

DIN EN 419211-3

ICS 03.160; 35.040; 35.240.15

**Schutzprofile für sichere Signaturerstellungseinheiten –
Teil 3: Einheiten mit Schlüsselimport;
Deutsche Fassung EN 419211-3:2013**

Protection profiles for secure signature creation device –
Part 3: Device with key import;
German version EN 419211-3:2013

Profils de protection des dispositifs sécurisés de création de signature –
Partie 3: Dispositif avec import de clé;
Version allemande EN 419211-3:2013

Gesamtumfang 48 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 419211-3:2013) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

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

Deutsche Fassung

Schutzprofile für sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsseliport

Protection profiles for secure signature creation device —
Part 3: Device with key import

Profils de protection des dispositifs sécurisés de création de
signature —
Partie 3: Dispositif avec import de clé

Diese Europäische Norm wurde vom CEN am 14. September 2013 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 Management-Zentrum des CEN-CENELEC 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, 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: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Einführung in Schutzprofile.....	5
4.1 Schutzprofilreferenz	5
4.2 Überblick über das Schutzprofil.....	5
4.3 Überblick über den Evaluationsgegenstand.....	6
5 Konformität.....	11
5.1 CC-Konformität	11
5.2 Schutzprofil-Konformität, Paket-Konformität	11
5.3 Begründung der Konformität	12
5.4 Konformitätsangabe	12
6 Definition des Sicherheitsproblems	12
6.1 Zu schützende Werte, Benutzer und Bedrohungsagenten	12
6.2 Bedrohungen.....	13
6.3 Organisatorische Sicherheitsvorgaben	13
6.4 Annahmen	14
7 Sicherheitsziele.....	15
7.1 Sicherheitsziele für den EVG	15
7.2 Sicherheitsziele für die Einsatzumgebung	16
7.3 Begründung der Sicherheitsziele.....	19
8 Erweiterte Komponentendefinition	24
9 Sicherheitsanforderungen	25
9.1 Funktionale Sicherheitsanforderungen.....	25
9.2 Anforderungen an die Vertrauenswürdigkeit der Sicherheit	40
9.3 Begründung der Sicherheitsanforderungen	41
Literaturhinweise	46

Vorwort

Dieses Dokument (EN 419211-3:2013) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation, elektronische Signatur, maschinenlesbare Karten sowie zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2014, und etwaige entgegenstehende nationale Normen müssen bis April 2014 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt CWA 14169:2004.

Dieses Dokument wurde zur CEN-Umfrage als prEN 14169-3 vorgelegt.

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, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Diese Europäische Normenreihe legt Common Criteria Schutzprofile für sichere Signaturerstellungseinheiten fest und wird vom CEN/ISSS (ISSS: Information Society Standardization System, Normungssystem für die Informationsgesellschaft) als aktualisierte Fassung des CEN/ISSS Workshop Agreements CWA 14169:2004, Anhang B und Anhang C, zu Schutzprofilen sicherer Signaturerstellungseinheiten, „EAL 4+“, herausgegeben.

Diese Europäische Normenreihe besteht aus den folgenden Teilen:

- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*
- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Einheiten mit Schlüsselerzeugung*
- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsselimport*
- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung*
- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung*
- *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur sicheren Signaturerstellungsanwendung*

Bei der Erstellung dieses Dokuments als Schutzprofil (protection profile, PP) wurden die Regeln der Common Criteria Version 3.1 [2], [3] und [4] befolgt.

1 Anwendungsbereich

Diese Europäische Norm legt ein Schutzprofil für eine sichere Signaturerstellungseinheit, mit der Möglichkeit Signaturschlüssel zu importieren, fest: SSCD mit Schlüsselimport.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

prEN 14169-1:2011, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Akronyme und Begriffe nach prEN 14169-1:2011.

4 Einführung in Schutzprofile

4.1 Schutzprofilreferenz

Titel:	Schutzprofile für sichere Signaturerstellungseinheiten – Teil 3: Einheiten mit Schlüsselimport
Version:	1.0.2
Autor:	CEN/CENELEC (TC 224/WG 17)
Veröffentlichungsdatum:	2012-07-24
Registrierung:	BSI-CC-PP-0075
CC-Version:	3.1 Revision 3
Bearbeiter:	Arnold Abromeit, TÜV Informationstechnik GmbH
Allgemeiner Status:	final
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur, Schlüsselimport

4.2 Überblick über das Schutzprofil

Dieses Schutzprofil wurde vom CEN als eine Europäische Norm für Produkte zur Erstellung elektronischer Signaturen erstellt. Sie erfüllt die Anforderungen der Richtlinie¹⁾ 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über *gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*.

Nach Artikel 9 dieser Richtlinie kann die vorliegende Norm von der Europäischen Kommission im Amtsblatt der Europäischen Gemeinschaften als allgemein anerkannte Norm für Produkte zur Erstellung elektronischer Signaturen angegeben werden.

