

DIN EN 419241-2

ICS 35.030

Entwurf

Einsprüche bis 2017-07-19
 Mit E DIN EN 419241-1:2017-05
 als Ersatz für
 DIN CEN/TS 419241
 (DIN SPEC 91126):2014-06

**Vertrauenswürdige Systeme, die Serversignaturen unterstützen –
 Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur
 Serversignierung;
 Deutsche und Englische Fassung prEN 419241-2:2017**

Trustworthy Systems Supporting Server Signing –
 Part 2: Protection profile for QSCD for Server Signing;
 German and English version prEN 419241-2:2017

Systèmes fiables permettant l'utilisation d'un serveur de signature –
 Partie 2: Profil de protection pour le module de création de signatures fiables (PP-TSCM);
 Version allemande et anglaise prEN 419241-2:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-05-19 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 131 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)



Nationales Vorwort

Dieses Dokument (prEN 419241-2:2017) 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 deutsche Normungsgremium ist der Unterausschuss 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 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen.

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) Definition eines Schutzprofils in DIN EN 419241-2.

Vertrauenswürdige Systeme, die Serversignaturen unterstützen — Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung

Systèmes fiables permettant l'utilisation d'un serveur de signature — Partie 2 : Profil de protection pour le module de création de signatures fiables (PP-TSCM)

Trustworthy Systems Supporting Server Signing — Part 2: Protection profile for QSCD for Server Signing

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

Inhalt

	Seite
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe, Symbole und Abkürzungen	6
3.1 Begriffe	6
3.2 Symbole und Abkürzungen	7
4 Einleitung	7
4.1 Allgemeines	7
4.2 Schutzprofil-Referenz	7
4.3 Schutzprofil-Übersicht — Europäische Gesetzgebung	7
4.4 TOE Übersicht	8
4.4.1 Allgemeines	8
4.4.2 TOE Typ	9
4.4.3 TOE Lebenszyklus	10
4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des TOE	10
4.4.5 TOE-Umgebung allgemeine Übersicht	11
4.4.6 Verfügbare nicht TOE-bezogene Hardware/Software/Firmware	11
4.4.7 Wählbare Festlegung	11
5 Konformitätsanspruch	12
5.1 CC Konformitätsanspruch	12
5.2 PP Anspruch	12
5.3 Begründung der Konformität	12
5.4 Konformitätsaussage	12
6 Definition Sicherheitsproblem	12
6.1 Werte	12
6.2 Themen	15
6.3 Bedrohungen	16
6.3.1 Allgemeines	16
6.3.2 Registrierung	16
6.3.3 Unterzeichner-Verwaltung	17
6.3.4 Nutzung	17
6.3.5 System	19
6.4 Beziehung zwischen Bedrohungen und Werten	20
6.5 Organisatorische Sicherheitsrichtlinien	21
6.6 Annahmen	22
7 Sicherheitsziele	23
7.1 Allgemeines	23
7.2 Sicherheitsziele für das TOE	23
7.2.1 Registrierung	23
7.2.2 Anwenderverwaltung	24
7.2.3 Nutzung	24
7.2.4 System	25
7.3 Sicherheitsziele für die Betriebsumgebung	26
7.3.1 Allgemeines	26
7.3.2 Definition Sicherheitsproblem und Sicherheitsziele	28

7.3.3	Begründung für die Sicherheitsziele	33
8	Erweiterte Komponenten Definitionen — Generierung von zufälligen Zahlen (FCS_RNG)	36
9	Sicherheitsanforderungen	37
9.1	Übersicht SFRs	37
9.2	Sicherheitsfunktionsanforderungen	39
9.2.1	Sicherheitsaudit (FAU)	39
9.2.2	Kryptographische Unterstützung (FCS)	40
9.2.3	Anwenderdatenschutz (FDP)	42
9.2.4	Identifizierung und Authentifizierung (FIA)	50
9.2.5	Sicherheitsverwaltung (FMT)	52
9.2.6	Schutz der TSF (FPT)	54
9.2.7	Vertrauenswürdige Pfade/Kanäle (FTP)	55
9.3	Sicherheitsbestätigungsanforderungen	57
10	Begründung	58
10.1	Sicherheitsanforderungen Begründung	58
10.1.1	Sicherheitsanforderungen Abdeckung	58
10.2	SFR-Abhängigkeiten	62
10.2.1	Allgemeines	62
10.2.2	Begründungen für SARs	64
	Literaturhinweise	65

Europäisches Vorwort

Dieses Dokument (prEN 419241-2:2017) 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.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

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

Überarbeitungen

ÜBERARBEITUNG VOR DER FREIGABE, NUR FÜR DIE REDAKTIONELLE VERFOLGUNG, FÜR DAS FINALE PP ERSETZEN

v0.01	28.08.2015	Erster Entwurf für TC 224/WG 17 Gruppendiskussion, einschließlich Übersicht, Konformitätsanspruch, Werte und Bedrohungen
v0.02	10.11.2015	Aktualisierte Werte und Bedrohungen, basierend auf den Diskussionen anlässlich des TC 224/WG 17 Meetings in La Ciotat, September 2015 sowie auf erhaltenen Anmerkungen im Anschluss an das Meeting.
v0.03	25.11.2015	Aktualisierung basierend auf Anmerkungen von BSI und Thales vor dem CEN/TC 224/WG 17 Meeting in Kochel, November 2015.
v0.4	08.02.2016	Aktualisierung auf Grundlage von Anmerkungen auf v0.03.
v0.5	08.03.2016	Mit SFRs aktualisiert.
v0.6	05.06.2016	Aktualisierung mit Sicherheitsanforderungen und Anmerkungen auf v0.5
v0.7	08.08.2016	Aktualisierung mit SFRs-Anmerkungen auf Version 0.6. Nutzungsbeschreibung aktualisiert, Themen vereinfacht. SFRs stark umstrukturiert, um die Anmerkungen zu behandeln.
v0.8	11.11.2016	Aktualisierung auf Grundlage von Anmerkungen auf v0.7.
v0.9	20.11.2016	Aktualisierung auf Grundlage von Anmerkungen auf v0.8. Begründung beendet.
v0.10	16.12.2016	Aktualisierung auf Grundlage von Anmerkungen auf v0.9, erhalten anlässlich CEN/TC 224/WG 17. Insbesondere für direkte und indirekte Authentifizierung.
v0.11	27.01.2017	Aktualisierung auf Grundlage von Anmerkungen auf v0.10, erhalten anlässlich CEN/TC 224/WG 17 und Oppida.
v0.12	02.02.2017	Aktualisierung auf Grundlage von Anmerkungen auf v0.11, erhalten anlässlich CEN/TC 224/WG 17 und Oppida, vorrangig während des London Meetings.

Einleitung

Dieses Schutzprofil für „QSCD für Serversignaturen“ (SAMP-PP) wird vom Europäischen Komitee für Normung (CEN)/TC 224 ausgestellt.

Das Dokument wurde als ein Schutzprofil (PP) unter Einhaltung der Regeln und Formate von ISO 15408 erstellt, auch bekannt unter der Bezeichnung Common Criteria, Version 3.1r4 [CC1] [CC2] [CC3].

Dieses Dokument gehört inhaltlich zur Reihe 419241, die aus den folgenden Teilen besteht:

- Teil 1: Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen;
- Teil 2: Dieses Dokument

Weitere Einzelheiten dieser Reihe können in Teil 1 gefunden werden.

Aufbau des Dokuments

Abschnitt 1 bietet einleitendes Material für das Schutzprofil.

Abschnitt 3 beschreibt Begriffe.

Abschnitt 4 umfasst die Einleitung.

Abschnitt 5 liefert den Konformitätsanspruch.

Abschnitt 6 umfasst die Definition des Sicherheitsproblems. Er bietet die Werte, Bedrohungen, organisatorische Sicherheitsbestimmungen und Annahmen in Bezug auf das TOE.

Abschnitt 7 definiert in die Sicherheitsziele sowohl für TOE als auch die TOE-Umgebung.

Abschnitt 8 enthält eine erweiterte Komponenten Definition, um die zufällige Zahlengenerierung aufzunehmen.

Abschnitt 9 umfasst die funktionalen Anforderungen und die Sicherheitsanforderungen, die aus den Common Criteria (CC), Teil 2 [CC2] und Teil 3 [CC3] abgeleitet wurden, die vom TOE erfüllt werden sollten.

Abschnitt 10 bietet Begründungen, um zu belegen, dass:

- die Sicherheitsziele den Richtlinien und Bedrohungen genügen;
- SFR zu den Sicherheitszielen passt;
- SFR-Abhängigkeiten erfüllt sind;
- Die SARs angemessen sind.

Ein Referenzabschnitt ist vorgesehen, um Hintergrundmaterialien zu identifizieren.

Eine Liste mit Abkürzungen wurde zur Verfügung gestellt, um häufig verwendete Abkürzungen zu definieren.

1 Anwendungsbereich

Dieser Teil von EN 419241 spezifiziert ein Schutzprofil für ein Unterschriftenaktivierungsmodul (SAM), das darauf abzielt, die Anforderungen eines QSCD, wie in der Verordnung (EU) Nr. 910/2014 [eIDAS] angegeben, zu erfüllen.

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).

prEN 419241-1:2017, *Vertrauenswürdige Systeme, die Serversignaturen unterstützen — Teil 1: Allgemeine Systemsicherheitsanforderungen*

prEN 419221-5:2016, *Schutzprofile für kryptographische Module von Vertrauensdiensteanbietern — Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste*

3 Begriffe, Symbole und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach prEN 419241-1:2017, prEN 419221-5:2016, eIDAS Artikel 3 und die folgenden Begriffe.

ANMERKUNG Die Begriffe aus Common Criteria sind in ISO/IEC 15408-1 angegeben.

3.1.1

Zertifikat

Zertifikat für elektronische Signatur, wie definiert in eIDAS Artikel 3

3.1.2

beauftragte Partei

Subunternehmer des TSP oder notifizierter eID-Anbieter nach eIDAS-Bestimmung, verwendet für die Authentifizierung

3.1.3

digitaler Signaturwert

Ergebnis einer kryptographischen Bedienung, die den Signierschlüssel involviert

Note 1 to entry: Innerhalb dieses Dokuments bezeichnen die Begriffe Siegel, Signatur, digitale Signatur oder digitales Siegel den digitalen Signaturwert.

3.1.4

einmalige Unterzeichnungsschlüssel

Unterzeichnungsschlüssel, der auf einer einzelnen Autorisierung erstellt, verwendet und verworfen wird, üblicherweise in Verbindung mit einer Einzelsitzungsunterzeichnung DTBS/R(s). Im Gegensatz zu Unterzeichnungsschlüsseln, die in mehreren Unterzeichnungssitzungen verwendet werden können

3.2 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Symbole und Abkürzungen nach prEN 419241-1:2017, prEN 419221-5:2016, und eIDAS Artikel 3 und die folgenden.

CA	Zertifizierungsinstanz
CM	Kryptographisches Modul, zertifiziert nach [EN 419221-5]
CSR	Zertifikat der Unterschriftenanforderung
DTBS/R(s)	DTBS/R oder einen Satz an DTBS/R.

