

**DIN EN 419251-3**

ICS 35.240.15

**Sicherheitsanforderungen für Geräte zur Authentisierung –  
Teil 3: Zusätzliche Funktionalitäten für Sicherheitsziele;  
Deutsche Fassung EN 419251-3:2013**

Security requirements for device for authentication –  
Part 3: Additional functionality for security targets;  
German version EN 419251-3:2013

Profils de protection pour support d'authentification –  
Partie 3: Fonctionnalités additionnelles;  
Version allemande EN 419251-3:2013

Gesamtumfang 88 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

## **Nationales Vorwort**

Dieses Dokument (EN 419251-3:2013) 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 NA 043-01-17 AA „Karten und persönliche Identifikation“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Deutsche Fassung

Sicherheitsanforderungen für Geräte zur Authentisierung -  
Teil 3: Zusätzliche Funktionalitäten für Sicherheitsziele

Security requirements for device for authentication - Part 3:  
Additional functionality for security targets

Profils de protection pour dispositif d'authentification -  
Partie 3: Fonctionnalités additionnelles

Diese Europäische Norm wurde vom CEN am 7. Dezember 2012 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 .....                                           | 6     |
| 1 Anwendungsbereich .....                               | 7     |
| 2 Normative Verweisungen .....                          | 7     |
| 3 Konformität.....                                      | 7     |
| 3.1 CC-Konformität .....                                | 7     |
| 3.2 Schutzprofil-Konformität .....                      | 7     |
| 3.3 Paket-Konformität.....                              | 7     |
| 3.4 Begründung der Konformität .....                    | 7     |
| 3.5 Konformitätsangabe .....                            | 7     |
| 4 Begriffe .....                                        | 8     |
| 5 Symbole und Abkürzungen .....                         | 10    |
| 6 Überblick über den Evaluationsgegenstand.....         | 10    |
| 6.1 EVG-Typ.....                                        | 10    |
| 6.2 EVG-Einsatz.....                                    | 11    |
| 6.3 Sicherheitsmerkmale des EVG.....                    | 11    |
| 6.4 Erforderliche Nicht-EVG-Hardware und -Software..... | 11    |
| 6.5 Schutzprofil-Nutzung .....                          | 11    |
| 6.6 Gruppen .....                                       | 11    |
| 6.6.1 Allgemeines .....                                 | 11    |
| 6.6.2 Hauptgruppen .....                                | 12    |
| 6.6.3 Umgebungsbezogene Gruppen .....                   | 12    |
| 6.7 Konfigurationen .....                               | 14    |
| 6.7.1 Allgemeines .....                                 | 14    |
| 6.7.2 Regeln .....                                      | 14    |
| 6.7.3 Mögliche Konfigurationen .....                    | 15    |
| 6.8 EVG-Umgebung .....                                  | 17    |
| 6.8.1 Allgemeiner Überblick.....                        | 17    |
| 6.8.2 Personalisierungsanwendung.....                   | 18    |
| 6.8.3 Administrationsanwendung .....                    | 19    |
| 6.8.4 Authentisierungsanwendung .....                   | 20    |
| 6.8.5 Prüfer .....                                      | 21    |
| 6.8.6 Schlüsselerzeuger .....                           | 21    |
| 6.8.7 Zertifizierungsinstanz.....                       | 22    |
| 6.8.8 Anwendungsbeispiele .....                         | 22    |
| 6.9 Lebenszyklus .....                                  | 24    |
| 6.9.1 Überblick.....                                    | 24    |
| 6.9.2 Vorpersonalisierungsphase .....                   | 25    |
| 6.9.3 Personalisierungsphase .....                      | 25    |
| 6.9.4 Einsatzphase .....                                | 26    |
| 7 Definition des Sicherheitsproblems .....              | 28    |
| 7.1 Zu schützende Werte (Assets) .....                  | 28    |
| 7.1.1 Allgemeines .....                                 | 28    |
| 7.1.2 „Core“-Gruppe .....                               | 28    |
| 7.1.3 „KeyGen“-Gruppe.....                              | 29    |
| 7.1.4 „Admin“-Gruppe .....                              | 29    |
| 7.2 Benutzer.....                                       | 29    |
| 7.2.1 „Core“-Gruppe .....                               | 29    |

