

DIN EN 419211-2

ICS 03.160; 35.040; 35.240.15

**Schutzprofile für sichere Signaturerstellungseinheiten –
Teil 2: Einheiten mit Schlüsselerzeugung;
Deutsche Fassung EN 419211-2:2013**

Protection profiles for secure signature creation device –
Part 2: Device with key generation;
German version EN 419211-2:2013

Profils de protection des dispositifs sécurisés de création de signature –
Partie 2: Dispositif avec génération de clé;
Version allemande EN 419211-2:2013

Gesamtumfang 47 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 419211-2:2013) 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 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 2: Einheiten mit Schlüsselerzeugung

Protection profiles for secure signature creation
device —
Part 2: Device with key generation

Profils de protection des dispositifs sécurisés de création
de signature —
Partie 2: Dispositif avec génération de clé

Diese Europäische Norm wurde vom CEN am 8. Mai 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

Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Vereinbarungen und Terminologie	4
3.1 Vereinbarungen.....	4
3.2 Begriffe	4
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.....	12
5.1 CC-Konformität	12
5.2 Schutzprofil-Konformität, Paket-Konformität	12
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	14
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.....	18
8 Erweiterte Komponentendefinition	22
9 Sicherheitsanforderungen	23
9.1 Funktionale Sicherheitsanforderungen.....	23
9.2 Anforderungen an die Vertrauenswürdigkeit der Sicherheit	38
9.3 Begründung der Sicherheitsanforderungen	39
Literaturhinweise	45

Vorwort

Dieses Dokument (EN 419211-2:2013) 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 Januar 2014, und etwaige entgegenstehende nationale Normen müssen bis Januar 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 zum Umfrage-Verfahren als prEN 14169-2 vorgelegt.

Diese Reihe EN 419211 besteht aus den folgenden Teilen:

- *Teil 1: Überblick*
- *Teil 2: Einheiten mit Schlüsselerzeugung*
- *Teil 3: Einheiten mit Schlüsselimport*
- *Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikat-erzeugungsanwendung*
- *Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur sicheren Signaturerstellungsanwendung*
- *Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur sicheren Signaturerstellungsanwendung*

Bei der Erstellung dieses Dokuments als Schutzprofil (en: Protection Profile, PP) wurden die Regeln der ISO/IEC 15408-1 befolgt.

Schriftverkehr und Kommentare zu diesem Schutzprofil für sichere Signaturerstellungseinheiten (PP SSCD mit Schlüsselerzeugung) können an das CEN/TC 224 Sekretariat gerichtet werden.

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.

1 Anwendungsbereich

Diese Europäische Norm legt ein Schutzprofil für eine sichere Signaturerstellungseinheit fest, die Signaturschlüssel intern erzeugen kann: sichere Signaturerstellungseinheit mit Schlüsselerzeugung (SSCD KG).

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).

EN 419211-1, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*¹⁾

ISO/IEC 15408-1:2009²⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2²⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3²⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Vereinbarungen und Terminologie

3.1 Vereinbarungen

Der Inhalt und Struktur dieses Dokuments halten die Regeln und Vereinbarungen von ISO/IEC 15408-1 ein.

Normative Anforderungen dieser Europäischen Norm sind in Übereinstimmung mit den Common Criteria Regeln festgelegt und werden nicht speziell durch das Verb „müssen“ gekennzeichnet.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe und Akronyme nach EN 419211-1.

1) Noch zu veröffentlichen. Dieses Dokument wurde zum Umfrage-Verfahren als prEN 14169-1 vorgelegt.

2) ISO/IEC 15408-1, ISO/IEC 15408-2 und ISO/IEC 15408-3 entsprechen den Common Criteria zur Sicherheitsevaluierung in der Informationstechnik, Teile 1, 2 und 3.

