

DIN EN 14169-2

ICS 03.160; 35.040; 35.100.05

Einsprüche bis 2010-07-17

Entwurf**Schutzprofile für Sichere Signaturerstellungseinheiten –
Teil 2: Geräte mit Schlüsselerzeugung;
Deutsche Fassung prEN 14169-2:2010**

Protection Profile for Secure signature creation device –
Part 2: Device with key generation;
German version prEN 14169-2:2010

Dispositif sécurisé de signature électronique –
Partie 2: Dispositif avec génération de clé;
Version allemande prEN 14169-2:2010

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2010-05-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an nia@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

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

Gesamtumfang 49 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (prEN 14169-2:2010) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird.

Der zuständige deutsche Arbeitsausschuss ist der NA 043-01-27 AA „IT-Sicherheitsverfahren“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Geräte mit Schlüsselerzeugung

Dispositif sécurisé de signature électronique — Partie 2 : Dispositif avec génération de clé

Protection Profile for Secure signature creation device — Part 2: Device with key generation

ICS: 03.160 ; 35.040 ; 35.100.05

Deskriptoren

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

Inhalt

	Seite
Vorwort	3
0 Einleitung.....	4
0.1 Allgemeines.....	4
0.2 Aufbau des Dokuments.....	5
1 Anwendungsbereich	6
2 Normative Verweisungen.....	6
3 Begriffe und Akronyme	6
4 Einführung in Schutzprofile.....	6
4.1 Überblick über diesen Abschnitt.....	6
4.2 Schutzprofilreferenz	7
4.3 Überblick über das Schutzprofil.....	7
4.4 Überblick über den Evaluationsgegenstand.....	8
5 Konformität.....	14
5.1 CC-Konformität	14
5.2 Schutzprofil-Konformität, Paket-Konformität	14
5.3 Begründung der Konformität	15
5.4 Konformitätsangabe.....	15
6 Definition des Sicherheitsproblems	15
6.1 Allgemeines.....	15
6.2 Bedrohungen.....	16
6.3 Organisatorische Sicherheitsvorgaben	16
6.4 Annahmen	17
7 Sicherheitsziele.....	17
7.1 Allgemeines.....	17
7.2 Sicherheitsziele für den EVG.....	18
7.3 Sicherheitsziele für die Einsatzumgebung	19
7.4 Begründung der Sicherheitsziele.....	21
8 Erweiterte Komponentendefinition	25
8.1 FPT_EMSEC.1 EVG-Ausstrahlung	25
9 IT-Sicherheitsanforderungen.....	26
9.1 Allgemeines.....	26
9.2 Funktionale EVG-Sicherheitsanforderungen.....	26
9.3 Anforderungen an die Vertrauenswürdigkeit der EVG-Sicherheit	40
10 Begründung.....	41
10.1 Begründung der Sicherheitsanforderungen.....	41
10.2 Begründung der Abhängigkeiten der funktionalen Sicherheitsanforderungen	44
10.3 Begründung für EAL4 Augmentiert	45
Literaturhinweise	47

Vorwort

Dieses Dokument (prEN 14169-2:2010) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird CEN/CWA 14169 ersetzen.

0 Einleitung

0.1 Allgemeines

Diese Europäische Normenreihe legt 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 14169:2002, Anhang C, zu Schutzprofilen sicherer Signaturerstellungseinheiten, „EAL 4+“, herausgegeben.

Das vorliegende Dokument ist dazu vorgesehen, von der Europäischen Kommission gemäß Artikel 9 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen [1] im Amtsblatt der Europäischen Gemeinschaften als allgemein anerkannte Norm für Produkte zur Erstellung elektronischer Signaturen angegeben zu werden. Dieses Schutzprofil beschreibt grundlegende Sicherheitsanforderungen an sichere Signaturerstellungseinheiten nach [1], Anhang III.

Diese Europäische Normenreihe besteht aus den folgenden Teilen:

- Teil 1: Überblick;
- Teil 2: Geräte mit Schlüsselerzeugung;
- Teil 3: Geräte mit Schlüsselimport;
- Teil 4: Erweiterung für Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikat-erzeugungsanwendung;
- Teil 5: Erweiterung für Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur sicheren Signaturerstellungsanwendung;
- Teil 6: Erweiterung für Geräte mit Schlüsselimport und vertrauenswürdigen Kanal zur sicheren Signatur-erstellungsanwendung.