|         |                                                                         |    |
|---------|-------------------------------------------------------------------------|----|
| 7.2.2   | „KeyImp“-Gruppe .....                                                   | 30 |
| 7.2.3   | „KeyGen“-Gruppe .....                                                   | 30 |
| 7.2.4   | „Admin“-Gruppe .....                                                    | 30 |
| 7.3     | Bedrohungen .....                                                       | 31 |
| 7.3.1   | Allgemeines .....                                                       | 31 |
| 7.3.2   | „Core“-Gruppe .....                                                     | 31 |
| 7.3.3   | „KeyGen“-Gruppe .....                                                   | 32 |
| 7.3.4   | „Admin“-Gruppe .....                                                    | 32 |
| 7.4     | Organisatorische Sicherheitsvorgaben .....                              | 32 |
| 7.4.1   | „Core“-Gruppe .....                                                     | 32 |
| 7.4.2   | „KeyGen“-Gruppe .....                                                   | 33 |
| 7.4.3   | „Admin“-Gruppe .....                                                    | 33 |
| 7.5     | Annahmen .....                                                          | 33 |
| 7.5.1   | „Core“-Gruppe .....                                                     | 33 |
| 7.5.2   | „KeyGen“-Gruppe .....                                                   | 34 |
| 7.5.3   | „Admin“-Gruppe .....                                                    | 34 |
| 8       | Sicherheitsziele .....                                                  | 34 |
| 8.1     | Allgemeines – Übertragung sensibler Daten .....                         | 34 |
| 8.2     | Sicherheitsziele für den EVG .....                                      | 35 |
| 8.2.1   | „Core“-Gruppe .....                                                     | 35 |
| 8.2.2   | „KeyImp“-Gruppe .....                                                   | 36 |
| 8.2.3   | „KeyGen“-Gruppe .....                                                   | 36 |
| 8.2.4   | „Admin“-Gruppe .....                                                    | 37 |
| 8.2.5   | Untrusted PersoAppli .....                                              | 37 |
| 8.2.6   | Untrusted AuthAppli .....                                               | 37 |
| 8.2.7   | Untrusted Verifier .....                                                | 37 |
| 8.2.8   | Untrusted CA .....                                                      | 38 |
| 8.2.9   | Untrusted AdminAppli .....                                              | 38 |
| 8.3     | Sicherheitsziele für die Einsatzumgebung .....                          | 38 |
| 8.3.1   | „Core“-Gruppe .....                                                     | 38 |
| 8.3.2   | „KeyImp“-Gruppe .....                                                   | 39 |
| 8.3.3   | „Admin“-Gruppe .....                                                    | 39 |
| 8.3.4   | Trusted PersoAppli .....                                                | 39 |
| 8.3.5   | Trusted AuthAppli .....                                                 | 39 |
| 8.3.6   | Trusted Verifier .....                                                  | 39 |
| 8.3.7   | Trusted CA .....                                                        | 40 |
| 8.3.8   | Trusted AdminAppli .....                                                | 40 |
| 8.4     | Begründung für Sicherheitsziele .....                                   | 40 |
| 9       | Erweiterte Komponentendefinition – Definition der Familie FCS_RNG ..... | 46 |
| 10      | Sicherheitsanforderungen .....                                          | 47 |
| 10.1    | Allgemeines .....                                                       | 47 |
| 10.2    | Einleitung .....                                                        | 48 |
| 10.2.1  | Subjekte, Objekte und Sicherheitsattribute .....                        | 48 |
| 10.2.2  | Operationen .....                                                       | 49 |
| 10.3    | Funktionale Sicherheitsanforderungen .....                              | 50 |
| 10.3.1  | Allgemeines .....                                                       | 50 |
| 10.3.2  | „Core“-Gruppe .....                                                     | 50 |
| 10.3.3  | „KeyImp“-Gruppe .....                                                   | 59 |
| 10.3.4  | „KeyGen“-Gruppe .....                                                   | 62 |
| 10.3.5  | „Admin“-Gruppe .....                                                    | 66 |
| 10.3.6  | Untrusted PersoAppli .....                                              | 71 |
| 10.3.7  | Untrusted AuthAppli .....                                               | 72 |
| 10.3.8  | Untrusted Verifier .....                                                | 72 |
| 10.3.9  | Untrusted CA .....                                                      | 73 |
| 10.3.10 | Untrusted AdminAppli .....                                              | 74 |
| 10.4    | Vertrauenswürdigkeitsanforderungen .....                                | 74 |

|                                                             | Seite |
|-------------------------------------------------------------|-------|
| 10.5 SFR/Sicherheitsziele .....                             | 74    |
| 10.6 SFR-Abhängigkeiten .....                               | 81    |
| 10.7 Begründung für die Vertraulichkeitsanforderungen ..... | 83    |
| Literaturhinweise .....                                     | 85    |
| Stichwortverzeichnis .....                                  | 86    |