4 Einführung in Schutzprofile

4.1 Schutzprofilreferenz

Titel:	Schutzprofil für sichere Signaturerstellungseinheit — Teil 2: Gerät mit Schlüsselerzeugung
Version:	2.0.1
Autor:	CEN (TC 224/WG 17)
Veröffentlichungsdatum:	2013
Registrierung:	BSI-CC-PP-0059-2009-MA-01
CC-Version:	3.1 Revision 3
Bearbeiter:	Arnold Abromeit, TÜV Informationstechnik GmbH
Allgemeiner Status:	Final draft
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur

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 Richtlinie³⁾ 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über *gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*.

Gemäß 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 legt funktionale Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (en: secure signature creation device, SSCD) fest, 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 Übereinstimmung mit den Anforderungen von Anhang III der Richtlinie vorliegt, wenn ein Produkt zur Erstellung sicherer Signaturen bezüglich eines Sicherheitsziels (en: Security Target, ST), welches konform mit diesem Schutzprofil ist, evaluiert wurde.

Dieses Schutzprofil beschreibt die grundlegenden Sicherheitsanforderungen an ein sicheres Gerät, das einen Signaturschlüssel⁴⁾ erzeugen kann [Signaturstellungsdaten (en: signature creation data), SCD] und mit dem erzeugten Schlüssel elektronische Signaturen erstellt. Ein Gerät, das nach diesem Schutzprofil evaluiert wurde und das in den festgelegten Umgebungen eingesetzt wird, ist hinreichend vertrauenswürdig, um jede Art von digitaler Signatur zu erstellen. Somit kann dieses Schutzprofil für jedes Gerät verwendet werden, das für die Erstellung einer digitalen Signatur konfiguriert wurde. Speziell erlaubt dieses PP, ein Produkt als ein Gerät zur Erstellung einer in der Richtlinie definierten fortgeschrittenen elektronischen Signatur zu qualifizieren.

3) Diese EU-Richtlinie wird im Folgenden als „**die Richtlinie**“ bezeichnet.

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

Wenn eine sichere Signaturerstellungseinheit einen Signaturschlüssel erzeugt hat, muss der entsprechende öffentliche Schlüssel (Signaturprüfdaten [en: signature verification data], SVD) als Eingabe für eine Zertifikaterzeugungsanwendung (en: certificate generation application, CGA) bereitgestellt werden. Die Sicherheitsanforderungen für den Export der Signaturprüfdaten sind nicht in diesem Dokument beschrieben, sondern in einem Schutzprofil, das eine Erweiterung des vorliegenden PP darstellt (EN 419211-4, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung*)⁵⁾

Bei Einsatz in einer für die Signaturerstellung sicheren Umgebung darf ein Unterzeichner für die Erstellung einer fortgeschrittenen elektronischen Signatur⁶⁾ eine SSCD verwenden, die nur diese grundlegenden Sicherheitsanforderungen erfüllt. Die Sicherheitsanforderungen an eine SSCD, die in Umgebungen eingesetzt wird, wo die Kommunikation zwischen SSCD und der Signaturerstellungsanwendung (en: signature creation application, SCA) als geschützt durch die SSCD und die SCA angesehen wird, sind nicht in diesem Dokument beschrieben, sondern in einem eigenen Schutzprofil, das eine Erweiterung des vorliegenden PP darstellt (EN 419211-5, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigen Kanal zur Signatur von Generierungsanwendungen*)⁷⁾

Für diese erweiterten Schutzprofile wird Konformität mit dem vorliegenden Schutzprofil angegeben.

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:

