- der an die externe Partei übertragene Authentifizierungsprozess elektronische Identifizierungsmittel benutzt, welche nach einer angemeldeten Regelung ausgestellt wurden, die in der von der Kommission nach Artikel 9 der eIDAS [6] Verordnung veröffentlichten Liste stehen.

5.8 Signatur-Aktivierungsdaten

Zum Erreichen der SCAL2 MUSS das SAM die Benutzung der SAD zur Sicherstellung der Kontrolle über den Schlüssel des Unterzeichners auferlegen.

Die Signatur-Aktivierung auf SCAL2 erfordert die Erfüllung mehrerer Bedingungen wie die Authentifizierung des Unterzeichners und die Authentizität der Signaturvorgangsanforderung des Unterzeichners (Einzelheiten sind in 5.7 angegeben).

Beide Eigenschaften DÜRFEN direkt von den SAD erfüllt werden. Es ist jedoch auch möglich, die Authentifizierung des Unterzeichners z. B. durch eine übertragene Authentifizierung vor der Generierung der SAD auszuführen.

Die SAD können ein Datensatz oder das Ergebnis von Verschlüsselungsvorgängen sein (Einzelheiten sind in **SRA_SAP.2** angegeben), von denen dieselben Informationen abgeleitet werden können.

Die SAD tragen zur direkten oder indirekten Authentifizierung des Unterzeichners bei.

Wenn die Authentifizierung des Unterzeichners vor der Erfassung der SAD stattfindet, MÜSSEN die SAD von einer bekannten Quelle bestätigte Elemente zum Identifizieren des Unterzeichners enthalten. Diese Bestätigung DARF entweder von der Interaktionskomponente des Unterzeichners (SIC) oder von einem vertrauenswürdigen Anbieter von elektronischen Identitäten kommen. Die Quelle der Bestätigung MUSS authentifiziert sein.

5.9 Signatur-Aktivierungsprotokoll

Das SAP MUSS so konzipiert sein, dass eine sichere Benutzung des Signierschlüssels für die Erstellung einer digitalen Signatur durch das Verschlüsselungsmodul im Auftrag eines Unterzeichners möglich ist.

Das SAP ist ein Protokoll, bei dem der Unterzeichner (über die SIC) und das TW4S kommunizieren, um die SAD zu generieren.

Das SAP MUSS so ausgelegt sein, dass es mindestens die folgenden Verifizierungen umfasst:

- Authentifizierung des Unterzeichners, wenn der Signierschlüssel benutzt wird,
- Authentizität der Signaturanforderung mit besonderen SAD,
- Der ausgewählte Signierschlüssel ist gültig und aktiv,
- Sichere Übertragung aller Elemente der SAD.

Das SAP SOLLTE die folgende Verifizierung umfassen:

- Vorhandensein eines gültigen, mit dem Signierschlüssel verbundenen Zertifikats.

ANMERKUNG Diese Empfehlung ist nicht anwendbar, wenn der Signierschlüssel zum Signieren eines Besitznachweises benutzt wird, um ein Zertifikat zu erhalten.

5.10 Interaktionskomponente des Unterzeichners

Die Interaktionskomponente des Unterzeichners (SIC) ist eine Software und/oder Hardware, die auf der Umgebung des Unterzeichners unter seiner alleinigen Kontrolle betrieben wird.

Die Benutzung dieser Komponente ist wesentlich im SAP-Prozess und für die Erstellung einer digitalen Signatur durch die SCDev.

Die SIC nimmt immer am SAP teil, um den Unterzeichner zu authentifizieren oder die SAD zu generieren:

- die SIC kann die SAD direkt generieren oder
- die SIC kann zum Authentifizieren des Unterzeichners benutzt werden, und die Bestätigung, die den Unterzeichner identifiziert, wird in der SAD-Generierung benutzt.

Diese Komponente kann zum Beispiel folgendes sein (Kombinationen sind möglich):

- eine von einem Browser ausgeführte Applikation (z. B. eine Form von HTTP POST über TLS),
- eine von einem Mobilgerät ausgeführte Applikation (z. B. Smartphone, Tablet),
- ein sicheres Element eines Handys (z. B. SIM-Karte, die SMS empfängt),
- eine Verschlüsselungseinheit des Unterzeichners (z. B. eID, eToken, FIDO-Token),
- [...].