4 Einleitung

4.1 Allgemeines

Dieser Abschnitt bietet die Dokumentenverwaltung und Übersichtsinformationen, die erforderlich sind, um die Schutzprofil-Registrierung auszuführen. 4.2 „PP Referenz“ bietet Kennzeichnungs- und beschreibende Informationen, die für die Registrierung des Schutzprofils (PP) notwendig sind. 4.3 „Übersichtsschutzprofil“ fasst das PP in Erzählform zusammen. 4.4 „TOE Übersicht“ fasst das TOE in Erzählform zusammen. Diese Abschnitte als solche geben einem potenziellen Anwender einen Überblick, um zu entscheiden, ob das PP für ihn von Interesse ist. Sie können als eigenständiger Abstrakt in PP-Katalogen und Registern verwendet werden.

4.2 Schutzprofil-Referenz

Titel	Common Criteria Schutzprofil – Schutzprofil für QSCD für Serversignatur
CC Überarbeitung	v3.1 Veröffentlichung 4
PP Version	0.12
Autoren	WG17
Datum der Veröffentlichung	xx/yy/2017 [**noch anzugeben]
Keywörter	Serversignatur,
Registrierung	xxx/yyy [**noch anzugeben]

4.3 Schutzprofil-Übersicht — Europäische Gesetzgebung

Die Verordnung (EU) Nr. 910/2014, eIDAS Punkt 52 berücksichtigt die Erstellung von remoten elektronischen Signaturen, wobei die elektronischen Signaturerstellungsdaten aus der Ferne von einem vertrauenswürdigen Dienstleister im Namen des Unterzeichners verwaltet werden.

Solche vertrauenswürdigen Dienstleister sollten spezifische Verwaltungs- und administrative Sicherheitsverfahren anwenden, um zu garantieren, dass die Erstellungsumgebung der elektronischen Signatur zuverlässig ist und im Rahmen der alleinigen Steuerung des Unterzeichners verwendet wird.

Diese Verordnung verlangt, für qualifizierte elektronische Signaturen, die Verwendung von qualifizierten elektronischen Signaturerstellungsgeräten und für qualifizierte elektronische Siegel, die Verwendung von qualifizierten elektronischen Siegelerstellungsgeräten, wie in dieser Verordnung definiert. Im vorliegenden Dokument werden beide Arten von Geräten als QSCD bezeichnet.

4.4 TOE Übersicht

4.4.1 Allgemeines

Ein vertrauenswürdiges System, das die Serversignatur (TW4S) unterstützt, ist ein System, das remote digitale Signaturen als einen Dienst anbietet. Es stellt sicher, dass der oder die Unterzeichnungsschlüssel des Unterzeichners nur unter der alleinigen Steuerung des Unterzeichners zum beabsichtigten Zweck verwendet werden.

In diesem Dokument verwendet das TW4S ein geographisches Modul, um den Unterzeichnungsschlüssel zu generieren und den digitalen Signaturwert zu erstellen.

Das System besteht aus einer lokalen und einer Remote-Umgebung. Der Unterzeichner befindet sich in der lokalen Umgebung und interagiert über ein Gerät (z. B. Laptop, Tablett oder Smartphone) mit der Serversignaturanwendung (SSA) in der Remote-Umgebung.

Der Zweck der Interaktion zwischen dem Gerät und der SSA ist, dass der Unterzeichner den Unterzeichnungsdienst der SSA verwendet. Die Aktion der Unterzeichnung wird über ein Signaturaktivierungsprotokoll (SAP) ausgeführt, das verlangt, dass die Signaturaktivierungsdaten (SAD) in der lokalen Umgebung zur Verfügung gestellt werden. Die SAD verbinden drei Elemente: Authentifizierung des Unterzeichners mit dem Unterzeichnungsschlüssel und die zu unterzeichnenden Daten (DTBS/R(s)).

Um sicherzustellen, dass der Unterzeichner die alleinige Kontrolle über seine Unterzeichnungsschlüssel hat, muss der Unterzeichnungsvorgang autorisiert werden. Dies erfolgt über ein Signaturaktivierungsmodul (SAM), das ein Ende des SAP handhaben, SAD prüfen und den Unterzeichnungsschlüssel innerhalb eines kryptographischen Moduls aktivieren kann. Sowohl das kryptographische Modul als auch das SAM müssen sich in einer eingriffsgeschützten Umgebung befinden. SAD-Verifizierung bedeutet, dass das SAM die Bindung zwischen den drei SAD-Elementen prüft sowie eine Überprüfung durchführt, dass der Unterzeichner authentifiziert ist.

Eines der drei SAD-Elemente ist die Unterzeichner-Authentifizierung. Von der Unterzeichner-Authentifizierung wird angenommen, dass sie für qualifizierte Signaturen nach prEN 419241-1:2017 SCAL.2 durchgeführt wird. Das heißt, die Unterzeichner-Authentifizierung kann auf eine der folgenden Art und Weisen ausgeführt werden:

- Direkt über das SAM. In diesem Fall überprüft das SAM den/die Authentifizierungsfaktor/en des Unterzeichners.
- Indirekt über das SAM. In diesem Fall, ein externer Authentifizierungsdienst als Teil von TW4S oder eine beauftragte Partei, die den/die Authentifizierungsfaktor/en des Unterzeichners prüfen und eine Erklärung ausstellen, dass der Unterzeichner authentifiziert wurde. Das SAM muss die Erklärung prüfen.
- Eine Kombination der zwei direkten oder indirekten Schemata, wobei ein Teil der Unterzeichner-Authentifizierung direkt über das SAM und der andere Teil indirekt über das SAM erfolgen.

Wenn die Unterzeichner-Authentifizierung nicht direkt über das SAM durchgeführt wird, muss das SAM (auf der Umgebung) annehmen, dass ein Teil der Authentifizierung oder die vollständige Authentifizierung stattgefunden hat und verlässt sich auf die Erklärung. In diesem PP bedeutet Unterzeichner-Authentifizierung, dass der Unterzeichner über eine der drei oben genannten Vorgehensweisen authentifiziert wurde.

Das SAM-Modul ist das TOE dieses PP. Die Zertifizierung des TOE und des kryptographischen Moduls nach prEN 419221-5:2016 ist erforderlich, um ein QSCD zu erhalten.

Das Bild unten gibt einen Überblick über die Umgebung, in die das TOE platziert wird.

Der Unterzeichner befindet sich in der lokalen Umgebung, mit einer Benutzerschnittstelle auf einem Gerät (z. B. Laptop, Tablett, Smartphone). Die Benutzerschnittstelle kann Dokumente für den Unterzeichner anzeigen. Das Gerät findet eine Unterzeichner-Interaktionskomponente (SIC), um mit der SSA zu kommunizieren. Die SSA leitet die Kommunikation von der SIC oder der SSA an das QSCD weiter. Innerhalb des QSCD empfängt das SAM die Nachrichten und kommuniziert optional mit der SSA, um die relevanten Daten zu erhalten. Wenn das SAM-Modul die SAD geprüft hat, kann es die Aktivierung des Unterzeichnungsschlüssels innerhalb des kryptographischen Moduls autorisieren und einen digitalen Signaturwert erzeugen. Der Wert wird an die SSA zurückgesendet und kann weiter an die SCA oder die SIC geliefert werden.

Das TEO generiert Audit-Datensätze. Es beruht darauf, dass die SSA Audit-Datensätze speichern.

TW4S beruht auf anderen Diensten:

- Die Unterzeichner müssen identifiziert und registriert werden. Dies kann die Errichtung eines Authentifizierungsmechanismus für einen Unterzeichner involvieren.
- Unterzeichnungsschlüssel werden von einer Zertifizierungsinstanz zertifiziert.
- Die Signaturerstellungsanwendung ist für die Erstellung des unterzeichneten Dokuments unter Verwendung der Signaturwerte, die von TW4S zur Verfügung gestellt werden, verantwortlich.

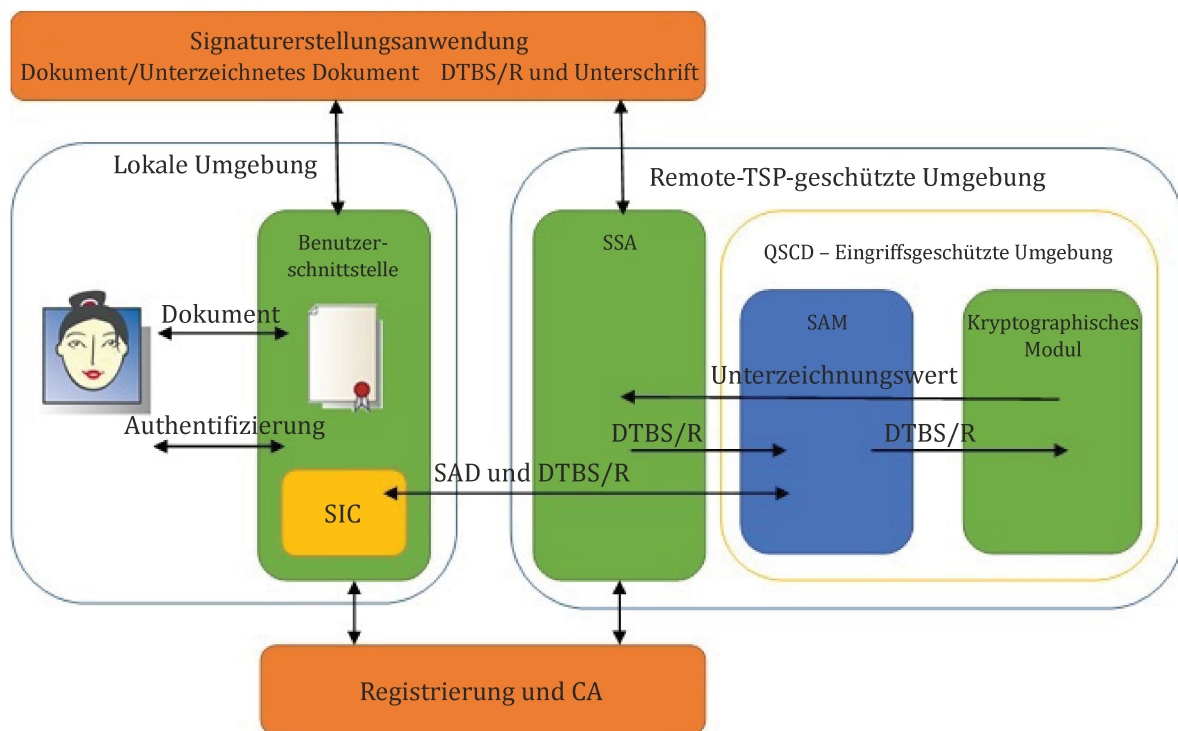


Bild 1

4.4.2 TOE Typ

Das TOE ist eine Softwarekomponente, die das Signaturaktivierungsprotokoll (SAP) implementiert. Sie ist entweder innerhalb des eingriffsgeschützten Teils des kryptographischen Moduls oder alternativ in einer zugewiesenen eingriffsgeschützten Umgebung umgesetzt, die über einen vertrauenswürdigen Kanal mit dem kryptographischen Modul verbunden ist.

Sie verwendet die Signaturaktivierungsdaten (SAD) vom Unterzeichner, um den entsprechenden Unterzeichnungsschlüssel zur Verwendung in einem kryptographischen Modul zu aktivieren.

Das TOE und das kryptographische Modul sind gemeinsam ein QSCD.

4.4.3 TOE Lebenszyklus

Der TOE Lebenszyklus besteht aus aufeinanderfolgenden Phasen für Entwicklung, Erzeugung, Vorbereitung und Betrieb.

Entwicklung: Der TOE-Entwickler entwickelt die TOE-Anwendung und deren Dokumentation der Benutzerführung unter Verwendung einer geeigneten Dokumentation zur Benutzerführung für Komponenten, die mit dem TOE arbeiten, darunter auch das kryptographische Modul.