## Bilder

|                                                        |    |
|--------------------------------------------------------|----|
| Bild 1 — EVG Sicherheitsmerkmale .....                 | 17 |
| Bild 2 — Umgebung der Personalisierungsanwendung ..... | 18 |
| Bild 3 — Umgebung der Administrationsanwendung .....   | 19 |
| Bild 4 — Umgebung der Authentisierungsanwendung .....  | 20 |
| Bild 5 — EVG Lebenszyklus .....                        | 24 |

## Tabellen

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| Tabelle 1 — Basiskonfigurationen .....                                                   | 15 |
| Tabelle 2 — IDTrusted-Konfigurationen .....                                              | 15 |
| Tabelle 3 — Schutz sensibler Daten .....                                                 | 35 |
| Tabelle 4 — Sicherheitsziele und Problemdefinition .....                                 | 41 |
| Tabelle 5 — Sicherheitsattribute .....                                                   | 48 |
| Tabelle 6 — Core-Sicherheitsattribute .....                                              | 53 |
| Tabelle 7 — Core-Sicherheitsattribute .....                                              | 54 |
| Tabelle 8 — Core-Sicherheitsattribute – Operationen .....                                | 55 |
| Tabelle 9 — Core-Sicherheitsattribute – Anfangswert .....                                | 56 |
| Tabelle 10 — Core-Sicherheitsattribute – Aktualisierungen .....                          | 56 |
| Tabelle 11 — TSF-Daten – Aktualisierungen .....                                          | 57 |
| Tabelle 12 — KeyImp-Sicherheitsattribute .....                                           | 59 |
| Tabelle 13 — KeyImp-Sicherheitsattribute – Operationen .....                             | 60 |
| Tabelle 14 — KeyImp-Sicherheitsattribute – Aktualisierung der autorisierten Rollen ..... | 61 |
| Tabelle 15 — KeyImp-Sicherheitsattribute – Aktualisierung der Werte .....                | 62 |
| Tabelle 16 — KeyGen-Operationen .....                                                    | 63 |
| Tabelle 17 — KeyGen-Sicherheitsattribute .....                                           | 64 |
| Tabelle 18 — Regeln für KeyGen-Operationen .....                                         | 64 |
| Tabelle 19 — KeyGen-Sicherheitsattribute – Aktualisierung der autorisierten Rollen ..... | 65 |
| Tabelle 20 — KeyGen-Sicherheitsattribute – Anfangswerte .....                            | 65 |
| Tabelle 21 — KeyGen-Sicherheitsattribute – Aktualisierung der Werte .....                | 65 |
| Tabelle 22 — Admin-Sicherheitsattribute – Aktualisierung der autorisierten Rollen .....  | 69 |
| Tabelle 23 — Admin-Sicherheitsattribute – Anfangswerte .....                             | 69 |
| Tabelle 24 — Admin-Sicherheitsattribute – Aktualisierung der Werte .....                 | 70 |

|                                                        |           |
|--------------------------------------------------------|-----------|
| <b>Tabelle 25 — Admin-TSF-Daten – Operationen.....</b> | <b>70</b> |
| <b>Tabelle 26 — SFR und Sicherheitsziele .....</b>     | <b>75</b> |
| <b>Tabelle 27 — SFR-Abhängigkeiten .....</b>           | <b>81</b> |

## Vorwort

Dieses Dokument (EN 419251-3:2013) 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 September 2013, und etwaige entgegenstehende nationale Normen müssen bis September 2013 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.

EN 419251 besteht aus den folgenden Teilen:

- EN 419251-1, *Sicherheitsanforderungen für Geräte zur Authentisierung — Teil 1: Schutzprofil für Kernfunktionalitäten*
- EN 419251-2, *Sicherheitsanforderungen für Geräte zur Authentisierung — Teil 2: Schutzprofil für Erweiterung für vertrauenswürdigen Kanal zur Zertifizierung von Generierungsanwendungen*
- EN 419251-3, *Sicherheitsanforderungen für Geräte zur Authentisierung — Teil 3: Zusätzliche Funktionalitäten für Sicherheitsziele (dieses Dokument)*

Das vorliegende Dokument wurde zur CEN-Umfrage unter der Referenz prEN 16248-3 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.