Dieses Schutzprofil beschreibt funktionale Sicherheitsanforderungen und Sicherheitsanforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (en: secure signature creation device, SSCD), die mit denen in Anhang III **der Richtlinie** übereinstimmen. Diese sichere Signaturerstellungseinheit ist der Evaluationsgegenstand (EVG) dieses Schutzprofils.

Die Mitgliedsstaaten der EU dürfen davon ausgehen, dass eine Übereinstimmung mit den in Anhang III **der Richtlinie** [1] festgelegten Anforderungen vorliegt, wenn ein Produkt zur Erstellung elektronischer Signaturen anhand eines Sicherheitsziels (en: security target, ST) evaluiert wurde, das diesem Schutzprofil (en: Protection Profile, PP) entspricht.

1) Diese Europäische Richtlinie wird im Folgenden als „die Richtlinie“ bezeichnet.

Dieses Schutzprofil beschreibt die grundlegenden Sicherheitsanforderungen an eine sichere Einheit, die einen Signaturschlüssel²⁾ importieren kann [Signaturerstellungsdaten (en: signature creation data), SCD] und mit dem importierten Schlüssel elektronische Signaturen erstellt. Eine Einheit, die nach diesem Schutzprofil evaluiert wurde und die in den festgelegten Umgebungen eingesetzt wird, ist hinreichend vertrauenswürdig, um jede Art von digitaler Signatur zu erstellen. Somit kann dieses Schutzprofil für jede Einheit verwendet werden, die für die Erstellung einer digitalen Signatur konfiguriert wurde. Speziell erlaubt dieses PP, ein Produkt als eine Einheit zur Erstellung einer in **der Richtlinie** definierten fortgeschrittenen elektronischen Signatur zu qualifizieren.

Ziel dieses Schutzprofils ist es, die in **der Richtlinie** [1], Anhang III, für sichere Signaturerstellungseinheiten (SSCD) definierten Anforderungen an die funktionale Sicherheit und Vertrauenswürdigkeit festzulegen, die den Evaluationsgegenstand (EVG) darstellen. Die Mitgliedstaaten müssen davon ausgehen, dass eine Übereinstimmung mit den in Anhang III **der Richtlinie** [1] festgelegten Anforderungen vorliegt, wenn ein Produkt zur Erstellung elektronischer Signaturen anhand eines Sicherheitsziels (ST) evaluiert wurde, das diesem Schutzprofil (Protection Profile, PP) entspricht.

EN 419211-3 definiert die grundlegenden Sicherheitsanforderungen an SSCD, die Signaturerstellungsdaten (SCD) importieren und fortgeschrittene elektronische Signaturen erstellen, die, sofern sie auf gültigen qualifizierten Zertifikaten basieren, qualifizierte elektronische Signaturen sind. Eine SSCD, die lediglich diese grundlegenden Sicherheitsanforderungen erfüllt, darf vom Unterzeichner in einer sicheren Umgebung zur Signaturerstellung verwendet werden. Der Zertifizierungsdienstanbieter (CSP) wird in einer sicheren Umgebung das SCD/SVD-Paar erzeugen und den privaten Schlüssel (SCD) in die SSCD importieren, so dass sie mit mindestens einem privaten Schlüssel und möglicherweise in der SSCD gespeicherten Zertifikatinformationen an den Unterzeichner ausgeliefert werden kann. Der EVG darf zusätzliche Sicherheitsfunktionen implementieren, z. B. um den Schutz der Integrität der importierten Daten zu unterstützen, die zu unterzeichnen sind. Die zugehörigen Sicherheitsanforderungen sind nicht Gegenstand dieses Basis-Schutzprofils, sondern des erweiterten Schutzprofils. EN 14169-6 „*Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur sicheren Signaturerstellungsanwendung*“ wird diese, für die Konformität mit diesem Basis-Schutzprofil angegeben wird, behandeln.

Die Vertrauenswürdigkeitsstufe für dieses Schutzprofil ist EAL4, augmentiert um AVA_VAN.5.

4.3 Überblick über den Evaluationsgegenstand

4.3.1 Einsatz des EVG

Dieser Abschnitt bietet einen funktionsbezogenen Überblick über den EVG in seinen einzelnen Einsatzumgebungen:

- die Vorbereitungsumgebung, in der der EVG durch eine SCD/SVD-Erzeugungsanwendung mit einem Zertifizierungsdienstanbieter (en: certification service provider, CSP) interagiert, um die Signaturerstellungsdaten (SCD) und eine Zertifikaterzeugungsanwendung (en: certificate-generation application, CGA) zu importieren, um ein Zertifikat für die Signaturprüfdaten (en: signature validation data, SVD) zu erhalten, die dem privaten Schlüssel (SCD) entsprechen, den der Zertifizierungsdienstanbieter erzeugt hat. Die SCD/SVD-Erzeugungsanwendung überträgt die SVD zur CGA. Des Weiteren interagiert die Initialisierungsumgebung mit dem EVG, um diesen mit dem Anfangswert der Referenz-Authentisierungsdaten (reference authentication data, RAD) zu personalisieren;
- die Signierumgebung, in der der EVG durch eine Signaturerstellungsanwendung (SCA) mit einem Unterzeichner interagiert, um Daten zu signieren, nachdem der Unterzeichner als Unterzeichnender authentisiert wurde. Die Signaturerstellungsanwendung stellt die zu signierenden Daten (DTBS) oder eine eindeutige Darstellung derselben (DTBS/R) als Eingabe für die EVG-Signaturerstellungsfunktion bereit und bezieht die resultierende digitale Signatur³⁾;

