

DIN EN 419241-2

ICS 35.030

**Vertrauenswürdige Systeme, die Serversignaturen unterstützen –
Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur
Serversignierung;
Deutsche Fassung EN 419241-2:2019**

Trustworthy Systems Supporting Server Signing –
Part 2: Protection profile for QSCD for Server Signing;
German version EN 419241-2:2019

Systèmes fiables de serveur de signature électronique –
Partie 2: Profil de protection de QSCD pour la signature par serveur;
Version allemande EN 419241-2:2019

Gesamtumfang 79 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (EN 419241-2:2019) 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).

Deutsche Fassung

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

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

Systèmes fiables de serveur de signature électronique —
Partie 2: Profil de protection de QSCD pour
la signature par serveur

Diese Europäische Norm wurde vom CEN am 26. November 2018 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

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

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



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

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

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	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	7
4.3.1 Europäische Gesetzgebung	7
4.4 EVG: Übersicht	8
4.4.1 Allgemeines	8
4.4.2 EVG-Typ	10
4.4.3 EVG-Lebenszyklus	10
4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des EVG	10
4.4.5 EVG-Umgebung: allgemeine Übersicht	11
4.4.6 Verfügbare nicht EVG-bezogene Hardware/Software/Firmware	11
4.4.7 Wählbare Festlegung	12
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 Subjekte	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	18
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 den EVG	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
7.4	Definition des Sicherheitsproblems und Sicherheitsziele	28
7.5	Begründung für die Sicherheitsziele	33
7.5.1	Allgemeines	33
7.5.2	Bedrohungen und Ziele	33
7.5.3	Organisatorische Sicherheitsrichtlinien und Ziele	35
7.5.4	Annahmen und Ziele	36
8	Definitionen der erweiterten Komponenten	36
8.1	Klasse FCS: Kryptographische Unterstützung	36
8.1.1	Allgemeines	36
8.1.2	Generierung von zufälligen Zahlen (FCS_RNG).....	37
9	Sicherheitsanforderungen	38
9.1	Typographische Festlegungen.....	38
9.2	Subjekte, Objekte und Vorgänge.....	38
9.3	Übersicht SFRs.....	40
9.4	Sicherheitsfunktionsanforderungen.....	42
9.4.1	Sicherheitsaudit (FAU)	42
9.4.2	Kryptographische Unterstützung (FCS)	43
9.4.3	Anwenderdatenschutz (FDP)	45
9.4.4	Identifizierung und Authentifizierung (FIA)	59
9.4.5	Sicherheitsverwaltung (FMT)	61
9.4.6	Schutz der TSF (FPT)	65
9.4.7	Vertrauenswürdige Pfade/Kanäle (FTP).....	66
9.5	Sicherheitsbestätigungsanforderungen	68
10	Begründung	69
10.1	Begründung der Sicherheitsanforderungen	69
10.2	SFR-Abhängigkeiten	74
10.2.1	Allgemeines	74
10.3	Begründungen für SARs	76
	Literaturhinweise.....	77

Europäisches Vorwort

Dieses Dokument (EN 419241-2:2019) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

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

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

Dieses Dokument wurde im Rahmen eines Mandats erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone CEN erteilt haben.

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

Einleitung

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

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

Dieses Dokument gehört zur Normenreihe EN 419241, die aus den folgenden Teilen besteht:

- EN 419241-1: Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen;
- EN 419241-2: Dieses Dokument

Weitere Einzelheiten dieser Normenreihe können in EN 419241-1 gefunden werden.

Aufbau des Dokuments

Abschnitt 1 umfasst einleitendes Material für das Schutzprofil.

Abschnitt 2 beschreibt normative Verweisungen.

Abschnitt 3 beschreibt Begriffe.

Abschnitt 4 enthält die Einleitung.

Abschnitt 5 umfasst den Konformitätsanspruch.

Abschnitt 6 umfasst die Definition des Sicherheitsproblems. Er stellt die Werte, Bedrohungen, organisatorische Sicherheitsbestimmungen und Annahmen in Bezug auf den EVG dar.

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

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

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

Abschnitt 10 umfasst 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 Abschnitt mit Verweisungen wurde zur Verfügung gestellt, um Hintergrundmaterialien zu identifizieren.