- der Vorbereitungsumgebung, in der er durch eine Zertifikaterzeugungsanwendung mit einem Zertifizierungsdienstanbieter (en: certification service provider, CSP) interagiert, um ein Zertifikat für die Signaturprüfdaten zu erhalten, die den vom EVG erzeugten Signaturstellungsdaten entsprechen. Weiterhin interagiert die Initialisierungsumgebung mit dem EVG, um diesen mit dem Anfangswert der Referenz-Authentisierungsdaten (en: reference authentication data, RAD) zu personalisieren;
- der Signierungsumgebung, in der er durch eine Signaturerstellungsanwendung (en: signature creation application, SCA) mit einem Unterzeichner interagiert, um Daten zu signieren, nachdem der Unterzeichner als Unterzeichnender authentisiert wurde. Die Signaturerstellungsanwendung stellt die zu signierenden Daten oder eine eindeutige Darstellung derselben (DTBS/R) als Eingabe für die EVG-Signaturerstellungsfunktion bereit und bezieht die resultierende digitale Signatur⁸⁾;
- der Managementumgebung, in der er mit dem Benutzer oder einem SSCD-Bereitstellungsdienstanbieter 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 Signierungsumgebung, die Managementumgebung und die Vorbereitungsumgebung sind sicher und schützen die mit dem EVG ausgetauschten Daten. Bild 2 in Teil 1 dieser Normenreihe stellt die Einsatzumgebungen dar.

5) Dieses Dokument wurde zum Umfrage-Verfahren als prEN 14169-4 vorgelegt.

6) Eine fortgeschrittene elektronische Signatur ist definiert als eine digitale Signatur, die von einer sicheren Signaturerstellungseinheit mit Hilfe eines öffentlichen Schlüssels erstellt wird, und zwar unter Anwendung eines entsprechend der Richtlinie erstellten öffentlichen Schlüsselzertifikats.

7) Dieses Dokument wurde zum Umfrage-Verfahren als prEN 14169-5 vorgelegt.

8) 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.

Der EVG speichert Signaturerstellungsdaten und Referenz-Authentisierungsdaten. Er kann mehrere Instanzen von privaten Schlüsseln (SCD) speichern. Ist dies der 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 von 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 darf 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 darf 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 dieser Daten.

Ein Zertifizierungsdiensteanbieter und ein SSCD-Bereitstellungsdiensteanbieter 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 vorbereitet wird von einer Komponente einer Signaturerstellungsanwendung, 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 sicher erstellen, verwenden und managen. Die SSCD schützt die Signaturerstellungsdaten während ihrer gesamten Lebensdauer 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:

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

Der EVG darf seine Funktion zur digitalen Signaturerstellung so implementieren, dass diese auch den Festlegungen von ETSI TS 101 733 (CAAdES) [3], ETSI TS 101 903 (XAdES) [4] und ETSI TS 101 903 (PAdES) [5] entspricht.

Er wird zur Verwendung durch den Unterzeichner wie folgt vorbereitet:

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

Nach der Vorbereitung muss sich der private Schlüssel (SCD) in nicht betriebsbereitem Zustand befinden. 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 des Unterzeichners informiert werden, die zur Verwendung des EVG beim Signieren erforderlich sind. Handelt es sich dabei um ein Passwort oder eine PIN, muss bei der Bereitstellung dieser Informationen die Vertraulichkeit und Integrität der entsprechenden RAD gewahrt bleiben.

Ist eine Verwendung eines privaten Schlüssels (SCD) nicht länger erforderlich, dann muss er, ebenso wie das dazugehörige Zertifikat, falls eines existiert, zerstört werden (z. B. durch Löschen aus dem Speicher).

4.3.3 Lebenszyklus des EVG

4.3.3.1 Allgemeines

Der EVG-Lebenszyklus unterscheidet die Stufen Entwicklung, Vorbereitung und Einsatz. Zu beachten ist, dass weitere Lebenszyklusdefinitionen möglich sind; wenn dieses Schutzprofil von anderen Schutzprofilen beansprucht wird (z. B. SCD/SVD-Erzeugung in einer vertrauenswürdigen Umgebung darf nach der Auslieferung zum Unterzeichner zugelassen werden, wenn es einen vertrauenswürdigen Kanal zum CGA gibt).

Die Entwicklungsphase beinhaltet die Entwicklung und die Produktion des EVG. Diese ist Gegenstand der Evaluation entsprechend der ALC-Klasse (ALC: assurance life cycle, Vertrauenswürdigkeits-Lebenszyklus). Sie endet damit, dass der EVG an den SSCD-Bereitstellungsdienst ausgeliefert wird.