2) Eine sichere Signaturerstellungseinheit, die ein SCD/SVD-Paar importieren kann, wurde in der früheren Version dieses Schutzprofils (CWA 14169) als SSCD vom Typ 2 bezeichnet. Die Idee der Typen gibt es in dieser Normenreihe nicht mehr. Zur Adressierung der gleichen Funktionalität sollte auf EN 419211-3 (d. h. Teil 3) verwiesen werden.

3) Auf rein funktionaler Ebene erstellt die SSCD eine digitale Signatur; für eine Implementierung der SSCD, die die Anforderungen dieses PP erfüllt und über ein nach Anhang I **der Richtlinie** erstelltes Schlüsselzertifikat verfügt, kann das Ergebnis des Signierprozesses verwendet werden, um eine qualifizierte elektronische Signatur zu erstellen.

- die Managementumgebung, in der der EVG mit dem Benutzer oder einem SSCD-Bereitstellungsdienstleister interagiert, um Managementoperationen auszuführen, z. B. damit der Unterzeichnende gesperrte RAD zurücksetzt. Ein einzelnes Gerät, z. B. ein Chipkartenendgerät, kann die erforderliche sichere Umgebung für das Management und die Signierung bereitstellen.

Die Vorbereitungsumgebung, die Signierumgebung und die Managementumgebung sind sicher und schützen die mit dem EVG ausgetauschten Daten. In prEN 14169-1:2011, Bild 3, ist die Einsatzumgebung dargestellt.

Der EVG speichert Signaturerstellungsdaten und Referenz-Authentisierungsdaten. Er kann mehrere Instanzen von privaten Schlüsseln (SCD) speichern. In diesem Fall stellt der EVG eine Funktion zur Identifizierung sämtlicher privaten Schlüssel (SCD) bereit, und die Signaturerstellungsanwendung kann eine Schnittstelle zum Unterzeichner bereitstellen, damit dieser einen in der Signaturerstellungsfunktion der SSCD zu verwendenden privaten Schlüssel (SCD) auswählen kann. Der EVG schützt die Vertraulichkeit und Integrität der Signaturerstellungsdaten und beschränkt deren Verwendung bei der Signaturerstellung auf den jeweiligen Unterzeichner. Die mit dem EVG erstellte digitale Signatur kann zum Erstellen einer fortgeschrittenen elektronischen Signatur, wie in Artikel 5.1 **der Richtlinie** definiert, verwendet werden. Die Feststellung, ob es sich um ein qualifiziertes Zertifikat handelt, liegt außerhalb des Anwendungsbereichs dieser Norm.

Die Signaturerstellungsanwendung übernimmt den Schutz der Integrität der Eingangsdaten, die sie der Signaturerstellungsfunktion des EVG bereitstellt und stellt sicher, dass diese den vom Unterzeichner zum Signieren freigegebenen Benutzerdaten entsprechen. Sofern dem EVG die Art der von der SCA bereitgestellten Signiereingangsdaten nicht bekannt ist, gibt die Signaturerstellungsanwendung diese an (als DTBS/R) und berechnet die erforderlichen Hash-Werte. Der EVG kann die DTBS/R um von ihm gespeicherte Signaturparameter erweitern und berechnet anschließend einen Hash-Wert über die Eingangsdaten, wie er von der Art der Eingangsdaten und vom verwendeten kryptographischen Algorithmus benötigt wird.

Der EVG speichert Referenz-Authentisierungsdaten des Unterzeichners, um einen Benutzer als den jeweiligen Unterzeichner zu authentisieren. Die RAD sind ein Passwort, z. B. eine PIN, eine biometrische Schablone oder eine Kombination daraus. Der EVG schützt die Vertraulichkeit und Integrität der RAD. Er kann eine Benutzerschnittstelle bereitstellen, um Prüfauthentisierungsdaten (en: verification authentication data, VAD) direkt vom Benutzer zu empfangen; alternativ kann er die VAD von der Signaturerstellungsanwendung empfangen. Wenn die Signaturerstellungsanwendung bei einer Anfrage VAD vom Benutzer bezieht, übernimmt sie den Schutz der Vertraulichkeit und Integrität dieser Daten.