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

1 Anwendungsbereich

Dieses Dokument spezifiziert ein Schutzprofil für ein Signatur-Aktivierungsmodul (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).

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

EN 419221-5, *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 EN 419241-1, EN 419221-5 und eIDAS Artikel 3 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

ANMERKUNG Die Begriffe aus Common Criteria sind in [CC1] angegeben.

3.1.1

Zertifikat

Zertifikat für elektronische Signatur, wie in eIDAS Artikel 3 definiert

3.1.2

beauftragte Partei

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

3.1.3

Wert der digitalen Signatur

Ergebnis eines Verschlüsselungsvorgangs, der den Signierschlüssel einbezieht

Anmerkung 1 zum Begriff: Innerhalb dieses Dokuments bezeichnen die Begriffe Siegel, Signatur, digitale Signatur oder digitales Siegel den Wert der digitalen Signatur.

3.1.4

einmaliger Signierschlüssel

Signierschlüssel, der auf Basis einer einzelnen Autorisierung erstellt, verwendet und verworfen wird, üblicherweise in Verbindung mit einer Einzelsitzungssignierung DTBS/R(s)

Anmerkung 1 zum Begriff: Im Gegensatz zu Signierschlüsseln, die in mehreren Signiersitzungen verwendet werden können.

3.2 Symbole und Abkürzungen

CA	Zertifizierungsstelle
CM	Kryptographisches Modul, zertifiziert nach [EN 419221-5]
CSR	Zertifizierungssignieranfrage
DTBS/R(s)	DTBS/R oder einen Satz an DTBS/R

4 Einleitung

4.1 Allgemeines

Dieser Abschnitt umfasst 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 „Schutzprofil-Übersicht“ fasst das PP in Erzählform zusammen. 4.4 „EVG: Übersicht“ fasst den EVG 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 eigenständige Übersicht 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	1.0
Autoren	WG17
Keywörter	Serversignatur

4.3 Schutzprofil-Übersicht

4.3.1 Europäische Gesetzgebung

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

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

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

4.4 EVG: Übersicht

4.4.1 Allgemeines

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

In diesem Dokument verwendet das TW4S ein kryptografisches Modul, um den Signierschlüssel zu generieren und den Wert der digitalen Signatur zu erstellen.

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

Der Zweck der Interaktion zwischen dem Gerät und der SSA ist, dass der Unterzeichner den Signierdienst der SSA verwendet. Der Signaturvorgang 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 Signierschlüssel und die zu unterzeichnenden Daten [DTBS/R(s)].

Um sicherzustellen, dass der Unterzeichner die alleinige Kontrolle über seine Signierschlüssel hat, muss der Signaturvorgang autorisiert werden. Dies erfolgt über ein Signaturaktivierungsmodul (SAM), das ein Ende des SAP handhaben, SAD prüfen und den Signierschlüssel 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 EN 419241-1 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 der TW4S oder eine beauftragte Partei, die den/die Authentifizierungsfaktor/en des Unterzeichners prüft und eine Erklärung ausstellt, 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 sich auf die Erklärung verlassen. In diesem PP bedeutet Unterzeichner-Authentifizierung, dass der Unterzeichner über eine der drei oben genannten Vorgehensweisen authentifiziert wurde.

Das SAM-Modul ist der EVG dieses PP. EVG und kryptographisches Modul, zertifiziert nach EN 419221-5, sind erforderlich, um ein QSCD zu erhalten.

Das Bild unten gibt einen Überblick über die Umgebung, in die der EVG 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 verwendet 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 Signierschlüssels innerhalb des kryptographischen Moduls autorisieren und einen Wert der digitalen Signatur erzeugen. Der Wert wird an die SSA zurückgesendet und kann weiter an die SCA oder die SIC geliefert werden. Aus Sicht des EVG dienen SSA und Benutzerschnittstelle als unterstützende Module, die Dokumente anzeigen und Kommunikationsnachrichten weiterleiten.

Der EVG generiert Prüfdatensätze für alle sicherheitsrelevanten Ereignisse und ist darauf angewiesen, dass die SSA die Prüfdatensätze speichert und die Zugriffskontrolle für sie zur Verfügung stellt.