Lieferung: Das TOE wird vom TOE-Entwickler sicher an den TSP geliefert.

Installation und Konfiguration: Der TSP installiert und konfiguriert das TOE mit den entsprechenden Konfigurations- und Initialisierungsdaten. Die Installation kann die Erstellung von privilegierten Anwendern ermöglichen.

Betriebsphase: Im Betrieb kann das TOE von privilegierten Anwendern verwendet werden, um privilegierte Anwender und Unterzeichner zu erstellen. Privilegierte Anwender können die TOE-Konfiguration warten. Privilegierte Anwender und Unterzeichner können Unterzeichnungsschlüssel für einen Unterzeichner generieren. Privilegierte Anwender und Unterzeichner können die zu unterzeichnenden Daten an das TOE liefern, allerdings kann nur der Unterzeichner die Erstellung einer Signatur autorisieren.

Das Ende der Lebensdauer des TOE fällt nicht unter den Anwendungsbereich dieses Dokuments.

4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des TOE

Die wesentlichen Sicherheitsmerkmale des TOE sind:

- Bedienerverwaltung:
 - Privilegierte Anwender können andere privilegierte Anwender erstellen.
- Systemverwaltung
 - Privilegierte Anwender können die Systemkonfiguration bearbeiten.
- Die Unterzeichner-Verwaltung deckt Folgendes ab:
 - Privilegierte Anwender können Unterzeichner erstellen
 - Privilegierte Anwender können eines der drei Authentifizierungsschemata (direkt, indirekt oder gemischt) einem Unterzeichner zuweisen.
 - Privilegierte Anwender oder Unterzeichner können Unterzeichnungsschlüssel und Signaturprüfdaten (SVD) unter Verwendung eines kryptographischen Moduls generieren und den Unterzeichnungs-Schlüsselbezeichner und SVD einem Unterzeichner zuweisen.
 - Privilegierte Anwender oder Unterzeichner können einen Unterzeichnungs- Schlüsselbezeichner deaktivieren, der von einem Unterzeichner verwendet werden soll.
- Handlung der Signatur
 - Privilegierte Anwender oder Unterzeichner können DTBS/R(s) zur Unterzeichnung vorlegen.
 - Die Verbindung zwischen der Unterzeichner-Authentifizierung, den DTBS/R(s) und dem Unterzeichnungs-Schlüsselbezeichner wird von den Signaturaktivierungsdaten (SAD) gehandhabt. Diese SAD werden mit dem TOE sicher unter Verwendung des Signaturaktivierungsprotokolls (SAP) ausgetauscht. Innerhalb des TOE werden die folgenden Aktionen durchgeführt:

- Die SAD werden in Integrität geprüft.
 - Die SAD werden darauf überprüft, dass sie die Unterzeichner-Authentifizierung, eine DTBS/R(s) und den Unterzeichnungs-Schlüsselbezeichner miteinander verbinden.
 - Der Unterzeichner, der in den SAD identifiziert wird, wird über die Verwendung eines der drei Authentifizierungsschemata authentifiziert.
 - Die für den Signaturvorgang verwendete DTBS/R(s) ist sie mit den SAD verbunden.
 - Der Unterzeichnungs-Schlüsselbezeichner wird dem Unterzeichner zugewiesen.
 - Das TOE verwendet Autorisierungsdaten, um den Unterzeichnungsschlüssel innerhalb des kryptographischen Moduls zu aktivieren.
 - Das TOE verwendet das kryptographische Modul, um Signaturen zu erstellen.
- Ein Audit-Trail aller sicherheitsrelevanten Ereignisse innerhalb des TOE wird erzeugt. Der Verwaltung Zugriff auf den Audit-Trail fällt nicht in den Anwendungsbereich des TOE.

Das TOE behandelt Datenwerte, wie in 6.1 angegeben.

4.4.5 TOE-Umgebung allgemeine Übersicht

Dieses PP zielt darauf ab, TSPs zu unterstützen, die für die Serversignatur ein QSCD verwenden müssen.

Vom TOE wird Folgendes erwartet:

- 1) als Teil des Serversignatursystems zu agieren, wie in prEN 419241-1:2017 angegeben;
- 2) von einem TSP mit Sicherheitsrichtlinien verwendet zu werden, wie von den TSPs verlangt wird, die Signaturerstellungsdienste bieten;
- 3) in Verbindung mit TSPs verwendet zu werden, die Zertifikate ausstellen.

4.4.6 Verfügbare nicht TOE-bezogene Hardware/Software/Firmware

Das TOE benötigt mindestens die folgende Hardware/Software/Firmware, um betrieben zu werden:

- Eine Signaturerstellungsanwendung (SCA), die das Dokument verwaltet, das zu unterzeichnen ist und dieses an die SSA, entweder direkt oder über die SIC, überträgt.
- Eine SSA-Komponente, die die Kommunikationen zwischen SAM im QSCD und der SIC im Unterzeichnungsgerät handhabt.
- Eine SIC, die lokal vom Unterzeichner verwendet wird, um mit den Remote-Systemen zu kommunizieren.
- Ein kryptographisches Modul, wie in prEN 419221-5:2016 angegeben, das den Betrieb des TOE unterstützt.

4.4.7 Wählbare Festlegung

Das Schutzprofil umfasst wählbare Festlegungen, die der ST-Schreiber spezifizieren muss. Um den ST-Schreiber bei der Identifizierung dieser wählbaren Festlegungen zu unterstützen, werden in Tabelle 1 zusammengefasst:

Tabelle 1

Option	Beschreibung
Umsetzung	Das TOE kann in einem kryptographischen Modul oder in einem bestimmten Hardware-Modul umgesetzt werden.

5 Konformitätsanspruch

5.1 CC Konformitätsanspruch

Dieses Schutzprofil geht mit den Common Criteria, Version 3.1, Revision 4 konform.

Präziser, dieses Schutzprofil ist:

- CC Teil 1 [ISO/IEC 15408-1],
- CC Teil 2 konform [ISO/IEC 15408-2],
- CC Teil 3 konform [ISO/IEC 15408-3].

Die Sicherungsanforderung dieses Schutzprofils ist **EAL4 Erweitert**. Erweiterungsergebnisse aus der Auswahl von:

- AVA_VAN.5 Erweiterte methodische Schwachstellenanalyse

5.2 PP Anspruch

Dieses PP beansprucht keine Konformität mit einem anderen Schutzprofil.

5.3 Begründung der Konformität

Da dieses PP keine Konformität mit einem anderen Schutzprofil beansprucht, ist hier keine Begründung notwendig.

5.4 Konformitätsaussage

Dieses PP verlangt die strikte Konformität eines jeden anderen SP oder PP, dass die Konformität mit diesem PP beansprucht.

6 Definition Sicherheitsproblem

6.1 Werte

Das TOE hat die folgenden Werte, die in Integrität und Vertraulichkeit, wie nachstehend beschrieben, geschützt werden müssen. Das TOE muss sicherstellen, dass, wann immer sich ein Wert außerhalb des TOE befindet, das TOE die notwendigen kryptographischen Aktivitäten durchgeführt hat, um die Vertraulichkeit durchzusetzen und erkennen kann, ob ein Wert verändert wurde. Die Zugriffskontrolle auf TOE-Werte außerhalb des TOE ist durch die Umgebung durchzusetzen.

R.Signing_Key_Id: Der Unterzeichnungsschlüssel ist der private Schlüssel eines asymmetrischen Schlüssel-paares für die Erstellung einer digitalen Signatur unter der alleinigen Kontrolle des Unterzeichners. Der Unterzeichnungsschlüssel kann nur über das kryptographische Modul verwendet werden. Das TOE verwendet den Wert R.Signing_Key_Id, der einen Unterzeichnungsschlüssel im kryptographischen Modul bezeichnet. Die Bindung des R.Signing_Key_Id mit R.Signer muss in der Integrität geschützt werden.

Anwendungshinweis 1

Die Integrität und die Vertraulichkeit des Unterzeichnungsschlüssels und der Verknüpfung zwischen R.Signing_Key_Id und dem Unterzeichnungsschlüssel liegen in der Verantwortung des kryptographischen Moduls. Das TOE muss sicherstellen, dass nur der Unterzeichner den Unterzeichnungsschlüssel unter seiner alleinigen Kontrolle verwenden kann.

R.Authorisation_Data: Hierbei handelt es sich um Daten, die vom TOE verwendet werden, um einen Unterzeichnungsschlüssel im kryptographischen Modul zu aktivieren. Der Unterzeichnungsschlüssel wird von R.Signing_Key_Id bezeichnet. Er muss in Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 2

R.Authorisation_Data wird vom kryptographischen Modul verwendet, um einen Unterzeichnungsschlüssel zu aktivieren. Die Daten können ein Wert des TOE sein oder vom TOE aus den SAD abgeleitet werden. In beiden Fällen muss das TOE die SAD überprüfen, bevor R.Authorisation_Data verwendet wird, um den Unterzeichnungsschlüssel im kryptographischen Modul zu aktivieren.

Wenn das TOE R.Authorisation_Data aus den SAD ableitet, werden diese Daten vom TOE möglicherweise nicht gehalten.

R.SVD: Signaturprüfdaten sind der öffentliche Teil, assoziiert mit dem Unterzeichnungsschlüssel, um die digitale Signaturprüfung durchzuführen. Die R.SVD müssen in Integrität geschützt sein.

Das TOE verwendet ein kryptographisches Modul für die Generierung des Unterzeichnungsschlüsselpaares. Als Teil der Generierung des Unterzeichnungsschlüsselpaares stellt das kryptographische Modul dem TOE die Werte R.Signing_Key_Id und R.SVD zur Verfügung. Das TOE stellt der SSA die R.SVD für die weitere Handhabung zu Verfügung, damit das Schlüsselpaar zertifiziert werden kann.

R.DTBS/R: Ein Datensatz, der an das TOE für die Erstellung der digitalen Signatur im Namen des Unterzeichners übermittelt wird. Der DTBS/R(s) wird an das TOE übermittelt. Die R.DTBS/R müssen in Integrität geschützt sein. Die Übertragung der DTBS/R(s) an das TOE muss verlangen, dass die sendende Partei - Unterzeichner oder privilegierter Anwender - authentifiziert wird.

Anwendungshinweis 3

Die Vertraulichkeit der R.DTBS/R wird von der Verordnung (EU) Nr. 910/2014 eIDAS nicht verlangt.

R.SAD: Signaturaktivierungsdaten sind ein Datensatz, der in das Signaturaktivierungsprotokoll involviert ist, der die Signaturerstellungsdaten aktiviert, um eine digitale Signatur unter der ausschließlichen Kontrolle des Unterzeichners erstellen zu können. R.SAD müssen Folgendes kombinieren:

- die starke Authentifizierung des Unterzeichners, wie in prEN 419241-1:2017 angegeben;
- wenn kein besonderer Schlüssel impliziert ist (z. B. ein Standard- oder ein einmaliger Schlüssel), ein eindeutiger Verweis auf R.Signing_Key_Id;
- eine gegebene R.DTBS/R.

Die R.SAD müssen in Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 4

Wenn die SAD keine verschlüsselten Daten verlangen, gilt die Vertraulichkeitsanforderung als erfüllt. Der ST-Schreiber muss beschreiben, welcher Teil der SAD in Vertraulichkeit geschützt werden muss.