Ein Zertifizierungsdienstleister und ein SSCD-Bereitstellungsdienstleister interagieren mit dem EVG in der sicheren Vorbereitungsumgebung, um Vorbereitungsfunktionen auszuführen, die erforderlich sind, bevor die Kontrolle über den EVG an den berechtigten Benutzer übergeben wird. Zu diesen Funktionen können gehören:

- Initialisieren der RAD;
- Erzeugen eines Schlüsselpaars;
- Speichern persönlicher Informationen des berechtigten Benutzers.

Ein typisches Beispiel für eine sichere Signaturerstellungseinheit ist eine Chipkarte. In diesem Fall kann ein Chipkartenendgerät vorhanden sein, das die erforderliche sichere Umgebung zur Behandlung einer Anfrage bezüglich einer Unterzeichnerautorisierung bereitstellt. Eine Signatur kann auf einem Dokument erhalten werden, das von einer Komponente einer Signaturerstellungsanwendung vorbereitet wird, die auf einem mit dem Kartenendgerät verbundenen PC läuft. Nachdem das Dokument dem Benutzer dargestellt und die Autorisierungs-PIN bezogen wurde, leitet die Signaturerstellungsanwendung durch das Endgerät die digitale Signaturerstellungsfunktion der Chipkarte ein.

4.3.2 Evaluationsgegenstand

Der EVG ist eine Kombination aus Hardware und Software, die so konfiguriert sind, dass sie Signaturerstellungsdaten (SCD) sicher importieren, verwenden und managen. Die SSCD schützt die Signaturerstellungsdaten während ihrer Lebensdauer, beginnend mit dem Import, so, dass sie ausschließlich vom Unterzeichner in einem Signaturerstellungsprozess verwendet werden können.

Der EVG umfasst sämtliche IT-Sicherheitsfunktionen, die erforderlich sind, um die Geheimhaltung der Signaturerstellungsdaten und die Sicherheit der digitalen Signatur sicherzustellen.

Der EVG stellt die folgenden Funktionen bereit:

- 1) Importieren von Signaturerstellungsdaten (SCD) und, optional, den entsprechenden Signaturprüfdaten (SVD);
- 2) optionales Empfangen und Speichern von Zertifikatinformationen;
- 3) Umschalten des EVG von einem nicht betriebsbereiten in einen betriebsbereiten Zustand;
- 4) im betriebsbereiten Zustand Erstellen digitaler Signaturen für Daten, und zwar in folgenden Schritten:
 - a) Auswählen eines Satzes von privaten Schlüsseln (SCD), wenn die SSCD über mehrere Sätze von SCDs verfügt;
 - b) Authentisieren des Unterzeichnenden und Feststellen der Signierabsicht;
 - c) Empfangen der zu signierenden Daten oder einer eindeutigen Darstellung derselben (DTBS/R);
 - d) Anwenden einer geeigneten kryptographischen Signaturerstellungsfunktion auf die DTBS/R unter Verwendung des gewählten privaten Schlüssels (SCD).

Der EVG kann seine Funktion zur digitalen Signaturerstellung so implementieren, dass diese den Festlegungen von ETSI TS 101 733 (CAAdES) [6], ETSI TS 101 903 (XAdES) [7] und ETSI TS 102 778 (PAdES) [8] entspricht.

Der EVG wird zur Verwendung durch den Unterzeichner wie folgt vorbereitet:

- 1) Import von mindestens einem Satz von privaten Schlüsseln (SCD) und
- 2) unterzeichnerbezogene Personalisierung, indem Folgendes im EVG gespeichert wird:
 - a) die Referenz-Authentisierungsdaten (RAD) des Unterzeichners;
 - b) optional: Zertifikatinformationen für mindestens einen privaten Schlüssel (SCD).

Nach dem Import ist der private Schlüssel (SCD) in einem nicht betriebsbereiten Zustand. Bei Empfang eines EVG muss der Unterzeichner den nicht betriebsbereiten Zustand überprüfen und ihn in den betriebsbereiten Zustand überführen.

Weiterhin sollte der vorgesehene, berechtigte Benutzer nach der Vorbereitung über die Prüfauthentisierungsdaten (VAD) des Unterzeichners informiert werden, die zur Verwendung des EVG beim Signieren erforderlich sind. Falls die VAD ein Passwort oder eine PIN sind, wird erwartet, dass mittels der Bereitstellung dieser Informationen die Vertraulichkeit und die Integrität der entsprechenden RAD gewahrt bleiben.

Ist die Verwendung eines privaten Schlüssels (SCD) nicht länger erforderlich, dann sollte er ebenso wie die dazugehörige Zertifikatsinformation, falls eine existiert, vernichtet werden, indem er sie z. B. aus dem Speicher löscht.

4.3.3 Lebenszyklus des EVG

4.3.3.1 Allgemeines

Der EVG-Lebenszyklus unterscheidet die Stufen Entwicklungs-, Vorbereitungs- und Einsatzphase. Es ist zu beachten, dass andere Definitionen des Lebenszyklus möglich sind, wenn dieses Schutzprofil durch andere Schutzprofile angefordert wird (z. B. bei einer SSCD, die zusätzliche vertrauenswürdige Kommunikationen mit der Signaturerstellungsanwendung zur Verfügung stellt).