Die SIC erlegt die Verknüpfung zwischen dem Unterzeichner und dem Signaturvorgang innerhalb des SAP auf

5.11 Signatur-Aktivierungsmodul

Das SAM ist eine Software, die die SAD benutzt, um mit einer hohen Vertrauensstufe zu garantieren, dass die Signierschlüssel unter der alleinigen Kontrolle des Unterzeichners für SCAL2 benutzt werden.

Das SAM erfordert die Benutzung in einer eingriffsgeschützten Umgebung.

Wenn das SAM nicht in derselben eingriffsgeschützten Umgebung wie die SCDev benutzt wird, ist ein sicherer Kanal zwischen den beiden eingriffsgeschützten Umgebungen erforderlich.

5.12 Umgebungen

Es sind drei verschiedene Umgebungen definiert.

5.12.1 Eingriffsgeschützte Umgebung

Die eingriffsgeschützte Umgebung wird in der TSP-geschützten Umgebung betrieben und gegen direkten Internetzugriff abgeschirmt. Sie gewährleistet die Integrität des Codes, der innerhalb dieser Umgebung ausgeführt wird.

Der Code schützt die Benutzung von Signierschlüsseln und erlegt die Signatur-Aktivierung unter Unterzeichnerkontrolle auf.

Die eingriffsgeschützte Umgebung schützt auch die Verknüpfung(en) zwischen dem(den) Signierschlüssel(n) und dem(den) Unterzeichner(n) (Verknüpfung wird erstellt und geprüft, wenn für eine Signaturerstellung gebraucht).

Für SCAL1 wird es empfohlen, private oder geheime Schlüssel in einer eingriffsgeschützten Umgebung zu generieren und zu benutzen.

Für SCAL2 ist es erforderlich, private oder geheime Schlüssel in einer eingriffsgeschützten Umgebung zu generieren und zu benutzen. Zusätzlich erfordert die Software des SAM die Benutzung in einer eingriffsgeschützten Umgebung.

5.12.2 TSP-geschützte Umgebung

Die TSP-geschützte Umgebung wird nach den Anforderungen an den sicheren Betrieb des Serversignatursystems geprüft.

Sie schützt gegen Angriffe aus dem Internet und verarbeitet Internetverbindungen zu/von den externen Umgebungen (z. B. Unterzeichner, SCA, RA).

Diese Umgebung kann in geschützter Form den(die) Signierschlüssel und die Verknüpfung(en) zwischen dem(den) Schlüssel(n) und dem(den) Unterzeichner(n) speichern.

Der TSP schützt diese Umgebung, um die SAD- und SAP-Anforderungen zu erfüllen und der RA-Umgebung Verpflichtungen (hinsichtlich der Registrierung) aufzuerlegen. Spezifikationen werden zum Beispiel in EN 319411-1, 6.2.2 und EN 319411-2, 6.2.2 angegeben.

Sie sollte auch die Anforderungen für die Zertifikatregistrierung erfüllen, um die alleinige Kontrolle nachzuweisen (von der RA benötigt). Diese Anforderungen werden zum Beispiel in EN 319411-1, 6.3.1.a und 6.3.3.d. festgelegt.

5.12.3 Umgebung des Unterzeichners

Sie ist die lokale Umgebung des Unterzeichners.

Der Unterzeichner ist verantwortlich für den Schutz seiner Umgebung. Wenn der Unterzeichner die Umgebung Dritter benutzt, ist der Dritte verantwortlich für den Schutz der Umgebung des Unterzeichners.

Die allgemeinen Elemente der Umgebung des Unterzeichners dürfen benutzt werden, um das zu signierende Dokument vorzubereiten und die Dokumentensignatur sowie die SIC zu formatieren.

Eine SIC wird vom Unterzeichner verwendet, um eine Verknüpfung zwischen dem Unterzeichner und dem gesamten, durch das SAP aktivierten Signaturvorgang zu erstellen.

Es gibt keine direkte Zertifizierungsanforderung an die SIC im Hinblick auf diese Norm. Bei dem Entwurf und der Implementierung der SIC müssen jedoch Anforderungen an die Übertragung/Berechnung der SAD und die Interaktion der SIC mit dem SAM über das SAP berücksichtigt werden, einschließlich der Authentifizierung des Unterzeichners.

5.13 Funktionsmodell

5.13.1 Allgemeines

Dieser Abschnitt stellt die konzeptionelle Architektur eines TW4S dar, um seine Anwendungsbereiche, seine Komponenten und seine Aktivierungsmechanismen zu präsentieren.