Anwendungshinweis 5

Die R.SAD kann einige oder alle Authentifizierungsfaktoren oder Nachweise aus anderen Systemen enthalten, dass einige oder alle Authentifizierungsfaktoren geprüft wurden.

Anwendungshinweis 6

Die eindeutige Referenz auf R.Signing_Key_Id in den R.SAD könnten zertifiziert, Schlüsselbezeichner oder abgeleitete Informationen sein, die aus der Authentifizierung des Unterzeichners erhalten werden.

Einige Lösungen können einmalige Unterzeichnungsschlüssel verwenden, die innerhalb einer begrenzten Unterzeichnungssitzung generiert, zertifiziert und verwendet werden. Die aus der Authentifizierung des Unterzeichners abgeleiteten Informationen können verwendet werden, um eine Sitzungstrennung zu bieten, wenn ein Unterzeichner mehrere gleichzeitige Unterzeichnungssitzungen mit dem TOE hat oder um eine R.Signing_Key_Id abzuleiten, wenn der Schlüssel ein einmaliger Schlüssel ist. Am Ende der Sitzung wird der Unterzeichnungsschlüssel zuverlässig deaktiviert.

Bei Lösungen, die nur einen Unterzeichnungsschlüssel für jeden Unterzeichner handhaben, kann die Referenz auf die R.Signing_Key_Id aus den SAD außerdem impliziert oder weggelassen werden.

Der ST-Schreiber muss beschreiben, welche R.Signing_Key_Id für ein spezifisches TOE gilt.

R.Signature: Ist das Ergebnis des Signaturvorgangs und ist ein digitaler Signaturwert. R.Signature wird auf den R.DTBS/R unter Verwendung einer R.Signing_Key_Id durch das kryptographische Modul erstellt, unter der Kontrolle des Unterzeichners als Teil des SAP. Die R.Signature muss in Integrität geschützt sein. Die R.Signature kann außerhalb des TOE unter Verwendung von R.SVD geprüft werden.

R.Audit: Hierbei handelt es sich um Audit-Aufzeichnungen, die Protokolle von Ereignissen enthalten, die überprüft werden müssen. Die Protokolle werden vom TOE erzeugt und extern gespeichert. R.Audit muss in Integrität geschützt sein.

R.Signer: Ist ein TOE-Subjekt, das den Datensatz enthält, der den Unterzeichner innerhalb des TOE eindeutig identifiziert. R.Signer muss in Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 7

R.Signer muss nur innerhalb des TOE eindeutig sein. Es liegt nicht in der Verantwortung des TOE, eine Verbindung zwischen R.Signer und der Identität des Unterzeichners herzustellen. Der Unterzeichner sollte das R.Signer-Objekt besitzen, das ihn innerhalb des TOE eindeutig identifiziert.

Anwendungshinweis 8

R.Signer kann Referenzen auf keine, eine oder mehrere R.Signing_Key_Ids und R.SVDs enthalten.

Anwendungshinweis 9

Wenn R.Signer keine verschlüsselten Daten verlangt, gilt die Vertraulichkeitsanforderung als erfüllt. Der ST-Schreiber muss beschreiben, welcher Teil von R.Signer in Vertraulichkeit geschützt werden muss.

R.Reference_Signer_Authentication_Data: Dies ist der Datensatz, der vom TOE zur Authentifizierung des Unterzeichners verwendet wird. Er enthält alle Daten (z. B. Seriennummer des OTP-Geräts, Telefonnummern, Protokolleinstellungen usw.) und Schlüssel (z. B. Geräteschlüssel, Verifizierungsschlüssel usw.), die vom TOE verwendet werden, um den Unterzeichner zu authentifizieren. Dies kann Signaturprüfdaten oder ein Zertifikat umfassen, um eine Erklärung, die als Ergebnis einer delegierten Authentifizierung zur Verfügung gestellt wurde, zu prüfen.

R.Reference_Signer_Authentication_Data müssen in Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 10

Die R.Reference_Signer_Authentication_Data werden vom TOE verwendet, um den Unterzeichner zu authentifizieren und die R.Authorisation_Data werden vom TOE verwendet, um einen Unterzeichnungsschlüssel im kryptographischen Modul zu aktivieren.

Anwendungshinweis 11

Wenn R.Reference_Signer_Authentication_Data keine verschlüsselten Daten verlangen, gilt die Vertraulichkeitsanforderung als erfüllt. Der ST-Schreiber muss beschreiben, welcher Teil von R.Reference_Signer_Authentication_Data in Vertraulichkeit geschützt werden muss.

R.TSF_DATA: Dies ist der TOE-Konfigurationsdatensatz, der verwendet wird, um das TOE zu betreiben. Er muss in Integrität geschützt sein.

Anwendungshinweis 12

Die TOE-Konfigurationsdaten können einen kryptographischen Algorithmus, die Schlüssellänge, Abläufe für SAP usw. enthalten.

R.Privileged_User ist ein TOE-Subjekt, das den Datensatz enthält, der einen privilegierten Anwender innerhalb des TOE eindeutig identifiziert. Er muss in Integrität geschützt sein.

R.Reference_Privileged_User_Authentication_Data ist der Datensatz, der vom TOE zur Authentifizierung des privilegierten Anwenders verwendet wird. Er muss in Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 13

Wenn R.Reference_Privileged_User_Authentication_Data keine verschlüsselten Daten verlangt, gilt die Vertraulichkeitsanforderung als erfüllt. Der ST-Schreiber muss beschreiben, welcher Teil von R.Reference_Privileged_User_Authentication_Data in Vertraulichkeit geschützt werden muss.

R.Random sind zufällige Sicherheitsinformationen, z. B. Schlüssel, die vom TOE für den Betrieb und die Kommunikation mit externen Parteien verwendet werden. Er muss in Integrität und Vertraulichkeit geschützt sein.

6.2 Themen

Die folgende Liste führt alle Subjekte auf, die mit dem TOE interagieren.

- Unterzeichner, dies ist die natürliche oder juristische Person, die das TOE über das SAP verwendet, wo die SAD zur Verfügung gestellt werden und DTBS/R(s) unterzeichnet werden kann, unter Verwendung des eigenen Unterzeichnungsschlüssels im kryptographischen Modul.
- Privilegierte Anwender, dieser führt die administrativen Funktionen des TOE aus und ist in der Lage, dem TOE als Teil des Signaturvorgangs DTBS/R(s) zur Verfügung zu stellen.

Anwendungshinweis 14

Die Liste der in prEN 419241-1:2017, 6.2.1.2, SRG M.1.2 beschriebenen Subjekte enthält mehr Rollen, da sie das gesamte T4WS abdeckt.

Der ST-Schreiber muss die spezifischen Rollen beschreiben, die er implementiert und wie diese in den SFRs mit den Autorisierungsregeln in Zusammenhang stehen.

Anwendungshinweis 15

Die SSA spielt eine besondere Rolle, da sie direkt mit dem TOE interagiert. Privilegierte Anwender können mit dem TOE direkt oder über die SSA interagieren. Wenn die SSA als ein Dienst administrative Funktionen ausführen kann, z. B. einen Unterzeichner erstellen, gilt dies in diesem PP als privilegierte Anwender.

Anwendungshinweis 16

Man erwartet, dass die Erstellung von Unterzeichnern, die Verwaltung von Referenz-Authentisierungsdaten eines Unterzeichners und die Generierung eines Unterzeichnungsschlüssels gemeinsam mit einer Registrierungsstelle (RA) ausgeführt wird, die einen Registrierungsdienst unter Verwendung der SSA, wie z. B. angegeben in ETSI EN 319 411-1 zur Verfügung stellt.

6.3 Bedrohungen

6.3.1 Allgemeines

Die folgenden Bedrohungen sind für das TOE definiert. Ein in jeder der Bedrohungen beschriebener Angreifer ist eine Person, die für die entsprechende Aktion nicht autorisiert ist, sich aber als ein unbekannter Anwender oder es eine der anderen definierten Personen präsentieren könnte.

6.3.2 Registrierung

Die Bedrohungen während der Registrierung sind:

T.ENROLMENT_SIGNER_IMPERSONATION

Ein Angreifer gibt sich während der Registrierung als Unterzeichner aus. Beispiele hierfür könnten sein:

- durch Übertragung des falschen R.Signer von RA an TOE;
- durch Übertragung der falschen R.Reference_Signer_Authentication_Data von RA an TOE.

Die Werte R.Signer und R.Reference_Signer_Authentication_Data sind bedroht.

Ein solcher Identitätsbetrug könnte eine mögliche falsche Unterzeichner-Authentifizierung zulassen, die zu einer unautorisierten Signatur im Namen des Unterzeichners führen könnte.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

Ein Angreifer ist in der Lage während der Registrierung alle oder einen Teil der R.Reference_Signer_Authentication_Data zu erhalten. Dies kann während der Generierung, der Speicherung oder der Übertragung an das TOE oder bei der Übertragung zwischen Unterzeichner und TOE erfolgen. Beispiele hierfür könnten sein:

- durch Lesen der Daten;
- durch Veränderung der Daten, z B. auf einen bekannten Wert.

Der Wert R.Reference_Signer_Authentication_Data ist bedroht.

Eine solche Offenlegung von Daten könnte eine mögliche falsche Unterzeichner-Authentifizierung zulassen, die zu einer unautorisierten Signatur im Namen des Unterzeichners führen könnte.

Die Bedrohungen bei der Registrierung sind Bedrohungen auf der Umgebung, im Falle dass die externe Authentifizierung vom TOE unterstützt wird.

T.SVD_FORGERY

Ein Angreifer modifiziert die R.SVD während der Übertragung an RA oder CA. Dies führt zu einem Verlust der R.SVD-Integrität in der Bindung der R.SVD an den Unterzeichnungsschlüssel und den R.Signer.

Der Wert R.SVD ist bedroht.

Wenn sich CA auf die Generierung des Schlüsselpaares, vom TOE gesteuert, wie in ETSI EN 319 411-1, 6.3.3 d) angegeben, verlässt, kann der Angreifer Signaturen fälschen, indem er sich als der Unterzeichner ausgibt.

Anwendungshinweis 17

Es sollte eine sichere Übertragung von R.SVD vom TOE an RA oder CA vorhanden sein. Vom SAM wird erwartet, ein CSR zu erzeugen.

Wenn die Registrierungsdienste des TSP ein Zertifikat erstellen, das einen „Besitznachweis oder die Kontrolle des privaten Schlüssels“ mit den SVD verbunden verlangen, wie in ETSI EN 319 411-1, 6.3.1 a) angegeben, kann dieser Bedrohung ohne spezifische Maßnahmen innerhalb des TOE entgegengetreten werden.

6.3.3 Unterzeichner-Verwaltung

T.ADMIN_IMPERSONATION

Der Angreifer gibt vor, ein privilegierter Anwender zu sein und aktualisiert R.Reference_Signer_Authentication_Data, R.Signing_Key_Id oder R.SVD.

Die Werte R.Reference_Signer_Authentication_Data, R.SVD und R.Signing_Key_Id sind bedroht.

Eine solche Modifizierung von Daten könnte eine mögliche falsche Unterzeichner-Authentifizierung zulassen, die zu einer unautorisierten Signatur im Namen des Unterzeichners führen könnte.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

Der Angreifer offenbart oder ändert (z. B. auf einen bekannten Wert) R.Reference_Signer_Authentication_Data während der Aktualisierung und ist in der Lage eine Signatur zu erstellen.

Die Werte R.Reference_Signer_Authentication_Data, und R.Signing_Key_Id sind bedroht.