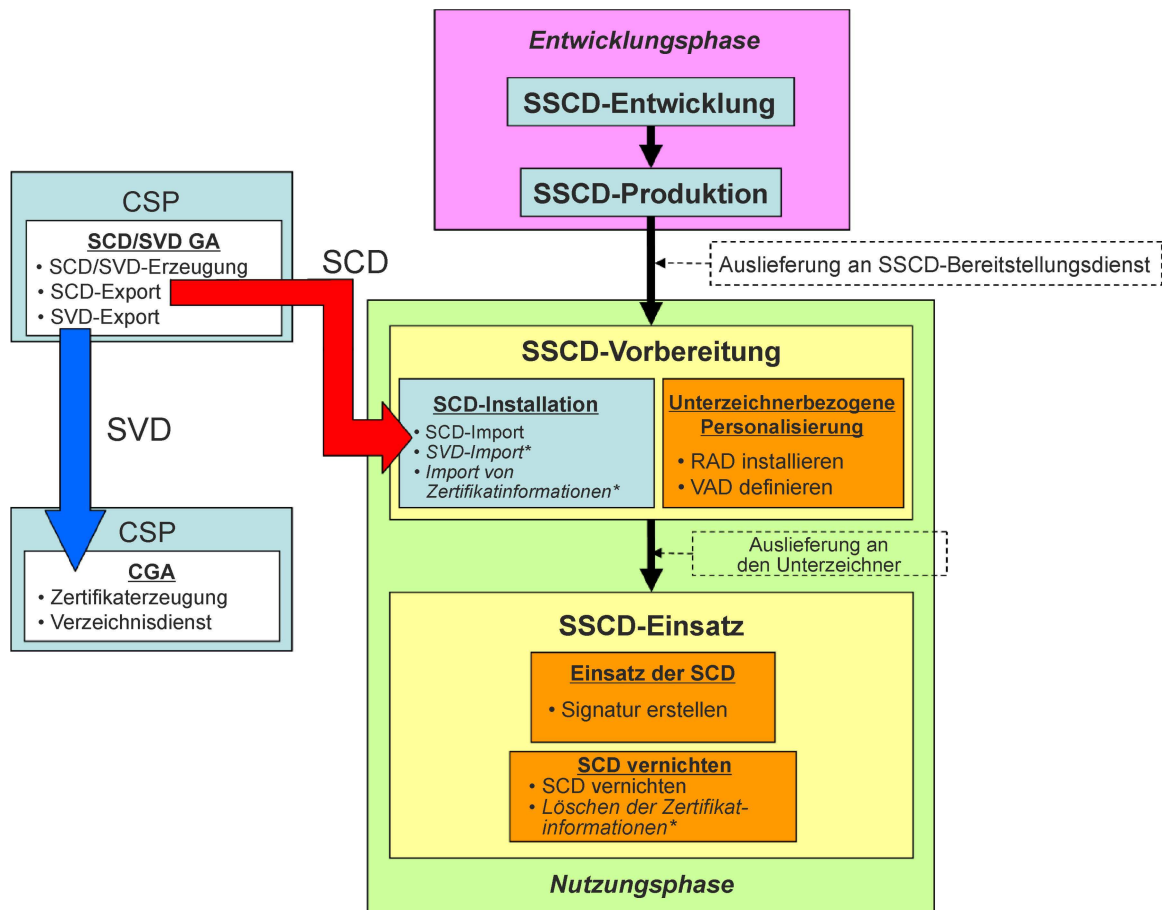


Bild 1 — Beispiel für den EVG-Lebenszyklus⁴⁾

Die Entwicklungsphase umfasst die Entwicklung und Produktion des EVG. Die Entwicklungsphase ist Gegenstand der Evaluation entsprechend der Klasse des Vertrauenswürdigkeits-Lebenszyklus (en: assurance life cycle, ALC). Die Entwicklungsphase endet mit der Auslieferung des EVG an den SSCD-Bereitstellungsdienst.

Der Nutzungsphase des EVG umfasst die Vorbereitungsphase und die Einsatzphase. Die Einsatzphase des EVG beginnt, wenn der Unterzeichner die VAD und die EVG erhalten hat. Für die Aktivierung des EVG zum Signieren ist mindestens eine in dessen Speicher vorhandene Menge von SCD erforderlich.

In Bild 1 ist ein Beispiel für den Lebenszyklus dargestellt, bei dem vor der Auslieferung an den Unterzeichner ein SCD oder SCD/SVD-Paar vom SSCD-Bereitstellungsdienst importiert wird. Der Lebenszyklus kann auch den Import des SCD oder SCD/SVD-Schlüsselpaars nach der Auslieferung an den Unterzeichner zulassen.