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

Schriftverkehr und Kommentare zu diesem Schutzprofil für sichere Signaturerstellungseinheiten (PP SSCD mit Schlüsselerzeugung) sollten an folgende Stelle gerichtet werden:

KONTAKTADRESSE

**CEN/ISSS Secretariat
Rue de Stassart 36
1050 Bruxelles
Belgien**

**Tel. +32 2 550 0813
Fax +32 2 550 0966**

E-Mail issc@cenorm.be

0.2 Aufbau des Dokuments

Abschnitte 1 bis 3	erfüllen die CEN-Vorgaben hinsichtlich der Veröffentlichung dieses Schutzprofils als Europäische Norm.
Abschnitt 4	bietet eine Einführung in das Schutzprofil, erläutert den allgemeinen Zweck und beschreibt den Evaluationsgegenstand (EVG).
Abschnitt 5	gibt die Konformität mit den Common Criteria an.
Abschnitt 6	enthält eine Erörterung des Sicherheitsproblems für die zu erwartende Einsatzumgebung des EVG. Dieser Abschnitt definiert die Bedrohungen, denen entweder durch in der EVG-Hardware oder –Software implementierte technische Gegenmaßnahmen oder durch die Kontrolleinrichtungen der Umgebung begegnet werden muss. Außerdem definiert dieser Abschnitt die zu befolgenden Sicherheitsvorgaben sowie Annahmen zur Einsatzumgebung.
Abschnitt 7	definiert die Sicherheitsziele für den EVG und die EVG-Umgebung.
Abschnitt 8	enthält die erweiterte Komponentendefinition für FPT_EMSEC.1.
Abschnitt 9	stellt die von den Common Criteria (CC), Teil 2 [3] und Teil 3 [4], abgeleiteten funktionalen Anforderungen und die Anforderungen an die Vertrauenswürdigkeit vor, die vom EVG erfüllt werden müssen.
Abschnitt 10	stellt eine Argumentation zur Verfügung, um explizit zu demonstrieren, dass die Sicherheitsziele die definierten Sicherheitsprobleme, wie in den organisatorischen Sicherheitsvorgaben, Bedrohungen und Annahmen beschrieben, abdecken. Es werden Beweise zur Verfügung gestellt, dass sämtliche organisatorischen Sicherheitsvorgaben, Bedrohungen und Annahmen abgedeckt werden.
Literaturhinweise	nennen Material, dem Hintergrundinformationen entnommen werden können.

1 Anwendungsbereich

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

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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 14169-1¹⁾, *Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick*

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

3 Begriffe und Akronyme

Für die Anwendung dieses Dokuments gelten die Begriffe und Akronyme nach EN 14169-1.

4 Einführung in Schutzprofile

4.1 Überblick über diesen Abschnitt

Der vorliegende Abschnitt bietet Informationen zum Dokumentenmanagement und gibt einen Überblick. Unterabschnitt 4.2 „Schutzprofilreferenz“ nennt die Kennung und weitere beschreibende Informationen, die notwendig sind, um dieses Schutzprofil in ein Register einzutragen. Unterabschnitt 4.3 „Überblick über das Schutzprofil“ stellt den Zweck dieses Schutzprofils im Kontext zusätzlicher Schutzprofile für erweiterte Sicherheitsanforderungen vor. Dieser Abschnitt soll als unabhängiger Auszug verwendet werden können, zum Beispiel in einem PP-Register. Unterabschnitt 4.4 „Überblick über den EVG“ enthält eine formlose Beschreibung der Funktionen des EVG und fasst die Sicherheitsanforderungen zusammen. Weiterhin soll dieser Abschnitt Implementierern als Grundlage für den formlosen Beschreibungsteil in CC-Dokumenten auf der Basis dieses Schutzprofils dienen.

1) Noch zu veröffentlichen.