Eine solche Offenlegung von Daten könnte eine mögliche falsche Unterzeichner-Authentifizierung zulassen, die zu einer unautorisierten Signatur im Namen des Unterzeichners führen könnte.

6.3.4 Nutzung

Dieser Abschnitt beschreibt die Bedrohungen für den Signaturvorgang einschließlich der Authentifizierung.

T.AUTHENTICATION_SIGNER_IMPERSONATION

Ein Angreifer gibt sich als Unterzeichner aus, unter Verwendung gefälschter R.Reference_Signer_Authentication_Data und übermittelt diese an das TOE während des SAP und verwendet sie, um dieselben oder modifizierte DTBS/R(s) zu signieren.

Die Werte R.Reference_Signer_Authentication_Data, R.SAD und R.Signing_Key_Id sind bedroht.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED

Ein Angreifer ist in der Lage, R.Reference_Signer_Authentication_Data innerhalb des TOE zu modifizieren.

Der Wert R.Reference_Signer_Authentication_Data ist bedroht.

Eine solche Modifizierung von Daten könnte eine mögliche falsche Unterzeichner-Authentifizierung zulassen, die zu einer unautorisierten Signatur im Namen des Unterzeichners führen könnte.

T.SAP_BYPASS

Ein Angreifer umgeht einen oder mehrere Schritte im SAP und ist in der Lage, eine Signatur zu erstellen, ohne dass der Unterzeichner diesen Vorgang autorisiert hat.

Der Wert R.SAD ist bedroht.

T.SAP_REPLAY

Ein Angreifer verwendet einen oder mehrere Schritte im SAP wieder und ist in der Lage, eine Signatur zu erstellen, ohne dass der Unterzeichner diesen Vorgang autorisiert hat.

Der Wert R.SAD ist bedroht.

T.SAD_FORGERY

Ein Angreifer fälscht oder manipuliert R.SAD während der Übertragung im SAP und ist in der Lage, eine Signatur zu erstellen, ohne dass der Unterzeichner diesen Vorgang autorisiert hat.

Der Wert R.SAD ist bedroht.

T.SIGNATURE_REQUEST_DISCLOSURE

Ein Angreifer erhält Kenntnis der R.DTBS/R oder R.SAD während der Übertragung an TOE.

Die Werte R.DTBS/R und R.SAD sind bedroht.

Anwendungshinweis 18

Wenn die R.DTBS/R oder R.SAD keine verschlüsselten Daten verlangen, ist diese Bedrohung geringer.

T.DTBSR_FORGERY

Ein Angreifer modifiziert R.DTBS/R während der Übertragung an TOE und ist in der Lage, eine Signatur auf diesen modifizierten R.DTBS/R zu erstellen, ohne dass der Unterzeichner den Vorgang auf diesen R.DTBS/R autorisiert hat.

Der Wert R.DTBS/R ist bedroht.

T.SIGNATURE_FORGERY

Ein Angreifer modifiziert R.Signature während oder nach der Erstellung oder während der Übertragung außerhalb des TOE.

Der Wert R.Signature ist bedroht.

Anwendungshinweis 19

Die Modifizierung einer Signatur kann über die SSA oder eine darauf beruhende Partei durch Validierung der Signatur erkannt werden.

6.3.5 System

T.PRIVILEGED_USER_INSERTION

Ein Angreifer kann R.Privileged_User inklusive R.Reference_Privileged_User_Authentication_Data erstellen und sich am TOE als ein privilegierter Anwender anmelden.

Die Werte R.Privileged_User und R.Reference_Privileged_User_Authentication_Data sind bedroht.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION

Ein Angreifer modifiziert R.Reference_Privileged_User_Authentication_Data und kann sich am TOE als ein privilegierter Anwender anmelden.

Der Wert R.Reference_Privileged_User_Authentication_Data ist bedroht.

T.AUTHORISATION_DATA_UPDATE

Ein Angreifer gibt sich als privilegierter Anwender aus und aktualisiert R.Authorisation_Data und könnte so in der Lage sein, einen Unterzeichnungsschlüssel zu aktivieren.

Die Werte R.Authorisation_Data und R.Signing_Key_Id sind bedroht.

Anwendungshinweis 20

In einigen Anwendungen kann es für einen Angreifer mit Zugriff auf R.Authorisation_Data und R.Signing_Key_Id ausreichen, den Unterzeichnungsschlüssel innerhalb des kryptographischen Moduls zu aktivieren. Da R.Signing_Key_Id nur in Integrität und nicht in Vertraulichkeit geschützt ist, sollte der Zugriff auf R.Authorisation_Data nur autorisierten Bedienern erlaubt sein.

T.AUTHORISATION_DATA_DISCLOSE

Ein Angreifer legt R.Authorisation_Data während der Aktualisierung offen und ist in der Lage, einen Unterzeichnungsschlüssel zu aktivieren.

Die Werte R.Authorisation_Data und R.Signing_Key_Id sind bedroht.

T.CONTEXT_ALTERATION

Ein Angreifer modifiziert die Systemkonfiguration R.TSF_DATA, um eine unbefugte Handlung auszuführen.

Die Werte R.Signing_Key_Id, R.SVD, R.SAD, R.Reference_Signer_Authentication_Data und R.TSF_DATA sind bedroht.

T.AUDIT_ALTERATION

Ein Angreifer modifiziert das Systemaudit und ist in der Lage, Spuren der Modifizierung oder Nutzung des TOE zu verbergen.

Die Werte R.SVD, R.SAD, R.Signer, R.Reference_Signer_Authentication_Data, R.DTBS/R, R.Signature, R.AUDIT und R.TSF_DATA sind bedroht.

T.RANDOM

Ein Angreifer ist in der Lage, Systemsicherheitsinformationen R.RANDOM zu erraten und kann TOE-Objekte erstellen oder modifizieren oder an der Kommunikation mit externen Systemen teilnehmen.

6.4 Beziehung zwischen Bedrohungen und Werten

Tabelle 2 bietet einen Überblick über die Beziehungen zwischen Wert, den zugehörigen Sicherheitsdimensionen und Bedrohungen. Für weitere Einzelheiten ist in den einzelnen Bedrohungen in den vorherigen Abschnitten nachzulesen.

Tabelle 2

Wert	Sicherheitsdimensionen	Bedrohungen
R.Signing_Key_Id	Integrität	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Authorisation_Data	Integrität	T.AUTHORISATION_DATA_UPDATE
	Vertraulichkeit	T.AUTHORISATION_DATA_UPDATE T.AUTHORISATION_DATA_DISCLOSE
R.SVD	Integrität	T.SVD_FORGERY T.ADMIN_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
R.DTBS/R	Integrität	T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY
	Vertraulichkeit	T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY
	Ursprung Authentifizierung	T.DTBSR_FORGERY
R.SAD	Integrität	T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION T.SAP_BYPASS T.SAP_REPLAY T.SAD_FORGERY
	Vertraulichkeit	T.AUTHENTICATION_SIGNER_IMPERSONATION T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrität	T.SIGNATURE_FORGERY
R.Audit	Integrität	T.AUDIT_ALTERATION
R.Signer	Integrität	T.ENROLMENT_SIGNER_IMPERSONATION

Wert	Sicherheitsdimensionen	Bedrohungen
R.Reference_Signer_Authentication_Data	Integrität	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTHENTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Vertraulichkeit	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTHENTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Privileged_User	Integrität	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.Reference_Privileged_User_Authentication_Data	Integrität	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
	Vertraulichkeit	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.RANDOM	Integrität	T.RANDOM
	Vertraulichkeit	T.RANDOM
R.TSF_DATA	Integrität	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

6.5 Organisatorische Sicherheitsrichtlinien

Das TOE hat die folgenden organisatorischen Sicherheitsrichtlinien (OSP) als Sicherheitsregeln, Verfahren, Praktiken oder Richtlinien, die von einer Organisation den eigenen Tätigkeiten auferlegt werden, zu erfüllen.

OSP.TSP_AUDITED

TSP, die SSA und TOE umsetzen, sollten ein qualifizierter TSP nach Artikel 3 (20) der Verordnung (EU) Nr. 910/2014 eIDAS sein und sollten auf die Einhaltung der Anforderungen für TSP, die von eIDAS auferlegt werden, überprüft werden.

OSP.AUTH_DATA

Das SAP muss so konzipiert sein, dass die Aktivierung des Unterzeichnungsschlüssels in der alleinigen Kontrolle des Unterzeichners, mit einem hohen Grad an Sicherheit, liegt. Wenn SAD vom TOE empfangen werden, muss sichergestellt werden, dass die SAD unter der alleinigen Kontrolle des Unterzeichners durch Mittel in seinem Besitz übermittelt wurden.

OSP.RANDOM

Das TOE muss zufällige Zahlen generieren können, die eine spezifische Qualitätsmetrik erfüllen. Diese zufälligen Zahlen müssen sich zur Verwendung als Schlüssel, Authentifizierungs-/Autorisierungsdaten oder Ursprungsdaten für einen weiteren Generator für zufällige Zahlen eignen, der für diese Zwecke verwendet wird.

OSP.CRYPTO

Das TOE darf nur Algorithmen, Algorithmusparameter und Schlüssellängen verwenden, die von anerkannten Stellen als für TPSs geeignet befürwortet werden. Dies beinhaltet die Generierung von zufälligen Zahlen, Unterzeichnungsschlüsselpaaren und Signaturen sowie die Integrität und Vertraulichkeit der TOE-Werte.

Anwendungshinweis 21

Für kryptographische Algorithmen innerhalb der Europäischen Union sind diese wie in eIDAS angegeben und eine exemplarische Liste von Algorithmen und Parametern ist in ETSI/TS 119 312 oder SOGIS zur Verfügung gestellt.

6.6 Annahmen

A.PRIVILIGED_USER

Es wird angenommen, dass alle Mitarbeiter, die das TOE verwalten, vertrauenswürdig und kompetent sind und über die Ressourcen und Fähigkeiten verfügen, die für diese Aufgabe erforderlich sind und entsprechend für die Aktivitäten in ihrer Verantwortung geschult sind.

A.SIGNER_ENROLMENT

Der Unterzeichner sollte registriert sein und Zertifikate müssen verwaltet werden, in Übereinstimmung mit den Vorschriften, die in eIDAS angegeben sind. Anleitungsspezifikationen sind z. B. in EN 319411-1 angegeben oder, für qualifizierte Zertifikate, z. B. in EN 319411-2.

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

Es wird angenommen, dass der Unterzeichner seine Authentifizierungsfaktoren nicht offenlegt.

A.SIGNER_DEVICE

Es wird angenommen, dass das Gerät und die SIC, die vom Unterzeichner zur Interaktion mit der SSA und dem TOE verwendet werden, unter der Kontrolle des Unterzeichners für die Signatur stehen, d. h. gegen bössartige Codes geschützt sind.

A.CA

Es wird angenommen, dass der TSP, das Unterzeichnungszertifikate ausstellt, die Anforderungen für TSPs, wie sie in eIDAS definiert sind oder, für qualifizierte Zertifikate, die Anforderungen für qualifizierte TSPs, wie sie in eIDAS definiert sind, erfüllt.

A.ACCESS_PROTECTED

Es wird angenommen, dass das TOE in einer geschützten Umgebung betrieben wird, die physisch den Zugriff auf das TOE auf autorisierte privilegierte Anwender beschränkt. Die TOE-Software- und Hardware-Umgebung (einschließlich Client-Anwendungen) wird von privilegierten Anwendern in einem sicheren Status installiert und aufrechterhalten, der die spezifischen Risiken, die für die Umsetzungsumgebung gelten, mildert.