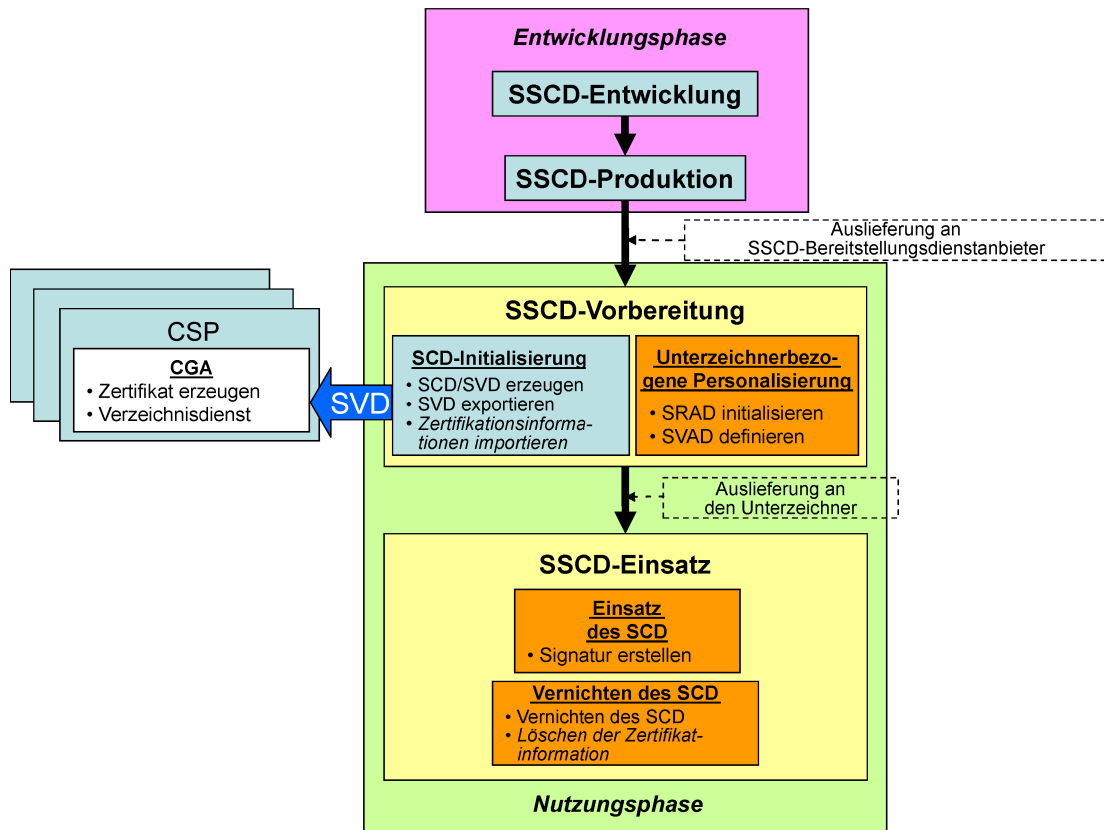


Bild 1 — Beispiel eines EVG-Lebenszyklus⁹⁾

Der Einsatz des EVG beinhaltet die Vorbereitungs- und die Einsatzphase. Die Einsatzstufe 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.

Bild 1 zeigt ein Beispiel des Lebenszyklus, bei dem ein SCD/SVD-Paar auf dem EVG vor Auslieferung an den Unterzeichner generiert wird. Der Lebenszyklus darf die Erstellung von SCD oder SCD/SVD-Schlüsselpaaren auch nach der Auslieferung an den Unterzeichner erlauben.

4.3.3.2 Vorbereitungsstufe

Nachdem ein SSSD-Bereitstellungsdienstleister einen EVG von einem Hersteller angenommen hat, bereitet er diesen zur Verwendung vor und übergibt ihn an den berechtigten Benutzer. Die Vorbereitungsphase endet, wenn der berechtigte Benutzer den EVG von einem SSSD-Bereitstellungsdienst empfangen hat und einen im EVG, möglicherweise bereits vorhandenen, privaten Schlüssel (SCD) zur Verwendung beim Signieren aktiviert hat.