4.2 Schutzprofilreferenz

Titel:	Schutzprofil für sichere Signaturerstellungseinheit mit Schlüsselerzeugung
Version:	1.00
Autor:	CEN/CENELEC (TC 224/WG 17)
Veröffentlichungsdatum:	(noch nicht festgelegt)
Registrierung:	BSI-CC-PP-0059
CC-Version:	3.1 Revision 3
Bearbeiter:	Wolfgang Killmann, T-System GEI GmbH
Allgemeiner Status:	interner Entwurf
Schlüsselwörter:	sichere Signaturerstellungseinheit, elektronische Signatur, digitale Signatur

4.3 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 Richtlinie²⁾ 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 die in Anhang III **der Richtlinie** definierten funktionalen Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit für eine sichere Signaturerstellungseinheit (secure signature creation device, SSCD) auf formale Weise fest. Diese sichere Signaturerstellungseinheit ist der Evaluationsgegenstand (EVG) dieses Schutzprofils.

Für ein Produkt zur Erstellung sicherer Signaturen, für das die Evaluation nach den Common Criteria (Version 3.1) eine Übereinstimmung mit einem Sicherheitsziel (Security Target, ST) ergeben hat und das diesem Schutzprofil entspricht, müssen die Mitglieder der Europäischen Union nach dieser Europäischen Norm davon ausgehen, dass Übereinstimmung mit den Anforderungen von Anhang III **der Richtlinie** vorliegt.

Dieses Schutzprofil beschreibt die grundlegenden Sicherheitsanforderungen an ein sicheres Gerät, das einen Signaturschlüssel³⁾ erzeugen kann [Signaturstellungsdaten (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.

Wenn eine sichere Signaturerstellungseinheit einen Signaturschlüssel erzeugt hat, muss der entsprechende öffentliche Schlüssel (Signaturprüfdaten [signature verification data], SVD) als Eingabe für eine Zertifikaterzeugungsanwendung (certificate generating application, CGA) bereitgestellt werden. Die Sicherheitsanforderungen für den Export der Signaturprüfdaten sind nicht in diesem Dokument beschrieben,

2) Diese EG-Richtlinie wird im Folgenden als „**die Richtlinie**“ bezeichnet.

3) Eine sichere Signaturerstellungseinheit, die ihr eigenes SCD/SVD-Paar erstellen kann, wird als SSCD vom Typ 3 bezeichnet, um sie von dem in der vorherigen Version dieses Schutzprofils (CWI 14160) definierten Typ 1 und Typ 2 zu unterscheiden. Das Schutzprofil für eine SSCD vom Typ 2 findet sich in EN 14169-2, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 2: Geräte mit Schlüsselimport*.

sondern in einem Schutzprofil, das eine Erweiterung des vorliegenden PP darstellt (EN 14169-3, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 3: Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zwischen SSCD und CGA*).

Bei Einsatz in einer für die Signaturerstellung sicheren Umgebung darf ein Unterzeichner für die Erstellung einer fortgeschrittenen elektronischen Signatur⁴⁾ eine SSCD verwenden, die nur diese grundlegenden Sicherheitsanforderungen erfüllt. Die Sicherheitsanforderungen an eine SSCD, die in anderen Umgebungen eingesetzt wird, sind nicht in diesem Dokument beschrieben, sondern in einem eigenen Schutzprofil, das eine Erweiterung des vorliegenden PP darstellt (EN 14169-4, *Schutzprofil für sichere Signaturerstellungseinheiten — Teil 4: Geräte mit Schlüsselerzeugung und vertrauenswürdigen Kanal zwischen SSCD und SCA*).

Für diese erweiterten Schutzprofile wird Konformität mit dem vorliegenden Schutzprofil⁵⁾ angegeben.