Es wird angenommen, dass jedes Audit, das vom TOE generiert wird, nur von autorisierten Mitarbeitern in einer physisch sicheren Umgebung behandelt wird. Die Mitarbeiter, die diese Tätigkeiten ausführen, sollten im Rahmen der errichteten Praktiken handeln.

Es wird angenommen, dass jedes vom TOE generierte Audit nicht zulässt, dass Unterzeichnungsschlüssel verwendet werden und dass alle Informationen, die benötigt werden, um einen Unterzeichnungsschlüssel zu aktivieren, in Integrität und Vertraulichkeit geschützt bleiben.

A.SEC_REQ

Es wird angenommen, dass der TSP eine Betriebsumgebung nach den Sicherheitsanforderungen für SCAL2, definiert in prEN 419241-1:2017, errichtet.

7 Sicherheitsziele

7.1 Allgemeines

Dieser Abschnitt bezeichnet und definiert die Sicherheitsziele für das TOE und seine Betriebsumgebung.

Diese Sicherheitsziele spiegeln die angegebene Absicht wieder, begegnen den identifizierten Bedrohungen und berücksichtigen die Annahmen.

7.2 Sicherheitsziele für das TOE

Die folgenden Sicherheitsziele beschreiben die Sicherheitsfunktionen, die vom TOE zur Verfügung gestellt werden müssen.

7.2.1 Registrierung

OT.SIGNER_PROTECTION

Das TOE muss sicherstellen, dass mit R.Signer assoziierte Daten in Integrität und gegebenenfalls in Vertraulichkeit geschützt werden.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

Das TOE muss Signaturauthentisierungsdaten, R.Reference_Signer_ Authentication_Data, als Teil von R.Signer sicher handhaben können.

OT.SIGNER_KEY_PAIR_GENERATION

Das TOE muss das kryptographischen Modul sicher verwenden können, um Unterzeichner-Unterzeichnungsschlüsselpaare zu generieren und R.Signing_Key_Id und R.SVD R.Signer zuzuweisen.

OT.SVD

Das TOE muss sicherstellen, dass die R.SVD nicht modifiziert werden bevor sie zertifiziert sind.

Anwendungshinweis 22

Es wird erwartet, dass die R.SVD innerhalb des TOE mit R.Signer verknüpft werden. Das Ziel ist sicherzustellen, dass Signaturprüfdaten nicht modifiziert werden können.

7.2.2 Anwenderverwaltung

OT.PRIVILEGED_USER_MANAGEMENT

Das TOE muss sicherstellen, dass jede Modifizierung an R.Privileged_User und R.Reference_Privileged_User_Authentication_Data unter der Kontrolle eines privilegierten Anwenders durchgeführt wird.

OT.PRIVILEGED_USER_AUTHENTICATION

Das TOE muss sicherstellen, dass ein Administrator mit einem privilegierten Anwender authentifiziert wird, bevor eine Handlung am TOE durchgeführt wird.

OT.PRIVILEGED_USER_PROTECTION

Das TOE muss sicherstellen, dass mit R.Privileged_User assoziierte Daten in Integrität und gegebenenfalls in Vertraulichkeit geschützt werden.

OT.SIGNER_MANAGEMENT

Das TOE muss sicherstellen, dass jede Modifizierung an R.Signer, R.Reference_Signer_Authentication_Data, R.Signing_Key_Id und R.SVD unter der Kontrolle des Unterzeichners oder privilegierten Anwenders durchgeführt wird.

7.2.3 Nutzung

OT.SAD_VERIFICATION

Das TOE muss die SAD prüfen. Das heißt, es muss prüfen, dass eine Verknüpfung zwischen den SAD-Elementen besteht und sicherstellen, dass der Unterzeichner wirksam authentifiziert ist.

Anwendungshinweis 23

Wenn das TOE Autorisierungsdaten von Authentifizierungsdaten in den SAD ableitet und diese verwendet, um den Unterzeichnungsschlüssel im kryptographischen Modul zu aktivieren, kann diese Funktion von den Kontrollen, die vom kryptographischen Modul zur Verfügung gestellt werden, abhängen.

Anwendungshinweis 24

Die Anforderungen für die Authentifizierung sind in prEN 419241-1:2017, SRA_SAP.1.1 beschrieben.

OT.SAP

Das TOE muss das serverseitige Endgerät eines Signaturaktivierungsprotokolls (SAP) implementieren, das Folgendes zur Verfügung stellt:

- Unterzeichner-Authentifizierung;
- Integrität der übertragenen SAD;
- Vertraulichkeit von mindestens der Elemente der SAD, die sensible Informationen enthalten;
- Schutz gegen Wiederverwendung, Umgehung und Betrug.

Anwendungshinweis 25

Von der Unterzeichner-Authentifizierung wird angenommen, dass sie für qualifizierte Signaturen nach prEN 419241-1:2017, SCAL.2 durchgeführt wird. Das heißt, die Unterzeichner-Authentifizierung kann auf eine der folgenden Art und Weisen ausgeführt werden:

- Direkt über das SAM. In diesem Fall überprüft das SAM den/die Authentifizierungsfaktor/en des Unterzeichners.
- Indirekt über das SAM. In diesem Fall, ein externer Authentifizierungsdienst als Teil von TW4S oder eine beauftragte Partei, die den/die Authentifizierungsfaktor/en des Unterzeichners prüfen und eine Erklärung ausstellen, dass der Unterzeichner authentifiziert wurde. Das SAM muss die Erklärung prüfen.
- Eine Kombination der beiden direkten oder indirekten Schemata.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION

Das TOE muss sicherstellen, dass Signatur-Authentisierungsdaten gegen Angriffe bei der Übertragung an das TOE geschützt sind, die deren Nutzung für die Authentifizierung beeinträchtigen würden.

OT.DTBSR_INTEGRITY

Das TOE muss sicherstellen, dass die R.DTBS/R bei der Übertragung an das TOE in Integrität geschützt sind.

OT.SIGNATURE_INTEGRITY

Das TOE muss sicherstellen, dass eine Signatur innerhalb des TOE nicht modifiziert werden kann.

7.2.4 System

OT.ADMIN_AUTHENTICATION

Das TOE muss sicherstellen, dass das TOE einen privilegierten Anwender authentifiziert, wenn der privilegierte Anwender eine TOE-Aktion ausführt.

Anwendungshinweis 26

Der Ausnahmefall dieses Ziels ist, wenn der erste (Satz von) privilegierte Nutzer(n) als Teil der System-initialisierung erstellt wird.

OT.RANDOM

Generierte zufällige Zahlen, die vom TOE zur Verwendung als Schlüssel, in Protokollen oder Ursprungsdaten für einen anderen Zufallsgenerator von Zahlen, der für diese Zwecke verwendet wird, genutzt werden, müssen eine definierte Qualitätsmetrik erfüllen, um sicherzustellen, dass die zufälligen Zahlen nicht vorhersehbar sind und über ausreichend Entropie verfügen.

OT.SYSTEM_PROTECTION

Das TOE muss sicherstellen, dass die Modifizierung von R.TSF_DATA vom privilegierten Anwender autorisiert wird und dass unautorisierte Modifizierung erkannt werden kann.

Anwendungshinweis 27

Die Erkennung von unautorisierten Änderungen an R.TSF_DATA ist nur relevant, wenn diese im Ganzen oder teilweise außerhalb des TOE gespeichert werden.

OT.AUDIT_PROTECTION

Das TOE muss sicherstellen, dass Modifizierungen an R.AUDIT erkannt werden können.

7.3 Sicherheitsziele für die Betriebsumgebung

7.3.1 Allgemeines

OE.SVD_AUTHENTICITY

Die Betriebsumgebung muss sicherstellen, dass die Integrität der Signaturprüfdaten bei der Übertragung außerhalb des TOE oder des CA gewahrt bleibt.

OE.CA_REQUEST_CERTIFICATE

Die Betriebsumgebung muss ein Zertifikat inklusive Signaturprüfdaten, Unterzeichnerinformationen und CA-Signatur erstellen.

Die Betriebsumgebung muss einem Prozess für die Anforderung eines Zertifikats verwenden, einschließlich Signaturprüfdaten, Unterzeichner Informationen und CA-Signatur, und zwar auf eine Art und Weise, die belegt, dass der Unterzeichner die Kontrolle über den Unterzeichnungsschlüssel hat, der mit den Signaturprüfdaten, die zur Zertifizierung vorgelegt werden, assoziiert ist. Die Integrität der Anforderung muss geschützt sein.

OE.CERTIFICATE_VERIFICATION

Die Betriebsumgebung muss prüfen, dass das Zertifikat für die R.SVD die R.SVD enthält.

OE.SIGNER_AUTHENTICATION_DATA

Die Verwaltung von Daten von Unterzeichner-Authentifizierungsfaktoren außerhalb des TOE muss auf sichere Weise ausgeführt werden.

OE.DELEGATED_AUTHENTICATION

Wenn das TOE die delegierte Authentifizierung unterstützt oder für deren Verwendung konfiguriert ist, MUSS der TSP sicherstellen, dass alle Anforderungen in prEN 419241-1:2017, SRA_SAP.1.1 erfüllt sind.

Außerdem sollte der TSP sicherstellen, dass:

- die externe Partei alle relevanten Anforderungen dieser Norm und die Anforderungen für die Registrierung nach der Verordnung (EU) Nr. 910/2014 eIDAS 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 Verordnung (EU) Nr. 910/2014 eIDAS verwendet und
- wenn der Unterzeichner nur unter Verwendung einer delegierten Partei authentifiziert wird, muss der geheime Schlüssel, der für die Authentifizierung der delegierten Partei gegenüber dem TOE verwendet wird, in einem zertifizierten kryptographischen Modul, in Übereinstimmung mit der Anforderung wie in prEN 419241-1:2017, SRG_KM.1.1 definiert, integriert sein.

OE.DEVICE

Das Gerät, Computer/Tablett/Smartphone, das die SIC enthält und vom Unterzeichner für die Interaktion mit dem TOE verwendet wird, muss gegen schädliche Codes geschützt sein. Es muss unter Verwendung der SIC als lokalen Teil des SAP teilnehmen und kann die SAD wie in prEN 419241-1:2017 beschrieben berechnen. Es kann verwendet werden, um das zu unterzeichnende Dokument anzuzeigen.

OE.ENV

TSP, die SSA und TOE umsetzen, sollte ein qualifizierter TSP nach Artikel 3 (20) der Verordnung (EU) Nr. 910/2014 eIDAS sein und sollte auf die Einhaltung der Anforderungen für TSP, die von eIDAS auferlegt werden, überprüft werden.

Das TOE muss in einer geschützten Umgebung betrieben werden, die physisch den Zugriff auf das TOE auf autorisierte privilegierte Anwender beschränkt. Die TOE-Software- und Hardware-Umgebung (einschließlich Client-Anwendungen) muss von Administratoren in einem sicheren Status installiert und aufrechterhalten, der die spezifischen Risiken, die für die Umsetzungsumgebung gelten, mildert, einschließlich (wenn anwendbar):

- Schutz gegen Verlust oder Diebstahl des TOE oder all seiner extern gespeicherten Werte;
- Prüfungen, um Eingriffe (einschließlich Zugriffsversuche auf Seitenkanäle oder auf Verbindungen zwischen physisch getrennten Teilen des TOE oder Teilen des Hardware-Geräts) zu verhindern und zu erkennen;
- Schutz gegen die Möglichkeit von Angriffen basierend auf Emanationen aus dem TOE (z. B. Elektromagnetische Emanationen) in Übereinstimmung mit den für die Betriebsumgebung beurteilten Risiken;
- Schutz gegen unautorisierte Software- und Konfigurationsänderungen auf dem TOE und dem Hardware-Gerät;
- Schutz auf einer auf allen Instanzen des TOE, die dieselben Werte beinhalten, gleichwertigen Ebene (z. B. wenn ein Schlüssel als Backup in mehr als einer Instanz des TOE vorhanden ist).