9) Die Sternchen * markieren den optionalen Import des SVD und der Zertifikatsinformation während der EVG Vorbereitung und Löschung der Zertifikatsinformationen wenn das SCD zerstört wird.

Während der oben beschriebenen Vorbereitung des EVG führt ein SSCD-Bereitstellungsdienstanbieter folgende Aufgaben aus:

- a) Beziehen der Informationen zum beabsichtigten Empfänger des Geräts, die für den Vorbereitungsprozess und die Identifizierung als berechtigter Benutzer des EVG erforderlich sind;
- b) Erzeugen einer PIN und/oder Beziehen einer biometrischen Probe des berechtigten Benutzers, Speichern dieser Daten im EVG als RAD und Vorbereiten von Informationen zu den VAD zwecks Auslieferung an den berechtigten Benutzer;
- c) Erzeugen eines Zertifikats für mindestens einen privaten Schlüssel (SCD), entweder durch:
 - 1) Erzeugen eines SCD/SVD-Paares durch den EVG und Beziehen eines Zertifikats für die aus dem EVG exportierten Signaturprüfdaten oder durch
 - 2) Initialisieren von Sicherheitsfunktionen im EVG für einen geschützten Export der Signaturprüfdaten und Beziehen eines Zertifikats für die Signaturprüfdaten nach Empfang einer geschützten Anfrage vom EVG;
- d) optionales Vorlegen der Zertifikatinformationen bei der SSCD;
- e) Ausliefern des EVG und der zugehörigen VAD-Informationen an den berechtigten Benutzer.

Die Aufgabe der in diesem Schutzprofil festgelegten SVD-Zertifizierung (dritter Punkt in der oben stehenden Liste) durch einen SSCD-Bereitstellungsdienstanbieter darf einen zentralisierten, vor der Ausgabe stattfindenden Schlüsselerzeugungsprozess umfassen, bei dem vor Auslieferung an den berechtigten Benutzer mindestens ein Schlüssel erzeugt und zertifiziert wird. Alternativ oder zusätzlich darf diese Aufgabe eine Schlüsselerzeugung durch den Unterzeichner nach der Auslieferung und außerhalb der sicheren Vorbereitungsumgebung unterstützen. Ein EVG darf beide Schlüsselerzeugungsprozesse unterstützen, wobei zum Beispiel ein erster Schlüssel zentral erzeugt wird und zusätzliche Schlüssel vom Unterzeichner in der Einsatzstufe erzeugt werden.

In das SVD-Zertifikat müssen mindestens folgende Daten aufgenommen werden (Anhang II der Richtlinie):

- Signaturprüfdaten, die mit dem privaten Schlüssel (SCD), unter Kontrolle des Unterzeichners, übereinstimmen;
- Name des Unterzeichners oder ein Pseudonym, welches als solches identifiziert werden muss;
- ein Hinweis auf den Anfang und das Ende der Gültigkeitsdauer des Zertifikats.

Die im Zertifikat enthaltenen Daten können während der Personalisierung in der SSCD gespeichert gewesen sein.

Vor Einleitung der eigentlichen Zertifikatsignatur verifiziert die Zertifikaterzeugungsanwendung die vom EVG empfangenen Signaturprüfdaten, indem sie:

- a) den Sender als echte SSCD feststellt;
- b) feststellt, ob der zu zertifizierende öffentliche Schlüssel (SVD) seine von der Ursprungs-SSCD gesendete Integrität gewahrt hat;
- c) feststellt, ob die Ursprungs-SSCD für den berechtigten Benutzer personalisiert wurde;
- d) die Übereinstimmung zwischen privatem (SCD) und öffentlichem Schlüssel (SVD) feststellt und;
- e) bestätigt, dass der Signaturalgorithmus und die Schlüsselgröße für den öffentlichen Schlüssel (SVD) genehmigt und für den Zertifikattyp geeignet sind.