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

4.4 Überblick über den Evaluationsgegenstand

4.4.1 Einsatz des EVG

Bild 1 bietet einen funktionsbezogenen Überblick über den EVG in seinen einzelnen Einsatzumgebungen:

- der Signierumgebung, in der er durch eine Signaturerstellungsanwendung (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 Signatur⁶⁾;
- der Vorbereitungsumgebung, in der er durch eine Zertifikaterzeugungsanwendung mit einem Zertifizierungsdienstanbieter (certification service provider, CSP) interagiert, um ein Zertifikat für die Signaturprüfdaten zu erhalten, die den vom EVG erzeugten Signaturerstellungsdaten entsprechen. Weiterhin interagiert die Initialisierungsumgebung mit dem EVG, um diesen mit dem Anfangswert der Referenz-Authentisierungsdaten (reference authentication data, RAD) zu personalisieren;
- 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 Signierumgebung, die Managementumgebung und die Vorbereitungsumgebung sind sicher und schützen die mit dem EVG ausgetauschten Daten.

4) 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.

5) Siehe CC, Teil 1, Kapitel 8.5.

6) 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.

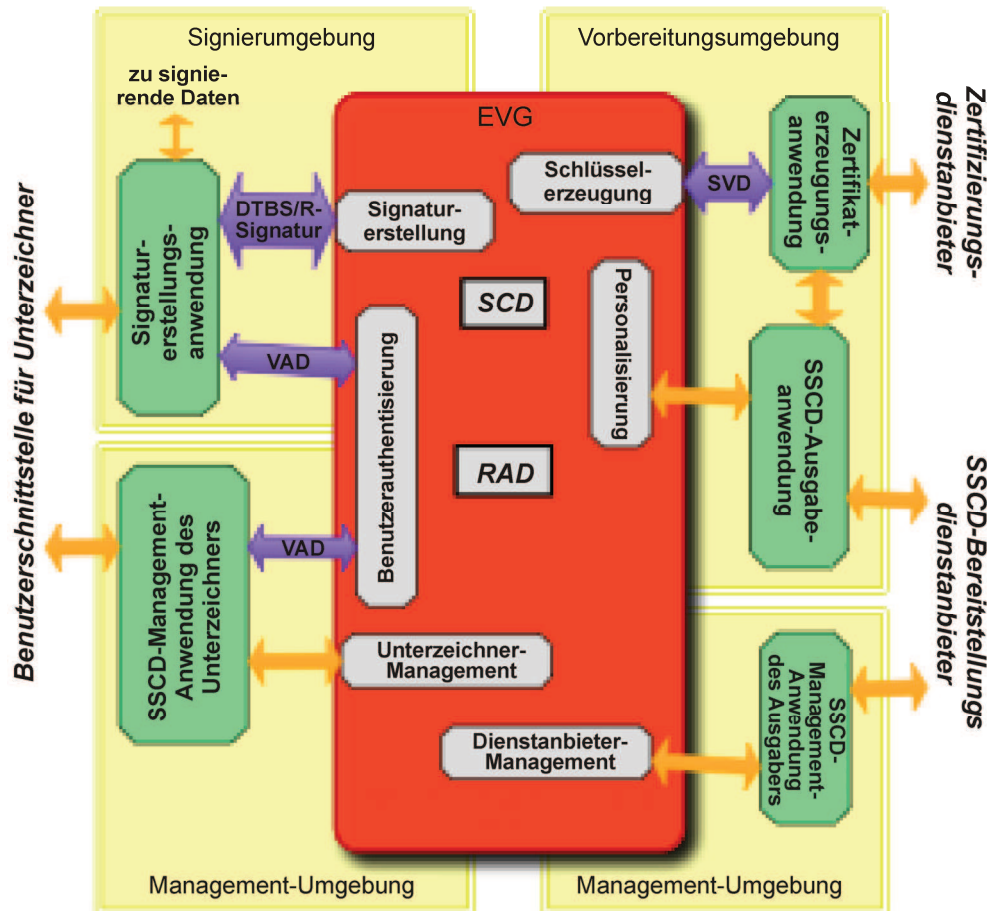


Bild 1 — Hauptfunktionen und Einsatzumgebungen der sicheren Signaturerstellungseinheit

Der EVG speichert Signaturerstellungsdaten und Referenz-Authentisierungsdaten. Er kann mehrere Instanzen von privaten Schlüsseln (SCD) speichern. Ist dies der Fall, muss der EVG eine Funktion zur Identifizierung sämtlicher privaten Schlüssel (SCD) bereitstellen, 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 der Signaturerstellungsdaten und beschränkt deren Verwendung bei der Signaturerstellung auf den jeweiligen Unterzeichner. Die mit dem EVG erstellte digitale Signatur ist eine in **der Richtlinie** definierte *qualifizierte elektronische Signatur*, wenn das Zertifikat für die Signaturprüfdaten ein qualifiziertes Zertifikat ist (Anhang I **der Richtlinie**). Die Feststellung, ob es sich um ein qualifiziertes Zertifikat handelt, liegt außerhalb des Anwendungsbereichs dieser Norm.