OE.CRYPTOMODULE_CERTIFIED

Wenn das TOE als lokale Anwendung innerhalb derselben physischen Grenze wie das kryptographische Modul wie definiert in prEN 419221-5:2016 implementiert ist, beruht das TOE auf dem kryptographischen Modul, um eine eingriffsgeschützte Umgebung und kryptographische Funktionalität und die Generierung von Zufallszahlen zur Verfügung zu stellen.

Wenn das TOE innerhalb einer separaten physischen Grenze implementiert ist, beruht das TOE auf dem kryptographischen Modul für kryptographische Funktionalität und die Generierung von Zufallszahlen.

Anwendungshinweis 28

Im Falle, dass das ST mit diesem PP und prEN 419221-5:2016 konform geht, wie im PP Abschnitt Anspruch beschrieben, deckt die Zertifizierung des ST diese Anforderung für die Betriebsumgebung ab.

OE.TW4S_CONFORMANT

Das TOE muss von einem qualifizierten TSP in einer Betriebsumgebung betrieben werden, die mit prEN 419241-1:2017 konform geht.

7.3.2 Definition Sicherheitsproblem und Sicherheitsziele

Die folgenden Tabellen bilden die Sicherheitsziele mit der Definition des Sicherheitsproblems ab.

TOE Sicherheitsziele und Bedrohungen.

Tabelle 3

	Registrierung	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD
Registrierung					
T.ENROLMENT_SIGNER_IMPERSONATION			X		
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		X	X		
T.SVD_FORGERY				X	X
Unterzeichner-Verwaltung					
T.ADMIN_IMPERSONATION					
T.MAINTENANCE_AUTHENTICATION_DISCLOSE			X		
Nutzung					
T.AUTHENTICATION_SIGNER_IMPERSONATION					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X		
T.SAP_BYPASS					
T.SAP_REPLAY					
T.SAD_FORGERY					
T.SIGNATURE_REQUEST_DISCLOSURE					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
System					
T.AUTHORISATION_DATA_UPDATE					
T.AUTHORISATION_DATA_DISCLOSE					
T.CONTEXT_ALTERATION					
T.AUDIT_ALTERATION					
T.RANDOM					

Tabelle 4

	Unterzeichner-Verwaltung	OT.PRIVILEGED_USER_AUTHENTICATION	OT.SIGNER_MANAGEMENT	System	OT.ADMIN_AUTHENTICATION	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
Registrierung								
T.ENROLMENT_SIGNER_IMPERSONATION			X					
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED								
T.SVD_FORGERY								
Unterzeichner-Verwaltung								
T.ADMIN_IMPERSONATION		X	X					
T.MAINTENANCE_AUTHENTICATION_DISCLOSE								
Nutzung								
T.AUTHENTICATION_SIGNER_IMPERSONATION								
T.SIGNER_AUTHENTICATION_DATA_MODIFIED								
T.SAP_BYPASS								
T.SAP_REPLAY								
T.SAD_FORGERY								
T.SIGNATURE_REQUEST_DISCLOSURE								
T.DTBSR_FORGERY								
T.SIGNATURE_FORGERY								
System								
T.PRIVILEGED_USER_INSERTION					X			
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION					X			
T.AUTHORISATION_DATA_UPDATE							X	
T.AUTHORISATION_DATA_DISCLOSE							X	
T.CONTEXT_ALTERATION							X	
T.AUDIT_ALTERATION								X
T.RANDOM						X		

Tabelle 5

	Nutzung	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY
Registrierung						
T.ENROLMENT_SIGNER_IMPERSONATION						
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED						
T.SVD_FORGERY						
Unterzeichner-Verwaltung						
T.ADMIN_IMPERSONATION						
T.MAINTENANCE_AUTHENTICATION_DISCLOSE						
Nutzung						
T.AUTHENTICATION_SIGNER_IMPERSONATION		X				
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X	X		
T.SAP_BYPASS			X			
T.SAP_REPLAY			X			
T.SAD_FORGERY			X	X		
T.SIGNATURE_REQUEST_DISCLOSURE						
T.DTBSR_FORGERY					X	
T.SIGNATURE_FORGERY						X
System						
T.PRIVILEGED_USER_INSERTION						
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION						
T.AUTHORISATION_DATA_UPDATE						
T.AUTHORISATION_DATA_DISCLOSE						
T.CONTEXT_ALTERATION						
T.AUDIT_ALTERATION						

TOE Sicherheitsziele und organisatorische Sicherheitsrichtlinien.

Tabelle 6

	Registrierung	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OT.RANDOM
OSP.TSP_AUDITED			X			
OSP.AUTH_DATA						
OSP.RANDOM						X

Bedrohungen und Sicherheitsziele für die Umgebung.

Tabelle 7

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Registrierung							
T.ENROLMENT_SIGNER_IMPERSONATION							X
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED			X	X			
T.SVD_FORGERY	X	X					
Unterzeichner-Verwaltung							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Nutzung							
T.AUTHENTICATION_SIGNER_IMPERSONATION							
T.SIGNER_AUTHENTICATION_DATA_MODIFIED							
T.SAP_BYPASS				X			
T.SAP_REPLAY				X			
T.SAD_FORGERY			X	X			
T.SIGNATURE_REQUEST_DISCLOSURE				X			
T.DTBSR_FORGERY				X			
T.SIGNATURE_FORGERY							
System							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Organisatorische Sicherheitsrichtlinien und Sicherheitsziele für die Umgebung und Annahmen und Sicherheitsziele für die Umgebung.

Tabelle 8

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S_CONFORMANT
Organisatorische Sicherheitsrichtlinien							
OSP.TSP_AUDITED							X
OSP.CRYPTO						X	
OSP.AUTH_DATA				X			
Annahmen							
A.PRIVILEGED_USER							X
A.SIGNER_ENROLMENT					X		
A.SIGNER_AUTHENTICATION_DATA_PROTECTION			X				
A.SIGNER_DEVICE				X			
A.CA		X					
A.ACCESS_PROTECTED					X		
A.SEC_REQ							X

7.3.3 Begründung für die Sicherheitsziele

Dieser Abschnitt bietet eine Begründung der Sicherheitsziele und deckt jede Bedrohung, jede organisatorische Sicherheitsrichtlinie und Annahme ab.

7.3.3.1 Bedrohungen und Ziele

T.ENROLMENT_SIGNER_IMPERSONATION wird abgedeckt von OT.SIGNER_MANAGEMENT, das verlangt, dass der Unterzeichner sicher erstellt wird.

Dies ist ebenfalls von OT.REFERENCE_SIGNER_AUTHENTICATION_DATA abgedeckt, das verlangt, dass das TOE in der Lage ist, Unterzeichner-Authentisierungsdaten dem Unterzeichner zuzuweisen.

Dies ist ebenfalls von OE.TW4S_CONFORMANT abgedeckt, da dies verlangt, dass Unterzeichner Informationen nach besten Praktiken gehandhabt werden, wenn der Unterzeichner registriert ist.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED wird abgedeckt von OT.REFERENCE_SIGNER_AUTHENTICATION_DATA, das verlangt, dass Authentisierungsdaten sicher gehandhabt werden.

Dies ist ebenfalls von OT.SIGNER_PROTECTION abgedeckt, das verlangt, dass die Attribute, darunter Unterzeichner-Authentisierungsdaten, in Integrität und gegebenenfalls in Vertraulichkeit geschützt sind.

Dies ist ebenfalls von OE.SIGNER_AUTHENTICATION_DATA abgedeckt, das verlangt, dass der Unterzeichner diese Authentisierungsdaten geheim hält.

Dies ist ebenfalls von OE.DEVICE abgedeckt, das verlangt, dass das vom Unterzeichner verwendete Gerät die Authentisierungsdaten nicht offen legt.

T.SVD_FORGERY ist abgedeckt von OT.SIGNER_KEY_PAIR_GENERATION, das ein kryptographisches Modul für die Generierung des Unterzeichnerschlüsselpaares verlangt.

Dies ist ebenfalls von OT.SVD abgedeckt, das verlangt, dass die SVD geschützt werden, während sie sich innerhalb des TOE befinden.

Dies ist ebenfalls von OE.SVD_AUTHENTICITY abgedeckt, das verlangt, dass die Umgebung die SVD während der Übertragung vom TOE an das CA schützt.

Dies ist ebenfalls von OE.CA_REQUEST_CERTIFICATE abgedeckt, das von der CA verlangt, ein Zertifikat auszustellen, das die Signaturprüfdaten enthält.

T.ADMIN_IMPERSONATION ist abgedeckt von OT.SIGNER_MANAGEMENT und OT.PRIVILEGED_USER_AUTHENTICATION, das verlangt, dass alle Änderungen an der Unterzeichner-Darstellung und den Attributen auf autorisierte Weise ausgeführt werden.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE wird abgedeckt von OT.REFERENCE_SIGNER_AUTHENTICATION_DATA, das verlangt, dass Authentisierungsdaten sicher gehandhabt werden.

T.AUTHENTICATION_SIGNER_IMPERSONATION wird abgedeckt von OT.SAD_VERIFICATION, das verlangt, dass das TOE die im SAP erhaltenen SAD prüft.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED wird abgedeckt von OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION, das verlangt, dass die SAD im SAP geschützt übermittelt werden.

Dies ist ebenfalls von OT.REFERENCE_SIGNER_AUTHENTICATION_DATA abgedeckt, das verlangt, dass Authentisierungsdaten sicher gehandhabt werden.

Dies ist ebenfalls von OT.SAP abgedeckt, das verlangt, dass die Integrität der SAD während der Übertragung im SAP geschützt wird.

T.SAP_BYPASS wird abgedeckt von OT.SAP, das verlangt, dass alle Schritte, einschließlich der SAD-Verifizierung des SAP abgeschlossen werden müssen.

Dies ist ebenfalls von OE.DEVICE abgedeckt, das verlangt, dass die SIC am SAP teilnimmt.

T.SAP_REPLAY wird abgedeckt von OT.SAP, das verlangt, dass das Signaturaktivierungsprotokoll im Ganzen oder teilweise gegen Wiederverwendung beständig sein muss.

Dies ist ebenfalls von OE.DEVICE abgedeckt, das verlangt, dass die SIC am SAP teilnimmt.

T.SIGNATURE_REQUEST_DISCLOSURE wird abgedeckt von OE.DEVICE das verlangt, dass die SIC am SAP teilnimmt.

T.SAD_FORGERY wird abgedeckt von OT.SAP, das verlangt, dass das TOE erkennen können muss, wenn die SAD während der Übertragung an das TOE modifiziert wurden.

Dies ist ebenfalls von OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION abgedeckt, das verlangt, dass die Signatur-Authentisierungsdaten während der Übertragung an das TOE geschützt sein müssen.

Dies ist ebenfalls von OE.SIGNER_AUTHENTICATION_DATA abgedeckt, das verlangt, dass der Unterzeichner seine Authentisierungsdaten schützt.