## 1 Anwendungsbereich

Diese Europäische Norm enthält Pakete, die Sicherheitsanforderungen an ein Gerät zur Authentisierung definieren. Bei dem vorliegenden Dokument handelt es sich um Teil 3. Teil 1 und Teil 2 sind Schutzprofile (PP), die auf den hier definierten Paketen basieren. Die im vorliegenden Dokument enthaltenen Pakete können in einem Sicherheitsziel (ST) hinzugefügt werden, das Konformität mit dem Schutzprofil nach Teil 1 oder Teil 2 beansprucht.

## 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).

ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

ISO/IEC 15408-1:2009 <sup>1)</sup>, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2<sup>1)</sup>, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3<sup>1)</sup>, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

## 3 Konformität

### 3.1 CC-Konformität

Die vorliegenden Pakete entsprechen den Common Criteria, Teil 2, erweitert, und den Common Criteria, Teil 3, und sind entsprechend ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 und ISO/IEC 18045 verfasst.

### 3.2 Schutzprofil-Konformität

Diese Pakete beanspruchen keine Konformität mit anderen Schutzprofilen.

### 3.3 Paket-Konformität

Die Vertrauenswürdigkeitsstufe für diese Pakete ist EAL4, augmentiert um die Komponenten AVA\_VAN.5 und ALC\_DVS.2.

### 3.4 Begründung der Konformität

Da diese Pakete keine Konformität mit anderen Schutzprofilen beansprucht, ist an dieser Stelle keine Begründung notwendig.

### 3.5 Konformitätsangabe

Bei der von diesen Paketen geforderten Konformität handelt es sich um die nachweisbare PP-Konformität (demonstrable PP conformance). Dies macht es den Autoren von Sicherheitszielen leichter, Konformität sowohl mit dem Schutzprofil „Authentisierungsgerät“ als auch mit weiteren Schutzprofilen zu beanspruchen.

---

1) ISO/IEC 15408-1, ISO/IEC 15408-2 und ISO/IEC 15408-3 entsprechen den *Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3*.

## **4 Begriffe**

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

### **4.1**

#### **Administrator**

Person die administrative Operationen auf dem Authentisierungsgerät ausführen darf

Anmerkung 1 zum Begriff: Weitere Einzelheiten siehe 7.2.

### **4.2**

#### **authentisierungsprotokollsensible Daten**

Daten, die bei der Authentisierung des EVG durch eine externe Entität verwendet werden

Anmerkung 1 zum Begriff: Diese Daten sind mit dem privaten Authentisierungsschlüssel verknüpft, z. B. Authentisierungszertifikat oder APuK.

Anmerkung 2 zum Begriff: Authentisierungsprotokollsensible Daten dürfen leer sein, wenn die Umgebung vertrauenswürdig und der Inhaber des öffentlichen Schlüssels dem System bekannt ist.

### **4.3**

#### **Zertifikat**

Bescheinigung, mit der der APuK einer Person zugeordnet wird und die Identität der Person bestätigt wird (Definition aus der Richtlinie [8], Artikel 2, Absatz 9)

### **4.4**

#### **Zertifikatinformationen**

Informationen, die einem Authentisierungsschlüsselpaar zugeordnet sind und

- entweder aus dem Public-Key-Zertifikat eines Unterzeichners bestehen oder
- aus einem oder mehreren Hash-Werten des Public-Key-Zertifikats eines Unterzeichners und dem Bezeichner der zur Berechnung dieser Hash-Werte verwendeten Hash-Funktion sowie Informationen, die es dem Unterzeichner erlauben, zwischen verschiedenen Unterzeichnerzertifikaten zu unterscheiden

### **4.5**

#### **Konfiguration**

Satz von Gruppen

Anmerkung 1 zum Begriff: Jede Konfiguration entspricht einem Schutzprofil. Konfigurationen haben jeweils ihre eigene Begründung. Siehe dieses Dokument.

### **4.6**

#### **Gruppe**

Satz von zu schützenden Werten (Assets), Bedrohungen, Zielen und Anforderungen, die sich auf eine bestimmte Funktion beziehen

Anmerkung 1 zum Begriff: Siehe dieses Dokument.

### **4.7**

#### **Inhaber**

rechtmäßiger Inhaber des Authentisierungsgeräts

Anmerkung 1 zum Begriff: Weitere Einzelheiten siehe 7.2.