TW4S ist auf andere Dienste angewiesen:

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

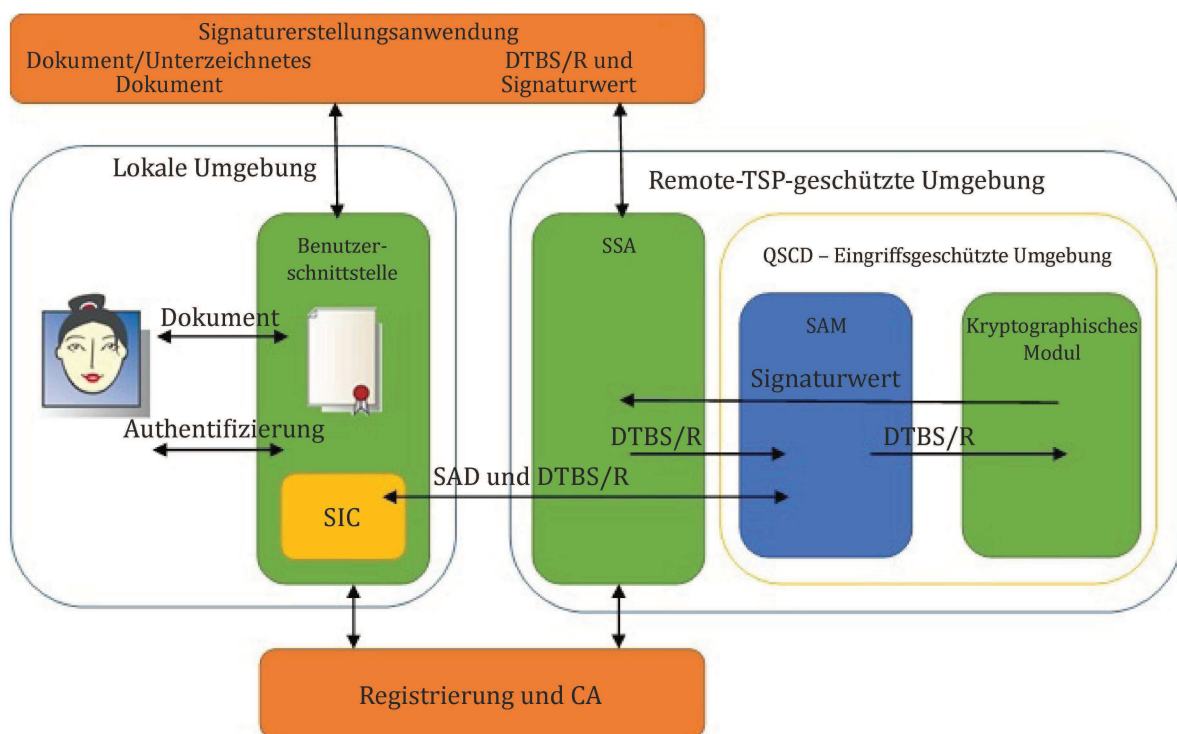


Bild 1

4.4.2 EVG-Typ

Der EVG 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 Signierschlüssel zur Verwendung in einem kryptographischen Modul zu aktivieren.

Der EVG und das kryptographische Modul sind gemeinsam ein QSCD.

4.4.3 EVG-Lebenszyklus

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

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

Lieferung: Der EVG wird vom EVG-Entwickler sicher an den TSP geliefert.

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

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

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

4.4.4 Nutzung und wesentliche Sicherheitsmerkmale des EVG

Die wesentlichen Sicherheitsmerkmale des EVG 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 Signierschlüssel und Signaturprüfdaten (SVD) unter Verwendung eines kryptographischen Moduls generieren und den Signierschlüsselbezeichner und die SVD einem Unterzeichner zuweisen.
 - Privilegierte Anwender oder Unterzeichner können einen Signierschlüsselbezeichner deaktivieren, der von einem Unterzeichner verwendet werden soll.