4) Die Sterne * kennzeichnen den optionalen Import von Signaturprüfdaten (SVD) und Zertifikatinformationen während der EVG-Vorbereitung sowie das Löschen der Zertifikatinformationen, wenn der private Schlüssel vernichtet wird.

4.3.3.2 Vorbereitungsstufe

Die Vorbereitungsphase des EVG-Lebenszyklus besteht aus der Verarbeitung des EVG, ausgehend von der Annahme des gelieferten EVG durch den Kunden bis zu einem Zustand, in dem der EVG für die Nutzung durch den Unterzeichner bereit ist. Der Kunde, der den EVG vom Hersteller empfängt, ist der SSCD-Bereitstellungsdienst, der die SSCD vorbereitet und den Teilnehmern zur Verfügung stellt. Die Vorbereitung umfasst:

- 1) Personalisierung des EVG für die Nutzung durch den Unterzeichner, d. h. die Installation der RAD im EVG und die Übergabe der VAD an den Unterzeichner;
- 2) die Initialisierung des EVG, d. h. der Zertifizierungsdienstanbieter (CSP) generiert das SCD/SVD-Paar mit Hilfe einer SCD/SVD-Erzeugungseinheit, lädt die SCD auf den EVG und sendet die Signaturprüfdaten (SVD) an die Zertifikaterzeugungsanwendung (CGA). Der EVG darf das SCD/SVD-Paar importieren und speichern;
- 3) die Erzeugung des (qualifizierten) Zertifikats umfasst unter anderem (vgl. [1], Anhang II):
 - a) die SCD, die den SCD unter der Kontrolle des Unterzeichners entsprechen;
 - b) den Namen des Unterzeichners oder eines Pseudonyms, das als solches zu identifizieren ist;
 - c) einen Hinweis auf den Anfang und das Ende der Gültigkeit des Zertifikats.
- 4) die Vorbereitung kann optional das Laden der Zertifikatinformationen in die SSCD zu Unterzeichnungszwecken umfassen.

Der Zertifizierungsdienstanbieter (CSP) erzeugt ein SCD/SVD-Paar und importiert SCD und optional auch SVD in die SSCD. Der CSP stellt folgendes sicher:

- a) die Übereinstimmung zwischen dem privaten (SCD) und dem öffentlichen (SVD) Schlüssel;
- b) dass der Algorithmus und die Schlüsselgröße für den öffentlichen Schlüssel (SVD) geeignet sind.

Es ist zu beachten, dass die Überprüfung, ob die behauptete Identität des Unterzeichners aus der angegebenen SSCD stammt, durch den Zertifizierungsdienstanbieter erfolgen muss, der die CGA betreibt.

Wenn der EVG zur Erstellung fortgeschrittener elektronischer Signaturen verwendet wird, verknüpft das Zertifikat die Signaturprüfdaten mit der Person (d. h. dem Unterzeichner) und bestätigt die Identität dieser Person (vgl. [1], Artikel 2, Abschnitt 9).

Dieses Schutzprofil fordert, dass der EVG Mechanismen für den Import der SCD, die Implementierung der SCD und die Personalisierung zur Verfügung stellt. Die Umgebung übernimmt den Schutz sämtlicher anderen Prozesse zur Vorbereitung des EVG, wie beispielsweise den SCD-Transfer zwischen der SCD/SVD-Erzeugungseinheit und dem EVG sowie den SVD-Transfer zwischen der SCD/SVD-Erzeugungseinheit und der CGA. Der Zertifizierungsdienstanbieter (CSP) darf die Signaturprüfdaten zum EVG zur internen Verwendung durch den EVG (z. B. Selbsttest) exportieren.

Vor der Generierung eines (qualifizierten) Zertifikats, wird erwartet, dass der Zertifizierungsdienstanbieter die SCD in einer SSCD speichert. Ein sicherer Kanal mit dem EVG kann zur Unterstützung verwendet werden, um die Integrität der SCD während der Übertragung zum EVG zu gewährleisten.

4.3.3.3 Einsatzphase

In dieser Phase des Lebenszyklus kann der Unterzeichner den EVG zur Erstellung fortgeschrittener elektronischer Signaturen verwenden.

Die Einsatzphase des EVG beginnt, wenn mindestens ein SCD/SVD-Paar durch die CSP erzeugt und der private Schlüssel in die SSCD importiert wird und wenn der Unterzeichner die Kontrolle über den EVG übernimmt und den privaten Schlüssel betriebsbereit macht. Der Unterzeichner verwendet den EVG nur mit einer vertrauenswürdigen Signaturerstellungsanwendung (SCA) in einer gesicherten Umgebung. Die SCA übernimmt den Schutz der zu signierenden Daten während der Übertragung zum EVG.

Der Unterzeichner kann außerdem mit der SSCD interagieren, um Managementaufgaben durchzuführen, z. B. Zurücksetzen eines RAD-Wertes oder Verwendungszählers, wenn das Passwort/die PIN in den Referenzdaten verloren gegangen ist oder gesperrt wurde. Derartige Managementaufgaben erfordern eine sichere Umgebung.