### **4.8**

#### **Ausgeber**

Benutzer des Authentisierungsgeräts während der Personalisierung

Anmerkung 1 zum Begriff: Weitere Einzelheiten siehe 7.2.

#### 4.9

##### **Schutzprofil**

##### **PP**

implementierungsunabhängige Angabe der Sicherheitserfordernisse eines EVG

[QUELLE: ISO/IEC 15408-1:2009, Abschnitt 4 „Terms and definitions“, modifiziert — in ISO/IEC 15408-1 bezieht sich das Schutzprofil auf einen EVG-Typ anstelle eines EVG, wie in diesem Dokument]

#### 4.10

##### **PP-Sammlung**

Dokument, das Gruppen und Konfigurationen definiert

#### 4.11

##### **Referenz-Authentisierungsdaten**

üblicherweise als RAD bezeichnete Daten, die im EVG gespeichert sind und als Bezugsgröße verwendet werden, mit der die VAD verglichen werden

Anmerkung 1 zum Begriff: Bei den RAD kann es sich um biometrische Daten handeln, um eine PIN oder um einen symmetrischen Schlüssel. Auch eine Kombination dieser drei Möglichkeiten ist denkbar. RAD sind keine zu schützenden Werte, sondern TSF-Daten.

#### 4.12

##### **vertrauenswürdiger Kanal**

Mittel, über das eine TSF und ein abgesetztes vertrauenswürdigen IT-Produkt mit der erforderlichen Vertraulichkeit kommunizieren können

[Quelle: ISO/IEC 15408-1:2009, Abschnitt 4: „Terms and definitions“]

#### 4.13

##### **vertrauenswürdige Umgebung**

Umgebung, die den Schutz sensibler Datenübertragungen zwischen dem EVG und einem abgesetzten vertrauenswürdigen IT-Produkt (bzw. einem Benutzer) sicherstellt

Anmerkung 1 zum Begriff: Die vertrauenswürdige (oder nicht vertrauenswürdige) Umgebung bezieht sich auf den gesamten Kommunikationskanal zwischen dem EVG und dem abgesetzten vertrauenswürdigen IT-Produkt (bzw. dem Benutzer).

#### 4.14

##### **nicht vertrauenswürdige Umgebung**

Umgebung, die den Schutz sensibler Datenübertragungen zwischen dem EVG und einem abgesetzten vertrauenswürdigen IT-Produkt (bzw. einem Benutzer) nicht sicherstellt

Anmerkung 1 zum Begriff: Dieser Schutz sollte vom EVG durch einen vertrauenswürdigen Kanal (bzw. einem vertrauenswürdigen Pfad) sichergestellt werden. Die nicht vertrauenswürdige (oder vertrauenswürdige) Umgebung bezieht sich auf den gesamten Kommunikationskanal zwischen dem EVG und dem abgesetzten vertrauenswürdigen IT-Produkt (bzw. dem Benutzer).

#### 4.15

##### **Benutzer**

jeweiliger Benutzer des EVG

Anmerkung 1 zum Begriff: Bei dem Benutzer kann es sich um den Ausgeber, Inhaber oder Administrator handeln.

#### 4.16

##### **Prüfer**

Entität, die eine authentifizierte Identität verlangt, oder ein Vertreter dieser Entität

Anmerkung 1 zum Begriff: Ein Prüfer umfasst die für Authentisierungsaustausche notwendigen Funktionen.

[QUELLE: ISO/IEC 10181-2:1996, modifiziert — in der ISO/IEC Norm wurde der ganze Satz am Ende der Definition in die vorliegende Anmerkung 1 zum Begriff umgewandelt.]

#### 4.17

##### Prüfauthentisierungsdaten

üblicherweise als VAD bezeichnete Daten, die in den EVG eingegeben und als Mittel zur Authentisierung mit den RAD verglichen werden

Anmerkung1 zum Begriff: Die VAD sind, ebenso wie die RAD, keine zu schützenden Werte, sondern TSF-Daten.