Die Signaturerstellungsanwendung muss die Integrität der Eingangsdaten, die sie der Signaturerstellungsfunktion des EVG bereitstellt, schützen und sicherstellen, 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 (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, muss sie die Vertraulichkeit dieser Daten schützen.

Ein Zertifizierungsdienstanbieter und ein SSCD-Bereitstellungsdienstanbieter 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.

4.4.2 Evaluationsgegenstand

Der EVG ist eine Kombination aus Hardware und Software, die so konfiguriert sind, dass sie Signaturstellungsdaten sicher erstellen, verwenden und managen. Die SSCD schützt die Signaturstellungsdaten während ihrer gesamten Lebensdauer so, dass sie ausschließlich vom Unterzeichner in einem Signaturstellungsprozess verwendet werden können.

Der EVG stellt die folgenden Funktionen bereit:

- a) Erzeugen von Signaturstellungsdaten 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;
- 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) Empfangen der zu signierenden Daten oder einer eindeutigen Darstellung derselben (DTBS/R);
 - 3) Authentisieren des Unterzeichnenden und Feststellen der Signierabsicht;
 - 4) 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 auch den Festlegungen von ETSI TS 101 733 (CAAdES) [6] und ETSI TS 101 903 (XAAdES) [7] entspricht. In diesem Fall kann der EVG zusätzliche unterstützende Funktionen bereitstellen, z. B. um den Empfang und/oder die Validierung eines Zeitstempels zu unterstützen.

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

Er wird zur Verwendung durch den Unterzeichner wie folgt vorbereitet:

- f) Erzeugung von mindestens einem SCD/SVD-Paar und
- g) 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 der entsprechenden RAD gewahrt bleiben.

Ist eine weitere Verwendung eines privaten Schlüssels (SCD) nicht länger erforderlich, deaktiviert der EVG die von ihm gehaltenen Signaturerstellungsdaten, indem er sie z. B. aus dem Speicher löscht.

4.4.3 Lebenszyklus des EVG

4.4.3.1 Allgemeines

Der EVG-Lebenszyklus in Bild 2 unterscheidet die Stufen Entwicklung, Vorbereitung und Einsatz. Die Entwicklung und die Produktion des EVG (vgl. CC, Teil 1, Absatz 139) bilden zusammen die Entwicklungsphase des EVG. Diese ist Gegenstand der CC-Evaluation entsprechend der ALC-Klasse (ALC: assurance life cycle, Vertrauenswürdigkeits-Lebenszyklus). Sie endet damit, dass der EVG an einen SSCD-Bereitstellungsdienstleister ausgeliefert wird. Bei dieser Auslieferung muss die funktionale Integrität des EVG geschützt werden.