Dies ist ebenfalls von OE.DEVICE abgedeckt, das verlangt, dass das vom Unterzeichner verwendete Gerät korrekt im SAP teilnimmt, insbesondere darf das Gerät Authentisierungsdaten nicht offenlegen.

T.DTBSR_FORGERY wird abgedeckt von OT.DTBSR_INTEGRITY, das verlangt, dass die R.DTBS/R während der Übertragung an das TOE in Integrität geschützt sind.

Dies ist ebenfalls von OE.DEVICE abgedeckt, das verlangt, dass die SIC am SAP teilnimmt.

T.SIGNATURE_FORGERY wird abgedeckt von OT.SIGNATURE_INTEGRITY, das verlangt, dass die Signatur innerhalb des TOE in Integrität geschützt ist.

T.PRIVILEGED_USER_INSERTION wird abgedeckt von OT.ADMIN_AUTHENTICATION.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION wird abgedeckt von OT.ADMIN_AUTHENTICATION.

T.AUTHORISATION_DATA_UPDATE wird abgedeckt von OT.SYSTEM_PROTECTION, das verlangt, dass alle unautorisierten Modifizierungen an der TOE-Konfiguration entdeckt werden können.

T.AUTHORISATION_DATA_DISCLOSE wird abgedeckt von OT.SYSTEM_PROTECTION, das verlangt, dass alle unautorisierten Modifizierungen an der TOE-Konfiguration entdeckt werden können.

T.CONTEXT_ALTERATION wird abgedeckt von OT.SYSTEM_PROTECTION, das verlangt, dass alle unautorisierten Modifizierungen an der TOE-Konfiguration entdeckt werden können.

T.AUDIT_ALTERATION wird abgedeckt von OT.AUDIT_PROTECTION, das verlangt, dass alle Audit-Modifizierungen entdeckt werden können.

T.RANDOM wird abgedeckt von OT.RANDOM.

7.3.3.2 Organisatorische Sicherheitsrichtlinien und Ziele

OSP.TSP_AUDITED wird abgedeckt von OT.SIGNER_MANAGEMENT, das verlangt, dass das TOE eine Unterzeichnerdarstellung sicher erstellen kann.

Dies ist ebenfalls von OE.SIGNER_AUTHENTICATION_DATA abgedeckt, das verlangt, dass der Unterzeichner seine Signatur-Authentisierungsdaten auf sichere Weise handhabt.

OSP.AUTH_DATA wird abgedeckt von OE.DEVICE, das verlangt, dass das Gerät korrekt im SAP teilnimmt.

OSP.RANDOM wird abgedeckt von OT.RANDOM.

OSP.CRYPTO wird abgedeckt von OE.CRYPTOMODULE_CERTIFIED.

7.3.3.3 Annahmen und Ziele

A.PRIVILEGED_USER wird abgedeckt von OE.TW4S_CONFORMANT, das verlangt, dass der Administrator des TOE geschult sein muss.

A.SIGNER_ENROLMENT wird abgedeckt von OE.ENV, das verlangt, dass der TSP überprüft werden muss.

A.SIGNER_AUTHENTICATION_DATA_PROTECTION wird abgedeckt von OE.SIGNER_AUTHENTICATION_DATA, das verlangt, dass der Unterzeichner seine Authentisierungsdaten schützt.

A.SIGNER_DEVICE wird abgedeckt von OE.DEVICE, das verlangt, dass das Gerät des Unterzeichners gegen schädliche Codes geschützt sein muss.

A.CA wird abgedeckt von OE.CA_REQUEST_CERTIFICATE, das verlangt, dass das CA Zertifikate erstellt, die die Signaturprüfdaten enthalten.

A.ACCESS_PROTECTED wird abgedeckt von OE.ENV, das verlangt, dass das TOE in einer Umgebung mit physischen Zugriffskontrollen betrieben wird.

A.SEC_REQ wird abgedeckt von OE.TW4S_CONFORMANT, das verlangt, dass das System, in dem das TOE betrieben wird, mit prEN 419241-1:2017 konform geht.

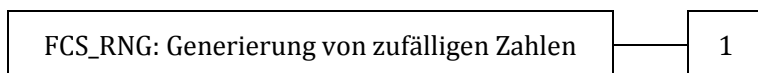
8 Erweiterte Komponenten Definitionen — Generierung von zufälligen Zahlen (FCS_RNG)

Diese Familie beschreibt die funktionalen Anforderungen an die Generierung von zufälligen Zahlen, die zu kryptographischen Zwecken verwendet werden.

Familienverhalten:

Diese Familie definiert die Qualitätsanforderungen für die Generierung von zufälligen Zahlen, die für die Verwendung für kryptographischen Zwecke bestimmt sind.

Komponenten-Einstufung:



Management: FCS_RNG.1

Es bestehen keine vorgesehenen Verwaltungsaktivitäten.

Audit: FCS_RNG.1

Es gibt keine Handlungen, die als zu prüfen definiert sind.

FCS_RNG.1	Generierung von zufälligen Zahlen
FCS_RNG.1.1	TSF muss einen [Auswahl: <i>physisch, nicht physisch wahr, deterministisch, hybrid physisch, hybrid deterministisch</i>] Zufallszahlengenerator zur Verfügung stellen, der Folgendes implementiert: [Zuweisung: <i>Liste der Sicherheitsfähigkeiten</i>].
FCS_RNG.1.2	TSF muss [Auswahl: <i>Bits, Achtbitzeichen, Zahlen</i> [Zuweisung: <i>Zahlenformat</i>]] zur Verfügung stellen, die [Zuweisung: <i>eine definierte Qualitätsmetrik</i>] erfüllen.

Anwendungshinweis 29

Ein physischer Zufallszahlengenerator (RNG) produziert eine Zufallszahl über eine Geräuschquelle, basierend auf physischen Zufallsprozessen. Ein nicht physischer wahrer RNG verwendet eine Geräuschquelle, basierend auf nicht physischen Zufallsprozessen, wie menschliche Interaktion (Tastendruck, Mausebewegung). Ein deterministischer RNG verwendet einen zufälligen Ursprung, um ein pseudozufälliges Ergebnis zu produzieren. Ein hybrider RNG kombiniert die Prinzipien von physischen und deterministischen RNGs, wobei ein hybrider physischer RNG mindestens die Menge an Entropie produziert, die das RNG-Ergebnis enthalten kann und der interne Zustand eines hybriden deterministischen RNG-Ergebnisses enthält frische Entropie, jedoch weniger als das Ergebnis des RNG enthalten kann.

9 Sicherheitsanforderungen

9.1 Übersicht SFRs

Dieser Abschnitt bietet eine Übersicht darüber, wie SFRs mit der Handhabung des TOE von Nutzungsszenarien und Unterzeichnerobjekten in Zusammenhang stehen.

Unterzeichnerobjekt

- FIA_ATD.1 und FIA_USB.1 verlangen, dass das Objekt R.Signer vom TOE aufrechterhalten wird.
- FDP_ITC.2/Signer beschreibt die Anforderungen für den Import des Objekts R.Signer.
- FDP_ETC.2/Signer beschreibt die Anforderungen für den Export des Objekts R.Signer.
- FDP_UIT.1 verlangt, dass das Objekt R.Signer beim Import und Export in Integrität geschützt ist.
- FPT_TDC.1 verlangt, dass das TOE in der Lage ist, die mit dem Objekt R.Signer zusammenhängenden Daten zu interpretieren, wenn diese mit SSA geteilt werden.
- FMT_MSA.1, FMT_MSA.2 und FMT_MSA.3 beschreiben Regeln für die Erstellung, Aufrechterhaltung und Nutzung des Objekts R.Signer sowie für dessen Werte.

Authentifizierung

- FIA_AFL.1 beschränkt die Anzahl der Authentifizierungsversuche
- FDP_UCT.1 stellt sicher, dass die Zugriffskontrolle und Informationsflussdaten auf vertrauliche Weise übertragen werden.
- FIA_UID.2 und FIA_UAU.1 verlangen, dass jeder Nutzer, bevor eine Handlung im Auftrag des Nutzers stattfinden kann, identifiziert und authentifiziert wird.
- FIA_UAU.5/Signer und FIA_UAU.5/Privileged User beschreiben die Liste der Authentifizierungsmechanismen

Unterzeichner erstellen

- FDP_ACC.1/Signer Creation unter Verwendung von FDP_ACF.1/Signer Creation beschreibt die Anforderungen an die Zugriffskontrolle für die Erstellung eines R.Signer-Objekts.
- FIA_USB.1 definiert die Autorisierungsregeln für die Erstellung neuer R.Signer-Objekte.

Unterzeichner-Schlüsselpaargenerierung

- FDP_ACC.1/Signer Key Pair Generation unter Verwendung von FDP_ACF.1/Signer Key Pair Generation beschreibt die Anforderungen an die Zugriffskontrolle für die Unterzeichnungs-Schlüsselpaargenerierung.
- FCS_CKM.1 beschreibt die Regeln dazu, wie Unterzeichnungs-Schlüsselpaare generiert werden

Unterzeichnerwartung

- FDP_ACC.1/Signer Maintenance unter Verwendung von FDP_ACF.1/Signer Maintenance beschreibt die Anforderungen an die Zugriffskontrolle für die Wartung des Objekts R.Signer.
- FCS_CKM.4 verlangt, dass Schlüssel sicher vernichtet werden.

Lieferung DTBS/R

- FDP_ACC.1/Supply DTBS/R unter Verwendung von FDP_ACF.1/Supply DTBS/R beschreibt die Anforderungen an die Zugriffskontrolle für einen privilegierten Anwender, um DTBS/R(s) zu liefern.

Signieren

- FDP_IFF.1/Signer und FDP_IFC.1/Signer beschreiben die Anforderungen an die Voraussetzungen, um eine Signatur ausführen zu können.
- FDP_UIT.1 verlangt, dass das Objekt R.SAD vor Modifizierung und Wiederverwendung geschützt ist.
- FDP_ACC.1/Signing unter Verwendung von FDP_ACF.1/Signing beschreibt die Anforderungen an die Zugriffskontrolle für die Unterzeichnung.
- FCS_COP.1 verlangt, dass das TOE kryptographische Tätigkeiten nach einer ST-spezifizierten Liste von Algorithmen durchführt.

Privilegiertes Anwenderobjekt

- FIA_ATD.1 und FIA_USB.1 verlangen, dass das Objekt R.Privileged User vom TOE aufrechterhalten wird.
- FDP_ITC.2/Privileged User beschreibt die Anforderungen an den Import des Objekts R.Privileged User.
- FDP_ETC.2/Privileged User beschreibt die Anforderungen an den Export des Objekts R.Privileged User.
- FDP_UIT.1 verlangt, dass das Objekt R.Privileged User beim Import und Export in Integrität geschützt ist.
- FPT_TDC.1 verlangt, dass das TOE in der Lage ist, das Objekt R.Privileged User zu interpretieren, wenn es mit einem vertrauenswürdigen IT-Produkt der SSA geteilt wird.
- FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 beschreiben Regeln für die Erstellung, Aufrechterhaltung und Nutzung des Objekts R.Privileged User sowie für dessen Werte.

Privilegierte Anwendererstellung

- FDP_ACC.1/Privileged User Creation unter Verwendung von FDP_ACF.1/Privileged User Creation beschreibt die Anforderungen an die Zugriffskontrolle für die Erstellung eines R.Privileged User-Objekts.
- FIA_USB.1 definiert die Autorisierungsregeln für die Erstellung neuer R.Privileged User-Objekte.