Er präsentiert keine physische Architektur, die in der Praxis zum Beispiel mehrere Server und Geräte für die Lastverteilung oder Redundanz umfassen würde.

Die Umgebung des Unterzeichners ist dem TW4S unbekannt. Es sollte z. B. durch das alleinige Installieren vertrauenswürdiger Software und die Benutzung eines Schutzes gegen Schadprogramme geschützt werden.

Der TSP, der die Signaturerstellungsdienste anbietet, schützt die Umgebung des TW4S. Das TW4S wird mit einer Sicherheitspolitik betrieben, die allgemeine physische, persönliche, prozedurale und dokumentarische Sicherheitsanforderungen umfasst, sowie spezifische Anforderungen an TSPs, die Signaturerstellungsdienste anbieten.

Eine Definition der Anforderungen steht zum Beispiel in ETSI EN 319 401.

Für SCAL2 werden der(die) Signierschlüssel und das SAM durch eine eingriffsgeschützte Umgebung geschützt (z. B. Verschlüsselungsmodul nach EN 419211 oder EN 419221).

5.13.2 Anwendungsbereich der Anforderungen

Ein TW4S gewährleistet eine sichere Fernverwaltung des Unterzeichner-Signierschlüssels und die Erstellung von digitalen Signaturen durch solch einen fernverwalteten Signierschlüssel.

Diese Norm schränkt nicht ein, wie die Server- und Unterzeichnersysteme auf eine oder mehrere Komponenten aufgeteilt werden DÜRFEN. Die Signaturerstellungsanwendung (SCA) liegt außerhalb des Anwendungsbereichs dieser Norm und Anforderungen an vertrauenswürdige Systeme für TSP in Bezug auf die Zertifikatsausstellung liegen außerhalb des Anwendungsbereichs (siehe CEN/TS 419261).