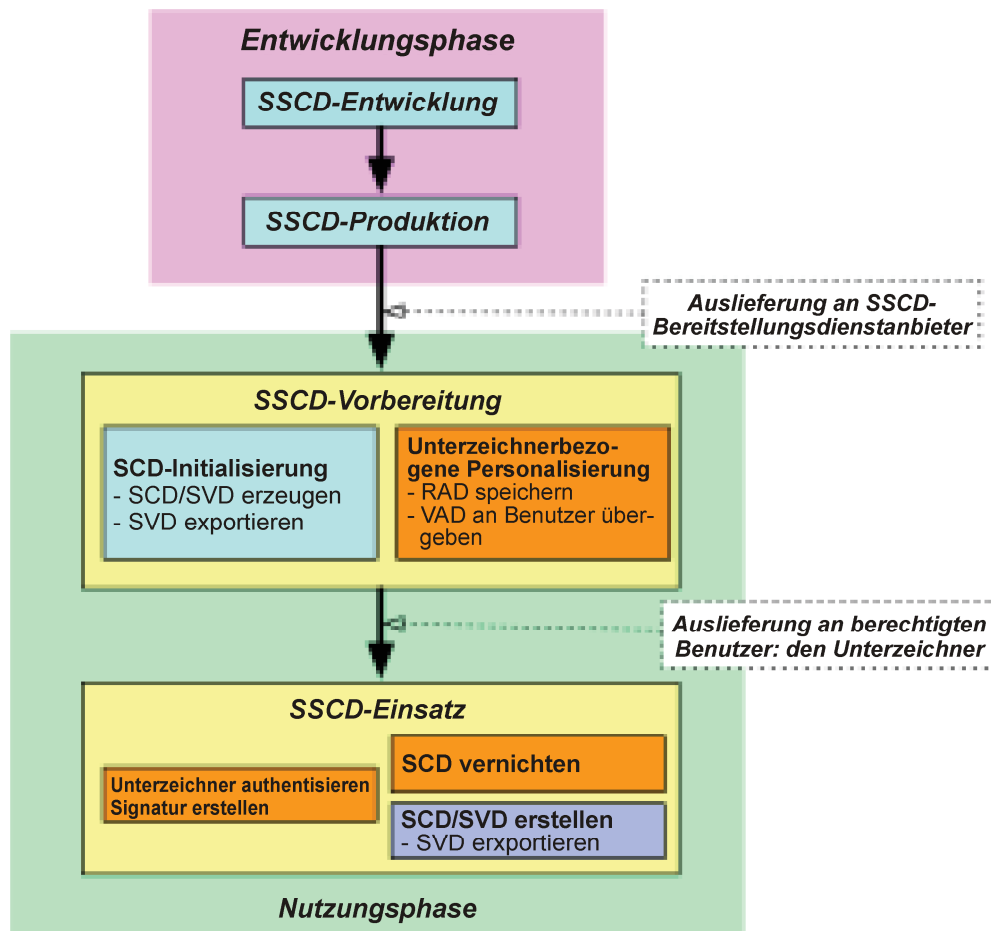


Bild 2 — Lebenszyklus des EVG

Die Einsatzstufe des EVG beginnt, wenn der Unterzeichner die EVG-Operation ausführt, die diesen zur Verwendung bei Signieroperationen aktiviert. Für die Aktivierung des EVG zum Signieren ist mindestens ein in dessen Speicher vorhandener Schlüssel erforderlich. Der EVG-Lebenszyklus endet, wenn alle gespeicherten Schlüssel dauerhaft unbrauchbar gemacht wurden. Das Unbrauchbarmachen eines Schlüssels in der SSCD kann das Löschen aller zugehörigen gespeicherten Zertifikatinformationen umfassen.

4.4.3.2 Vorbereitungsstufe

Nachdem ein SSCD-Bereitstellungsdienstanbieter 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, nachdem er den EVG von einem SSCD-Bereitstellungsdienst empfangen hat, einen im EVG gehaltenen privaten Schlüssel (SCD) zur Verwendung beim Signieren aktiviert. Während der oben beschriebenen Vorbereitung des EVG führt ein SSCD-Bereitstellungsdienstanbieter folgende Aufgaben aus:

- Beziehen der Informationen zum beabsichtigten Empfänger des Geräts, die für den Vorbereitungsprozess und die Identifizierung als berechtigter Benutzer des EVG erforderlich sind;
- 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 kann 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**):

- f) Signaturprüfdaten;
- g) Name des Unterzeichners, entweder
 - 1) ein legaler Name oder
 - 2) ein Pseudonym, zusammen mit der Angabe, dass es sich um ein solches handelt.

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:

- h) den Sender als echte SSCD feststellt;
- i) feststellt, ob der zu zertifizierende öffentliche Schlüssel (SVD) seine von der Ursprungs-SSCD gesendete Integrität gewahrt hat;
- j) feststellt, ob die Ursprungs-SSCD für den berechtigten Benutzer personalisiert wurde;
- k) die Übereinstimmung zwischen privatem (SCD) und öffentlichem Schlüssel (SVD) feststellt und
- l) 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