Der Unterzeichner kann einen privaten Schlüssel (SCD) im EVG dauerhaft unbrauchbar machen. Wird der letzte SCD im EVG dauerhaft unbrauchbar gemacht, so endet der Lebenszyklus des EVG als sichere Signaturerstellungseinheit.

Der EVG kann Funktionen zur Erzeugung zusätzlicher Signierschlüssel unterstützen. Ist dies der Fall, so wird der EVG weitere Funktionen zum sicheren Beziehen von Zertifikaten für die neuen Schlüssel unterstützen. Für einen zusätzlichen Schlüssel kann dem Unterzeichner erlaubt werden, die Art des Zertifikats zu wählen (qualifiziert oder nicht), das für die Signaturprüfdaten des neuen Schlüssels zu beziehen ist. Dem Unterzeichner kann außerdem erlaubt werden, anstelle seines richtigen Namens im Zertifikat ein Pseudonym zu verwenden.⁵⁾ Sind die Bedingungen für den Bezug eines qualifizierten Zertifikats erfüllt, kann der neue Schlüssel auch zur Erstellung von fortgeschrittenen elektronischen Signaturen verwendet werden. Die optionalen EVG-Funktionen für eine zusätzliche Schlüsselerzeugung und -zertifizierung können zusätzliche Sicherheitsfunktionen im EVG und eine Interaktion mit dem SSCD-Bereitstellungsdienstanbieter in einer sicheren Umgebung erfordern.

Der EVG-Lebenszyklus als SSCD endet, wenn sämtliche im EVG gespeicherten privaten Schlüssel (SCD) vernichtet wurden. Das kann das Löschen der zugehörigen Zertifikate umfassen.

5 Konformität

5.1 CC-Konformität

Dieses Schutzprofil entspricht den Common Criteria, Version 3.1, Revision 3 (siehe Literaturhinweise).

Für dieses Schutzprofil besteht Konformität mit den Common Criteria, Teil 2, [3] erweitert.

Für dieses Schutzprofil besteht Konformität mit den Common Criteria, Teil 3 [4].

5.2 Schutzprofil-Konformität, Paket-Konformität

Für dieses Schutzprofil besteht keine Konformität mit anderen Schutzprofilen.

Es besteht Konformität mit dem Vertrauenswürdigkeitspaket EAL4, augmentiert um die Komponenten AVA_VAN.5 entsprechend der Definition im Teil 3 der CC [4].

5) In diesem Fall enthält die Zertifikatanfrage den Namen des Unterzeichners als dem Anfragenden, da es zum Beispiel mit den bestehenden Signaturerstellungsdaten des Unterzeichners signiert sein kann.

5.3 Begründung der Konformität

Dieses Schutzprofil liefert keine Begründung zur Konformität, da keine Konformität mit anderen Schutzprofilen angegeben wird.

5.4 Konformitätsangabe

Sicherheitsziele oder Schutzprofile, für die Konformität mit dem vorliegenden Schutzprofil angegeben wird, müssen diese Konformität **aufs strengste** einhalten.

6 Definition des Sicherheitsproblems

6.1 Zu schützende Werte, Benutzer und Bedrohungsagenten

Die Common Criteria definieren zu schützende Werte als Entitäten, denen der Eigentümer des EVG vermutlich Wert beimisst. Der Begriff „zu schützender Wert“ wird in der Beschreibung der Bedrohungen in der Einsatzumgebung des EVG verwendet.

Zu schützende Werte und Objekte:

- 1) SCD: Signaturerstellungsdaten: ein zur Ausführung einer elektronischen Signaturoperation verwendeter privater Schlüssel. Die Vertraulichkeit, die Integrität sowie die alleinige Kontrolle des Unterzeichners über die Verwendung der Signaturerstellungsdaten müssen gewahrt bleiben;
- 2) SVD: Signaturprüfdaten: öffentlicher Schlüssel der mit den SCD verbunden ist und zur Prüfung der elektronischen Signatur dient. Die Integrität der SVD muss bei deren Export gewahrt bleiben.
- 3) DTBS und DTBS-Darstellung: Satz von Daten oder deren Darstellung, deren Signierung der Unterzeichner beabsichtigt. Ihre Integrität und die Fälschungssicherheit der durch die elektronische Signatur bereitgestellten Verknüpfung zum Unterzeichner müssen gewahrt bleiben.

Benutzer und für die Benutzer handelnde Subjekte:

- 1) Benutzer: Endbenutzer des EVG, der als Administrator oder Unterzeichner identifiziert werden kann. Das Subjekt S.User kann als S.Admin in der Rolle R.Admin oder als S.Sigy in der Rolle R.Sigy handeln;
- 2) Administrator: Benutzer, der dafür verantwortlich ist, die EVG-Initialisierung, EVG-Personalisierung und sonstige administrativen EVG-Funktionen auszuführen. Das Subjekt S.Admin handelt in der Rolle R.Admin für diesen Benutzer nach dessen erfolgreicher Authentisierung als Administrator;
- 3) Unterzeichner: Benutzer, die den EVG innehaben und diesen für sich selbst oder für die natürliche oder juristische Person oder Entität benutzen, die sie repräsentieren. Das Subjekt S.Sigy handelt in der Rolle R.Sigy für diesen Benutzer nach dessen erfolgreicher Authentisierung als Unterzeichner.