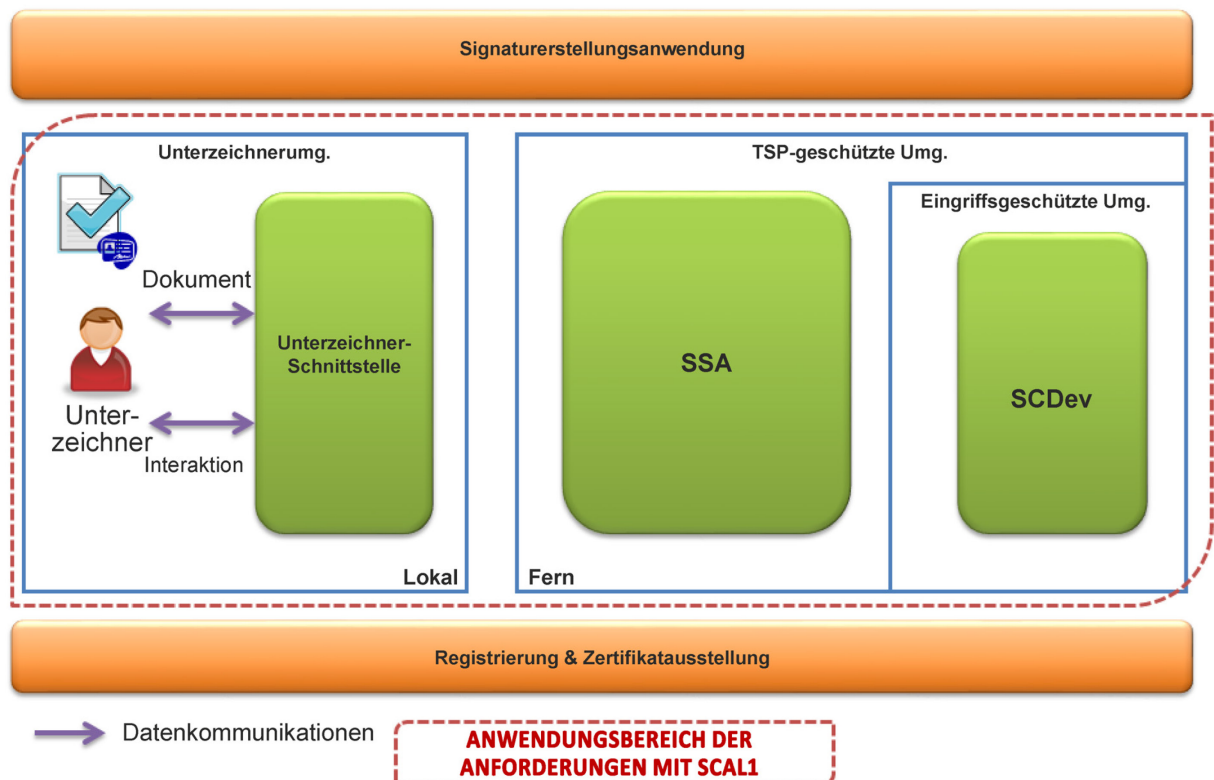


Bild 1 — Anwendungsbereich der Anforderungen

ANMERKUNG Der Anwendungsbereich der Anforderungen kann auf eine externe Partei ausgeweitet werden, wenn die Authentifizierungsübertragung verwendet wird (siehe 5.7.4).

5.13.3 Signatur-Aktivierungsmechanismus

5.13.3.1 Allgemeines

In diesem Abschnitt werden einige Modelle für die Signatur-Aktivierung zum Erstellen einer digitalen Signatur vorgeschlagen. Es DARF eine andere Architektur implementiert werden, die Abschnitt 6 entspricht.

Das TW4S wird normalerweise von einer Unterzeichnergruppe benutzt, wobei jeder Unterzeichner einen oder mehrere Signierschlüssel besitzt, und das TW4S kann eine oder mehrere SCDev umfassen, um Signaturvorgänge auszuführen.

Der Signierschlüssel kann sicher außerhalb der SCDev gespeichert und dynamisch geladen werden, vorausgesetzt, dass es Kontrollen gibt, welche die gleiche Sicherheit auf dem Signierschlüssel gewährleisten. Lade-/Entlademechanismen für Schlüssel, die zum Schützen von Signierschlüsseln benutzt werden müssen, liegen außerhalb des Anwendungsbereichs dieser Norm.

5.13.3.2 Signatur-Aktivierung für SCAL1

Die Vertraulichkeit und Integrität des Signierschlüssels werden von der SCDev gewährleistet. Die SCDev kann über die SSA aktiviert werden. Die Aktivierung kann für einen bestimmten Zeitraum und/oder für eine bestimmte Signaturanahl aufrechterhalten werden.

Für die Aktivierung des Signierschlüssels muss der Unterzeichner von der SSA authentifiziert worden sein. Wenn die Authentifizierung des Unterzeichners erfolgreich ist, DARF der entsprechende Signierschlüssel für den Signaturvorgang im Auftrag des Unterzeichners innerhalb eines bestimmten Zeitrahmens und/oder einer bestimmten Anzahl Signaturvorgängen benutzt werden. Dadurch kann die SSA für Massen-/Stapel-signaturzwecke benutzt werden.