- Signaturvorgang
 - Privilegierte Anwender oder Unterzeichner können DTBS/R(s) zum Signieren vorlegen.
 - Die Verbindung zwischen der Unterzeichner-Authentifizierung, den DTBS/R(s) und dem Signierschlüsselbezeichner wird von den Signaturaktivierungsdaten (SAD) gehandhabt. Diese SAD werden mit dem EVG sicher unter Verwendung des Signaturaktivierungsprotokolls (SAP) ausgetauscht. Innerhalb des EVG werden die folgenden Aktionen durchgeführt:
 - Die SAD werden auf Integrität geprüft.
 - Die SAD werden darauf überprüft, dass sie die Unterzeichner-Authentifizierung, eine DTBS/R(s) und den Signierschlüsselbezeichner 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 mit den SAD verbunden.
 - Der Signierschlüsselbezeichner wird dem Unterzeichner zugewiesen.
 - Der EVG verwendet Autorisierungsdaten, um den Signierschlüssel innerhalb des kryptographischen Moduls zu aktivieren.
 - Der EVG verwendet das kryptographische Modul, um Signaturen zu erstellen.
- Der EVG generiert Prüfdatensätze für alle sicherheitsrelevanten Ereignisse und beruht darauf, dass die SSA die Prüfdatensätze speichert und die Zugriffskontrolle für sie zur Verfügung stellt.

Der EVG behandelt Datenwerte, wie in 6.1 angegeben.

4.4.5 EVG-Umgebung: allgemeine Übersicht

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

Vom EVG wird Folgendes erwartet:

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

4.4.6 Verfügbare nicht EVG-bezogene Hardware/Software/Firmware

Der EVG 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, zertifiziert nach EN 419221-5, das den Betrieb des EVG unterstützt.

4.4.7 Wählbare Festlegung

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

Tabelle 1

Option	Beschreibung
Einsatz	Der EVG kann in einem kryptographischen Modul oder in einem dafür bestimmten Hardware-Modul umgesetzt werden. Der ST-Autor muss besonders auf die SFRs FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_RNG.1, FPT_PHP.1, FPT_PHP.3 und FTP_ITC.1/CM achten, da diese SFRs je nach Einsatz unterschiedlich erfüllt werden können.

5 Konformitätsanspruch

5.1 CC-Konformitätsanspruch

Dieses Schutzprofil (PP) beansprucht konform zu den Common Criteria Teil 2 erweitert und Common Criteria Teil 3 zu sein und ist entsprechend den Common Criteria, Version 3.1 R4 [CC1], [CC2] und [CC3] geschrieben.

Die Sicherungsanforderung dieser Schutzprofils ist **EAL4 Erweitert**. Die Erweiterung ergibt sich 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 ST oder PP, das die Konformität mit diesem PP beansprucht.

6 Definition Sicherheitsproblem

6.1 Werte

Der EVG hat die folgenden Werte, die hinsichtlich Integrität und Vertraulichkeit, wie nachstehend beschrieben, geschützt werden müssen. Der EVG muss sicherstellen, dass, wann immer sich ein Wert außerhalb des EVG befindet, der EVG die notwendigen Verschlüsselungsvorgänge durchgeführt hat, um die Vertraulichkeit durchzusetzen, und erkennen kann, ob ein Wert verändert wurde. Die Zugriffskontrolle auf EVG-Werte außerhalb des EVG ist durch die Umgebung durchzusetzen.

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

Anwendungshinweis 1

Die Integrität und die Vertraulichkeit des Signierschlüssels und der Verknüpfung zwischen R.Signing_Key_Id und dem Signierschlüssel liegen in der Verantwortung des kryptographischen Moduls. Der EVG muss sicherstellen, dass nur der Unterzeichner den Signierschlüssel unter seiner alleinigen Kontrolle verwenden kann.

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

Anwendungshinweis 2

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

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

R.SVD: Signaturprüfdaten sind der öffentliche Teil, assoziiert mit dem Signierschlüssel, um die Prüfung der digitalen Signatur durchzuführen. Die R.SVD müssen hinsichtlich Integrität geschützt sein.

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

R.DTBS/R: Ein Datensatz, der an den EVG für die Erstellung der digitalen Signatur im Namen des Unterzeichners übermittelt wird. Der DTBS/R(s) wird an den EVG übermittelt. Die R.DTBS/R müssen hinsichtlich Integrität geschützt sein. Die Übertragung der DTBS/R(s) an den EVG 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 EN 419241-1 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 hinsichtlich Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 4

Wenn die SAD keine verschlüsselten Daten verlangen, gilt die Vertraulichkeitsanforderung als erfüllt. Der ST-Autor muss beschreiben, welcher Teil der SAD hinsichtlich 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 ein Zertifikat, ein Schlüsselbezeichner oder abgeleitete Informationen sein, die aus der Authentifizierung des Unterzeichners erhalten werden.