Bedrohungsagenten:

- 1) Angreifer, entweder ein Mensch oder ein für diesen handelnder Prozess außerhalb des EVG. Hauptziel des Angreifers ist der Zugriff auf die Signaturerstellungsdaten oder die Fälschung der elektronischen Signatur. Ein Angreifer hat ein hohes Angriffspotential und kennt kein Geheimnis.

6.2 Bedrohungen

6.2.1 T.SCD_Divulg *Speichern, Kopieren und Freigeben der Signaturerstellungsdaten*

Ein Angreifer speichert oder kopiert die Signaturerstellungsdaten außerhalb des EVG. Er kann die Signaturerstellungsdaten während ihrer Erzeugung, Speicherung und Verwendung für die Signaturerstellung im EVG beziehen.

6.2.2 T.SCD_Derive *Ableiten der Signaturerstellungsdaten*

Ein Angreifer leitet die Signaturerstellungsdaten von öffentlich bekannten Daten ab, zum Beispiel von Signaturprüfdaten, die den Signaturerstellungsdaten entsprechen, oder von Signaturen, die mittels der Signaturerstellungsdaten erstellt wurden oder von sonstigen exportierten Daten außerhalb des EVG, was eine Bedrohung für die Geheimhaltung der Signaturerstellungsdaten darstellt.

6.2.3 T.Hack_Phys *Physischer Angriff durch die EVG-Schnittstellen*

Ein Angreifer interagiert physisch mit dem EVG, um Schwachstellen auszunutzen, was zu willkürlichen Sicherheitsgefährdungen führt. Diese Bedrohung richtet sich gegen SCD, SVD und DTBS.

6.2.4 T.SVD_Forgery *Fälschung der Signaturprüfdaten*

Ein Angreifer legt der Zertifikaterzeugungsanwendung gefälschte Signaturprüfdaten vor. Dies führt zum Verlust der Integrität der Signaturprüfdaten im Zertifikat des Unterzeichners.

6.2.5 T.SigF_Misuse *Missbrauch der Signaturerstellungsfunktion des EVG*

Ein Angreifer missbraucht die Signaturerstellungsfunktion des EVG, um ein signiertes Datenobjekt (SDO) für Daten zu erstellen, deren Signierung der Unterzeichner nicht beschlossen hat. Der EVG ist absichtlichen Angriffen durch Experten ausgesetzt, die ein hohes Angriffspotential und fortgeschrittene Kenntnisse über die vom EVG angewendeten Sicherheitsgrundsätze und -konzepte besitzen.

6.2.6 T.DTBS_Forgery *Fälschung der DTBS/R*

Ein Angreifer modifiziert die von der Signaturerstellungsanwendung gesendete DTBS/R. Die vom EVG zur Signierung verwendete DTBS/R entspricht somit nicht mehr den DTBS, die der Unterzeichner zu signieren beabsichtigt.

6.2.7 T.Sig_Forgery *Fälschung der elektronischen Signatur*

Ein Angreifer fälscht ein signiertes Datenobjekt möglicherweise durch Verwendung einer elektronischen Signatur, die durch den EVG erstellt wurde und die Verletzung der Integrität des signierten Datenobjekts ist durch den Unterzeichner oder durch Dritte nicht erkennbar. Die vom EVG erstellte Signatur ist absichtlichen Angriffen durch Experten ausgesetzt, die ein hohes Angriffspotential und fortgeschrittene Kenntnisse über die vom EVG angewendeten Sicherheitsgrundsätze und -konzepte besitzen.

6.3 Organisatorische Sicherheitsvorgaben

6.3.1 P.CSP_QCert *Qualifiziertes Zertifikat*

Der Zertifizierungsdienstanbieter verwendet eine vertrauenswürdige Zertifikaterzeugungsanwendung zur Erzeugung eines qualifizierten Zertifikats oder eines nicht qualifizierten Zertifikats (vgl. **die Richtlinie**, Artikel 2, Abschnitt 9 in Anhang I) für die Signaturprüfdaten. Die Zertifikate enthalten mindestens den Namen des Unterzeichners und die Signaturprüfdaten, die den Signaturerstellungsdaten entsprechen, welche im EVG implementiert sind und sich unter alleiniger Kontrolle des Unterzeichners befinden. Der Zertifizierungsdienstanbieter stellt mit Signaturen durch das Zertifikat oder sonstige öffentlich verfügbare Informationen sicher, dass die Verwendung des EVG als SSCD evident ist.