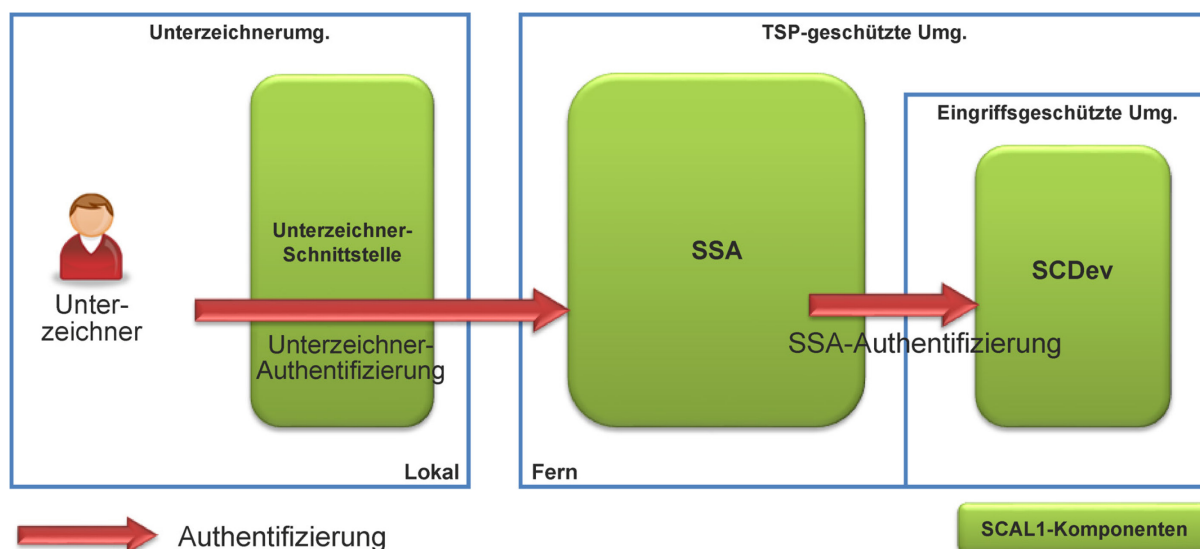


Bild 2 — Signatur-Aktivierungssystem mit SCAL1

ANMERKUNG Diese Architektur kann auf eine externe Partei ausgeweitet werden, wenn die Authentifizierungsübertragung verwendet wird (siehe 5.7.4).

Diese Architektur kann zum Erstellen eines Wertes (z. B. hashverschlüsselt mit dem privaten Schlüssel des Unterzeichners) der digitalen Signatur mit niedriger Gewährleistung der Kontrolle benutzt werden.

5.13.3.3 Signatur-Aktivierung für SCAL2

Die Vertraulichkeit und Integrität des Signierschlüssels werden von der Fern-SCDev gewährleistet.

Die Fern-SCDev wird von der SSA kontrolliert.

Die Fern-SCDev nimmt am SAP teil und gewährleistet, dass der Signaturvorgang unter der legitimen Kontrolle des Unterzeichners steht.

Die SSA stellt über einen sicheren Kanal eine Schnittstelle zum SAM der Fern-SCDev her, die die SAD überprüft, um den entsprechenden Signierschlüssel zu aktivieren.

Die Authentifizierung des Unterzeichners kann für einen bestimmten Zeitraum und/oder für eine bestimmte Signaturanahl aufrechterhalten werden. Aber die SAD-Berechnung MUSS für jeden Signaturvorgang ausgeführt werden. Die SAD DÜRFEN mit einem DTBS/R Satz verknüpft werden. Dadurch kann die SSA für Massen-/Stapelsignaturzwecke benutzt werden.

Die Authentifizierung des Unterzeichners kann mit einer Interaktionskomponente des Unterzeichners (SIC) erfolgen, die eine Verknüpfung zwischen dem Unterzeichner und der Signatur als Teil der SAD erstellt.

Die Verwendung der SAD erfolgt unter der Verantwortung des SAM:

- Wenn die SAD von der SIC generiert werden, MÜSSEN sie zur Verifizierung sicher von der SIC zum SAM übertragen werden.
- Wenn die SAD nicht von der SIC generiert werden, MÜSSEN sie bei/während einer erfolgreichen Authentifizierung des Unterzeichners mit der SIC generiert und zur Verifizierung sicher zum SAM übertragen werden.