## 5 Symbole und Abkürzungen

| Abkürzung    | Englische Bedeutung                     | Deutsche Bedeutung                        |
|--------------|-----------------------------------------|-------------------------------------------|
| APSD         | Authentication Protocol Sensitive Data  | authentisierungsprotokollsensible Daten   |
| APrK         | Authentication Private Key              | privater Authentisierungsschlüssel        |
| APuK         | Authentication Public Key               | öffentlicher Authentisierungsschlüssel    |
| CA           | Certificate Authority                   | Zertifizierungsinstanz                    |
| CC           | Common Criteria                         | —                                         |
| OBKG         | On-Board Key Generation                 | On-Board-Schlüsselerzeugung               |
| PIN          | Personal Identification Number          | persönliche Identifikationsnummer         |
| PC           | Personal Computer                       | —                                         |
| PP           | Protection Profile                      | Schutzprofil                              |
| RAD          | Reference Authentication Data           | Referenz-Authentisierungsdaten            |
| SSCD<br>SSEE | Secure Signature Creation Device (SSCD) | sichere Signaturerstellungseinheit (SSEE) |
| ST           | Security Target                         | Sicherheitsziel                           |
| EVG<br>TOE   | Target of Evaluation (TOE)              | Evaluationsgegenstand (EVG)               |
| VAD          | Verification Authentication Data        | Prüfauthentisierungsdaten                 |

## 6 Überblick über den Evaluationsgegenstand

### 6.1 EVG-Typ

Ziel ist die Definition von Sicherheitsanforderungen, die ein Authentisierungsgerät bei einer Sicherheits-evaluation erfüllen muss. Der in diesem Schutzprofil betrachtete Evaluationsgegenstand (EVG<sup>2)</sup>) entspricht einer Hardwarekomponente (zum Beispiel eine Chipkarte oder ein USB-Token), die es ihrem rechtmäßigen Inhaber erlaubt, sich beim Zugriff auf einen Online-Dienst zu authentisieren oder die Herkunftsaauthentisierung von vom Benutzer an einen abgesetzten Agenten<sup>3)</sup> gesendeten Daten zu garantieren.

Dieses PP ist so ausgelegt, dass es einem ST-Autor möglich ist, Konformität sowohl mit dem vorliegenden PP als auch PP-SSCD [3], [4], [5], [6], [7] zu beanspruchen und diese PPs ganz einfach in ein Sicherheitsziel zusammenzuführen.

---

2) Im vorliegenden Dokument sind die Bezeichnungen Authentisierungsgerät, Gerät und EVG gleichbedeutend.

3) Person, die authentifizierte Daten von den Benutzern empfängt.

## 6.2 EVG-Einsatz

Um sich mit einem Online-Dienst mit eingeschränktem Zugriff zu verbinden oder Daten zu senden, deren Herkunft authentisiert werden sollte, muss der Inhaber sein persönliches Authentisierungsgerät verwenden. Der von dem Gerät bereitgestellte Dienst erfordert zuvor, dass der Inhaber an einem Endgerät (siehe 6.4) Authentisierungsdaten eingibt. Bei der Authentisierung des Inhabers und der Gewährung des Zugriffs auf Online-Dienste mit eingeschränktem Zugriff oder der Herkunftsaauthentisierung von vom Inhaber gesendeten Daten verlässt sich der im EVG enthaltene Authentisierungsdienst ausschließlich auf die kryptographischen Mittel eines öffentlichen Schlüssels.

Zu beachten ist, dass Authentisierungsgeräte, die zur Authentisierung Mechanismen mit gemeinsamen (also symmetrischen) Schlüsseln implementieren, daher nicht in diesem PP betrachtet werden.

## 6.3 Sicherheitsmerkmale des EVG

Die primäre Funktionalität des EVG ist es, dem Inhaber die Authentisierung zu ermöglichen, damit dieser dann auf einen Online-Dienst zugreifen kann, oder die Herkunftsaauthentisierung von vom Inhaber an einen abgesetzten Agenten gesendeten Daten zu garantieren.

Um diese Dienste zu implementieren, muss zwischen dem EVG und dem Online-Dienst mit eingeschränktem Zugriff bzw. dem Agenten, der mit der Authentisierung der vom Inhaber gesendeten Daten betraut ist, eine Vertrauenskette aufgebaut werden. Diese Vertrauenskette wird in zwei Phasen erzeugt:

- Authentisierung des Inhabers durch den EVG;
- Authentisierung des EVG durch den Prüfer im Auftrag des Inhabers.

## 6.4 Erforderliche Nicht-EVG-Hardware und -Software

Das Authentisierungsgerät erfordert, dass die von einem Endgerät bereitgestellten Dienste dem Inhaber ermöglichen, seine Authentisierungsdaten einzugeben. Typischerweise stellt dieses Endgerät (z. B. ein PIN-Pad-Gerät) den Schutz der Vertraulichkeit und Integrität der eingegebenen Authentisierungsdaten und deren sichere Übertragung an den EVG sicher. Die allgemeinen Merkmale dieses Endgeräts sowie das zur Eingabe der Authentisierungsdaten angewendete Verfahren liegen nicht im Anwendungsbereich des EVG.