Der Nachweis der Übereinstimmung zwischen einem im EVG gespeicherten privaten (SCD) und einem öffentlichen Schlüssel (SVD) kann implizit in den von der Zertifikaterzeugungsanwendung angewendeten Sicherheitsmechanismen vorliegen. Optional darf der EVG eine Funktion zur Bereitstellung eines expliziten Nachweises der Übereinstimmung zwischen einem in ihm gespeicherten privaten Schlüssel (SCD) und einem durch Selbstzertifizierung realisierten öffentlichen Schlüssel (SVD) unterstützen. Eine derartige Funktion kann implizit in der SVD-Exportfunktion ausgeführt werden und in der Vorbereitungsumgebung ohne explizite Zustimmung des Unterzeichners aufgerufen werden.¹⁰⁾ Die Sicherheitsanforderungen zum Schutz der SVD-Exportfunktion und der Zertifizierungsdaten für den Fall, dass die Signaturprüfdaten vom Unterzeichner erzeugt und dann aus der SSCD in die CGA exportiert werden, sind in einem eigenen Schutzprofil festgelegt (siehe Unterabschnitt 4.2).

Vor Erzeugung des Zertifikats muss der Zertifizierungsdienstanbieter die Identität des in der Zertifizierungsanfrage festgelegten Unterzeichners als dem berechtigten Benutzer des EVG bestätigen.

4.3.3.3 Einsatzstufe

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

Die Einsatzstufe 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.

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 darf 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 darf 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 darf außerdem erlaubt werden, anstelle seines richtigen Namens im Zertifikat ein Pseudonym zu verwenden.¹¹⁾ 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 alle in der EVG gespeicherten Schlüssel gelöscht sind. Dies kann das Löschen aller zugehörigen gespeicherten Zertifikatinformationen einschließen.

10) Selbstzertifizierung der Signaturprüfdaten ist die Berechnung einer elektronischen Signatur mit den entsprechenden Signaturerstellungsdaten. Eine Signieroperation erfordert eine explizite alleinige Unterzeichnerkontrolle; dieser spezielle Fall stellt, sofern er unterstützt wird, eine Ausnahme dieser Regel dar, da vor Auslieferung an den Unterzeichner eine derartige Kontrolle augenscheinlich unmöglich ist.

11) 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 Konformität

5.1 CC-Konformität

Dieses Schutzprofil verwendet ISO/IEC 15408-3 (siehe Literaturhinweise).

Für dieses Schutzprofil besteht Konformität zu ISO/IEC 15408-2.

Für dieses Schutzprofil besteht Konformität zu ISO/IEC 15408-3.

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 in ISO/IEC 15408-3.

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

ISO/IEC 15408 definiert 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:

- a) 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.
- b) SVD: Signaturprüfdaten — mit dem privaten Schlüssel (SCD) verknüpfter und zur Verifizierung der elektronischen Signatur verwendeter öffentlicher Schlüssel. Wird dieser exportiert, muss seine Integrität gewahrt bleiben.
- c) DTBS und DTBS/R: 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 den Benutzer handelnde Subjekte:

- a) Benutzer: Endbenutzer des EVG, der als Administrator oder Unterzeichner identifiziert werden kann. Das Subjekt S.User darf als S.Admin in der Rolle R.Admin oder als S.Sigy in der Rolle R.Sigy handeln.
- b) 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.
- c) 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:

- a) Angreifer: 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 fälscht die Signaturprüfdaten, die vom Zertifikatdienstanbieter der Zertifikaterzeugungsanwendung vorgelegt werden. 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 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 unter Verwendung einer elektronischen Signatur, welche vom EVG erstellt wurde und die Verletzung der Integrität des signierten Datenobjekts ist durch den Unterzeichner oder eine dritte Partei nicht nachweisbar. Die vom EVG erzeugte Signatur ist absichtlichen Angriffen durch Experten ausgesetzt, die ein hohes Angriffspotential und fortgeschrittene Kenntnisse über die vom EVG angewendeten Sicherheitsgrundsätze und -konzepte besitzen.