Einige Lösungen können einmalige Signierschlüssel verwenden, die innerhalb einer begrenzten Signiersitzung 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 Signiersitzungen mit dem EVG hat, oder um eine R.Signing_Key_Id abzuleiten, wenn der Schlüssel ein einmaliger Schlüssel ist. Am Ende der Sitzung wird der Signierschlüssel zuverlässig deaktiviert.

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

Der ST-Autor muss beschreiben, welche R.Signing_Key_Id für einen spezifischen EVG gilt.

R.Signature: Ist das Ergebnis des Signaturvorgangs und ist ein Wert einer digitalen Signatur. 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 hinsichtlich Integrität geschützt sein. Die R.Signature kann außerhalb des EVG unter Verwendung von R.SVD geprüft werden.

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

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

Anwendungshinweis 7

R.Signer muss nur innerhalb des EVG eindeutig sein. Es liegt nicht in der Verantwortung des EVG, eine Verbindung zwischen R.Signer und der Identität des Unterzeichners herzustellen. Der Unterzeichner gilt als der Besitzer des R.Signer-Objekts, das ihn innerhalb des EVG 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-Autor muss beschreiben, welcher Teil von R.Signer hinsichtlich Vertraulichkeit geschützt werden muss.

R.Reference_Signer_Authentication_Data: Dies ist der Datensatz, der vom EVG 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 EVG 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 hinsichtlich Integrität und Vertraulichkeit geschützt sein.

Anwendungshinweis 10

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

Anwendungshinweis 11

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

R.TSF_DATA: Dies ist der EVG-Konfigurationsdatensatz, der verwendet wird, um den EVG zu betreiben. Er muss hinsichtlich Integrität geschützt sein.

Anwendungshinweis 12

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

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

R.Reference_Privileged_User_Authentication_Data ist der Datensatz, der vom EVG zur Authentifizierung des privilegierten Anwenders verwendet wird. Er muss hinsichtlich 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-Autor muss beschreiben, welcher Teil von R.Reference_Privileged_User_Authentication_Data hinsichtlich Vertraulichkeit geschützt werden muss.

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

6.2 Subjekte

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

- Unterzeichner, dies ist die natürliche oder juristische Person, die den EVG durch das SAP verwendet, wo er die SAD zur Verfügung stellt und DTBS/R(s), unter Verwendung des eigenen Signierschlüssels im kryptographischen Modul, unterzeichnen kann.
- Privilegierter Anwender, dieser führt die administrativen Funktionen des EVG aus und ist in der Lage, dem EVG als Teil des Signaturvorgangs DTBS/R(s) zur Verfügung zu stellen.

Anwendungshinweis 14

Die Liste der in EN 419241-1:2018, 6.2.1.2, SRG M.1.2 beschriebenen Subjekte enthält mehr Rollen, da sie das gesamte T4WS abdeckt.

Der ST-Autor 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 EVG interagiert. Privilegierte Anwender können mit dem EVG direkt oder über die SSA interagieren. Wenn die SSA als ein Dienst administrative Funktionen ausführen kann, z. B. einen Unterzeichner erstellen, gilt sie in diesem PP als privilegierter Anwender.

Anwendungshinweis 16

Es wird erwartet, dass die Erstellung von Unterzeichnern, die Verwaltung von Referenz-Authentisierungsdaten eines Unterzeichners und die Generierung eines Signierschlüssels gemeinsam mit einer Registrierungsstelle (RA) ausgeführt wird, die einen Registrierungsdienst unter Verwendung der SSA, wie z. B. in [ETSI EN 319411-1] angegeben, zur Verfügung stellt.

6.3 Bedrohungen

6.3.1 Allgemeines

Die folgenden Bedrohungen sind für den EVG 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 als 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 EVG;
- durch Übertragung der falschen R.Reference_Signer_Authentication_Data von RA an EVG.

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 den EVG oder bei der Übertragung zwischen Unterzeichner und EVG 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 für die Umgebung für den Fall, dass die externe Authentifizierung vom EVG unterstützt wird.