Es sollte jedoch beachtet werden, dass das Sicherheitsniveau des gesamten Betriebssystems, einschließlich des EVG, vom Sicherheitsniveau der Einsatzumgebung des EVG abhängt. Vor allem könnte in als nicht vertrauenswürdig geltenden Nutzungsumgebungen ein authentisiertes Endgerät zur Eingabe und Übertragung der Authentisierungsdaten des Inhabers erforderlich sein.

## 6.5 Schutzprofil-Nutzung

Die in diesem Schutzprofil dargelegten Anforderungen definieren die Mindestsicherheitsregeln, die ein Sicherheitsziel eines Authentisierungsgeräts einhalten muss, wobei es sich jedoch nicht um eine erschöpfende Darstellung dieser Regeln handelt. Es besteht die Möglichkeit, weitere Funktionalitäten zu ergänzen oder auch auf ein anderes PP zurückzugreifen. Abänderungen dieses PP sind jedoch durch die in Abschnitt 3 dargelegten Konformitätsregeln eingeschränkt.

Dieses PP hat zum Ziel, die Kompatibilität mit PP-SSCD [3], [4], [5], [6], [7] sicherzustellen, um ergänzende Sicherheitsanforderungen für Produkte, die sowohl Authentisierungs- als auch Signaturdienste anbieten, zu definieren.

## 6.6 Gruppen

### 6.6.1 Allgemeines

Eine Gruppe ist ein Satz von zu schützenden Werten (Assets), Bedrohungen, Zielen und Anforderungen, die sich auf eine bestimmte Funktion beziehen; zum Beispiel bezieht sich KeyGen auf die Schlüsselerzeugung auf dem EVG.

## **6.6.2 Hauptgruppen**

### **6.6.2.1 Allgemeines**

Das vorliegende Schutzprofil umfasst die folgenden Hauptgruppen: „Core“, „KeyImp“, „KeyGen“ und „Admin“.

#### **6.6.2.2 „Core“-Gruppe**

Die Gruppe „Core“ (Kern) gilt für alle Konfigurationen. Sie umfasst die grundlegenden Sicherheitsmerkmale für alle Authentisierungsgeräte.

#### **6.6.2.3 „KeyImp“-Gruppe**

Die Gruppe „KeyImp“ umfasst die Sicherheitsmerkmale, die direkt mit dem Import des privaten Authentisierungsschlüssels in die Karte zusammenhängen.

#### **6.6.2.4 „KeyGen“-Gruppe**

Die Gruppe „KeyGen“ umfasst die Sicherheitsmerkmale, die direkt mit der On-Board-Schlüsselerzeugung (OBKG) des privaten Authentisierungsschlüssels Karte zusammenhängen.

#### **6.6.2.5 „Admin“-Gruppe**

Die Gruppe „Admin“ umfasst die Sicherheitsmerkmale, die direkt mit folgenden administrativen Funktionen zusammenhängen, die in der Einsatzphase ausgeführt werden:

- Import und Export des öffentlichen Schlüssels und des Zertifikats durch den Administrator;
- Speicherung und Export der Protokolldaten durch den Administrator;
- Rücksetzen des Zählers für die fehlgeschlagenen Inhaberauthentisierungsversuche durch den Administrator.

## **6.6.3 Umgebungsbezogene Gruppen**

### **6.6.3.1 Allgemeines**

Dieses Schutzprofil weist zusätzliche Gruppen auf, um mit vertrauenswürdigen wie auch mit nicht vertrauenswürdigen Umgebungen umgehen zu können. Der EVG exportiert und importiert sensible Daten in bzw. aus folgenden Umgebungen:

- Personalisierungsanwendung;
- Authentisierungsanwendung;
- Prüfer;
- CA („KeyGen“-Gruppe);
- Administrationsanwendung („Admin“-Gruppe).

Für jede Umgebung sind zwei Gruppen definiert, eine vertrauenswürdige und eine nicht vertrauenswürdige Gruppe. Jede Konfiguration wählt aus jedem Paar eine Gruppe aus. Eine Konfiguration kann nicht beide Gruppen desselben Paares enthalten, sie kann jedoch keine enthalten, wenn der EVG keine sensiblen Daten aus der entsprechenden Umgebung importiert bzw. exportiert.