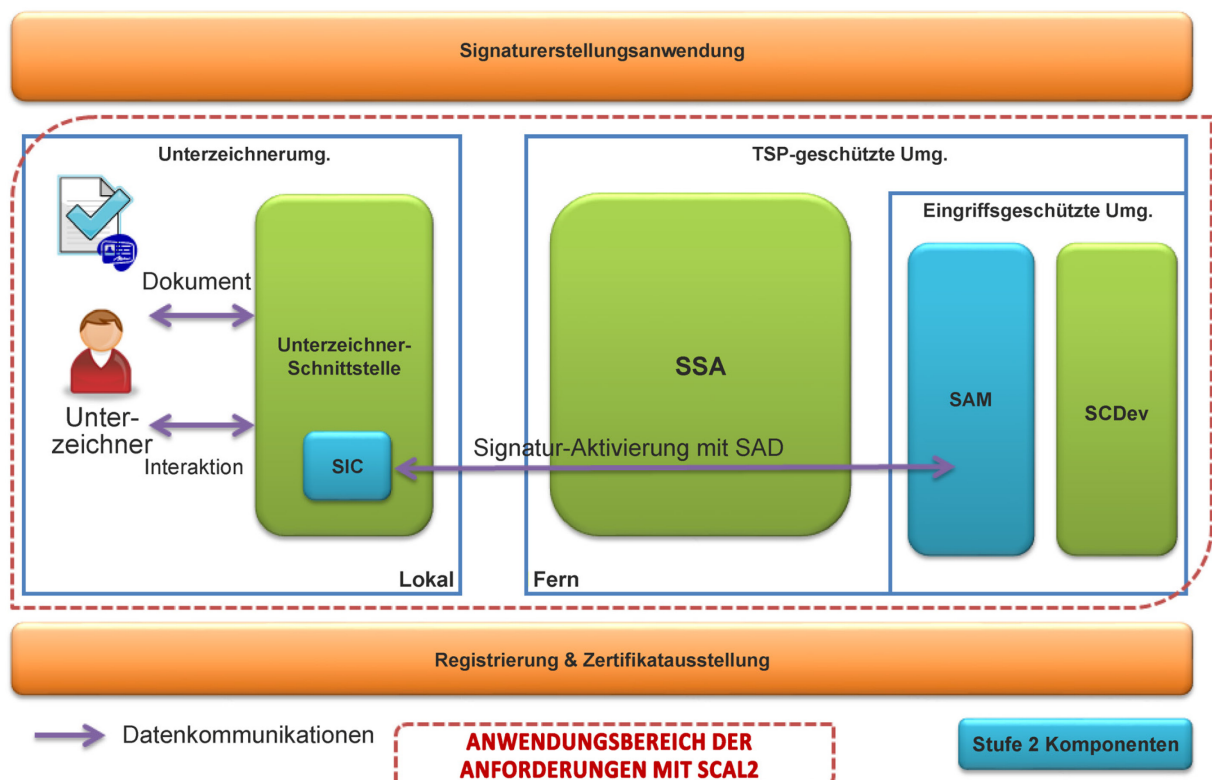


Bild 3 — Signatur-Aktivierungssystem mit SCAL2

ANMERKUNG 1 Diese Architektur kann auf eine externe Partei ausgeweitet werden, wenn die Authentifizierungsübertragung verwendet wird (siehe 5.7.4).

ANMERKUNG 2 Der Anwendungsbereich der Anforderungen kann auf eine externe Partei ausgeweitet werden, wenn die Authentifizierungsübertragung verwendet wird (siehe 5.7.4).

Diese Architektur kann zum Erstellen eines Wertes (z. B. hashverschlüsselt mit dem privaten Schlüssel des Unterzeichners) der digitalen Signatur mit höherer Gewährleistung der Kontrolle benutzt werden.

5.13.4 TW4S-Komponenten

Die Hauptteile eines TW4S, für welche diese Norm Anforderungen festlegt, sind die funktionalen Komponenten:

- Einrichtung der Signierschlüssel – Generierung der Signierschlüssel innerhalb der SCDev und deren Zuweisung zu berechtigten Unterzeichnern zur Benutzung.
- Verwaltung der Signierschlüssel – Löschung, Sicherung und Wiederherstellung von Signierschlüsseln innerhalb der SCDev.
- Authentifizierung des Unterzeichners – Zulassung der Benutzung des Signierschlüssels durch den Unterzeichner.
- Erstellung der digitalen Signatur – Herstellung der Schnittstelle zum berechtigten Unterzeichner, um die digitale Signatur innerhalb der SCDev zu erstellen.

Zur Verbesserung des Sicherheitsniveaus sind zusätzliche Komponenten obligatorisch, um SCAL2 zu erreichen:

- Interaktionskomponente des Unterzeichners – zur Erstellung einer Verknüpfung zwischen dem Unterzeichner und dem Signaturvorgang innerhalb des SAP. Die SIC DARF die SAD in der Umgebung des Unterzeichners generieren. Das SAM wird durch die eingriffsgeschützte Umgebung geschützt und ist für die Ausführung des SAP verantwortlich. Dieses Modul umfasst einen Komponentensatz:
- SAD-Generierung – Generierung der SAD in der eingriffsgeschützten Umgebung, wenn die SAD nicht von der SIC generiert werden.
- Aktivierung des Signierschlüssels – Verwaltung der SAD-Verifizierung und Aktivierung der Signierschlüssel.
- Generierung des Signierschlüssels – Verwaltung der Authentifizierungsfaktoren, die an Signierschlüssel gebunden sind.

6 Sicherheitsanforderungen

6.1 Allgemeines

Dieser Abschnitt beschreibt alle an ein Serversignatursystem gestellten Anforderungen, damit es als TW4S angesehen wird.

Die Anforderungen in 6.4 gelten für TW4S, welche das Alleinige Kontrolle Sicherheitsniveau 2 unterstützen.