T.SVD_FORGERY

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

Der Wert R.SVD ist bedroht.

Wenn sich die CA auf die vom EVG gesteuerte Generierung des Schlüsselpaares, wie in [ETSI EN 319411-1], 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 EVG an die RA oder die CA vorhanden sein. Vom SAM wird erwartet, ein CSR zu erzeugen.

Wenn die Registrierungsdienste des TSP, der ein Zertifikat erstellt, einen „Besitznachweis oder die Kontrolle des privaten Schlüssels“, der mit den SVD verbunden ist, verlangen, wie in [ETSI EN 319411-1], 6.3.1 a) angegeben, kann dieser Bedrohung ohne spezifische Maßnahmen innerhalb des EVG 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 den EVG mittels 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 EVG oder während der Instandhaltung 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 den EVG.

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

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 den EVG 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 EVG.

Der Wert R.Signature ist bedroht.

Anwendungshinweis 18

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 EVG 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 EVG 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 Signierschlüssel zu aktivieren.

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

Anwendungshinweis 19

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

T.AUTHORISATION_DATA_DISCLOSE

Ein Angreifer legt R.Authorisation_Data während der Aktualisierung offen und ist in der Lage, einen Signierschlüssel 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 EVG 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 EVG-Objekte erstellen oder modifizieren oder an der Kommunikation mit externen Systemen teilnehmen.

6.4 Beziehung zwischen Bedrohungen und Werten

Die folgende Tabelle bietet einen Überblick über die Beziehungen zwischen Wert, den zugehörigen Sicherheitseigenschaften und Bedrohungen. Weitere Einzelheiten können bei den einzelnen Bedrohungen in den vorherigen Abschnitten nachgelesen werden.

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
	Authentifizierung des Ursprungs	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.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrität	T.SIGNATURE_FORGERY
R.Audit	Integrität	T.AUDIT_ALTERATION

Wert	Sicherheitsdimensionen	Bedrohungen
R.Signer	Integrität	T.ENROLMENT_SIGNER_IMPERSONATION
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

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

OSP.RANDOM

Der EVG 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, der für diese Zwecke verwendet wird, eignen.

OSP.CRYPTO

Der EVG darf nur Algorithmen, Algorithmusparameter und Schlüssellängen verwenden, die von anerkannten Stellen als für TPSS geeignet befürwortet werden. Dies beinhaltet die Generierung von zufälligen Zahlen, Signierschlüsselpaaren und Signaturen sowie die Integrität und Vertraulichkeit der EVG-Werte.

Anwendungshinweis 20

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 119312] oder [SOGIS] zur Verfügung gestellt.

6.6 Annahmen

A.PRIVILEGED_USER

Es wird angenommen, dass alle Mitarbeiter, die den EVG 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 muss registriert sein und Zertifikate müssen, in Übereinstimmung mit den Vorschriften, die in [eIDAS] angegeben sind, verwaltet werden. Anleitungen, wie eine Registrierung und ein Zertifikatverwaltungssystem in Übereinstimmung mit [eIDAS] zu implementieren sind, 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 EVG verwendet werden, unter der Kontrolle des Unterzeichners für den Signaturvorgang stehen, d. h. gegen böartige Codes geschützt sind.

A.CA

Es wird angenommen, dass der qualifizierte TSP, der qualifizierte Zertifikate ausstellt, die relevanten Anforderungen für qualifizierte TSPs, wie sie in [eIDAS] definiert sind erfüllt.

A.ACCESS_PROTECTED

Es wird angenommen, dass der EVG in einer geschützten Umgebung betrieben wird, die den physischen Zugriff auf den EVG auf autorisierte privilegierte Anwender beschränkt. Die EVG-Software- und Hardware-Umgebung (einschließlich Client-Anwendungen) wird von privilegierten Anwendern in einem sicheren Zustand installiert und gewartet, der die spezifischen Risiken, die für die Einsatzumgebung gelten, mildert.

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

Es wird angenommen, dass in Fällen, in denen Kopien geschützter Daten durch den EVG außerhalb des EVG verwaltet werden, Client-Anwendungen und andere Stellen angemessenen Schutz für dieses Daten auf einem Niveau bieten müssen, das durch den Anwendungskontext und die Risiken der Einsatzumgebung erforderlich ist.