#### 6.6.3.2 Trusted PersoAppli

Die Gruppe „Trusted PersoAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Personalisierungsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen in einer geschützten Umgebung stattfinden, d. h. wenn die Umgebung potentiellen Angriffen entgegenwirkt.

Der private Authentisierungsschlüssel muss jedoch auch in einer vertrauenswürdigen Umgebung über einen vertrauenswürdigen Kanal importiert werden.

#### 6.6.3.3 Trusted AuthAppli

Die Gruppe „Trusted AuthAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Authentisierungsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen in einer geschützten Umgebung stattfinden, d. h. wenn die Umgebung potentiellen Angriffen entgegenwirkt.

Unter bestimmten, in diesem Dokument nicht festgelegten Bedingungen kann ein PC in einem Büro oder einer Wohnung als vertrauenswürdige Umgebung betrachtet werden.

#### 6.6.3.4 Trusted Verifier

Die Gruppe „Trusted Verifier“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen dem Prüfer und dem EVG zusammenhängen, wenn diese Übertragungen in einer geschützten Umgebung stattfinden, d. h. wenn die Umgebung potentiellen Angriffen entgegenwirkt.

Diese Gruppe ist auch erforderlich, wenn von der Authentisierungsanwendung zum Beispiel mittels SSL ein vertrauenswürdiger Kanal zum Prüfer eingerichtet wird, jedoch nicht vom EVG zum Prüfer.

#### 6.6.3.5 Trusted CA

Die Gruppe „Trusted CA“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen dem EVG und der CA zusammenhängen, wenn diese Übertragungen in einer geschützten Umgebung stattfinden, d. h. wenn die Umgebung potentiellen Angriffen entgegenwirkt.

Diese Gruppe ist nur erforderlich, wenn die „KeyGen“-Gruppe zur Konfiguration gehört.

#### 6.6.3.6 Trusted AdminAppli

Die Gruppe „Trusted AdminAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Administrationsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen in einer geschützten Umgebung stattfinden, d. h. wenn die Umgebung potentiellen Angriffen entgegenwirkt.

Diese Gruppe ist nur erforderlich, wenn die „Admin“-Gruppe zur Konfiguration gehört.

#### 6.6.3.7 Untrusted PersoAppli

Die Gruppe „Untrusted PersoAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Personalisierungsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen nicht in einer geschützten Umgebung stattfinden.

Das bedeutet, dass der EVG einen vertrauenswürdigen Kanal zur Personalisierungsanwendung einrichten muss.

#### 6.6.3.8 Untrusted AuthAppli

Die Gruppe „Untrusted AuthAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Authentisierungsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen nicht in einer geschützten Umgebung stattfinden.

Das bedeutet, dass der EVG einen vertrauenswürdigen Kanal zur Authentisierungsanwendung einrichten muss.

#### **6.6.3.9 Untrusted Verifier**

Die Gruppe „Untrusted Verifier“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen dem Prüfer und dem EVG zusammenhängen, wenn diese Übertragungen nicht in einer geschützten Umgebung stattfinden.

Das bedeutet, dass der EVG ein sicheres Protokoll für die Authentisierung des EVG durch den Prüfer verwenden muss.

#### **6.6.3.10 Untrusted CA**

Die Gruppe „Untrusted CA“ umfasst die Sicherheitsmerkmale, die direkt mit dem Export des öffentlichen Authentisierungsschlüssels an die CA zusammenhängen, wenn dieser Export nicht in einer geschützten Umgebung stattfindet.

Das bedeutet, dass der EVG einen vertrauenswürdigen Kanal zur CA einrichten muss.

Diese Gruppe ist nur erforderlich, wenn die „KeyGen“-Gruppe zur Konfiguration gehört.

#### **6.6.3.11 Untrusted AdminAppli**

Die Gruppe „Untrusted AdminAppli“ umfasst die Sicherheitsmerkmale, die direkt mit der Übertragung sensibler Daten zwischen der Administrationsanwendung und dem EVG zusammenhängen, wenn diese Übertragungen nicht in einer geschützten Umgebung stattfinden.

Das bedeutet, dass der EVG einen vertrauenswürdigen Kanal zur CA einrichten muss.

Diese Gruppe ist nur erforderlich, wenn die „Admin“-Gruppe zur Konfiguration gehört.

### **6.7 Konfigurationen**

#### **6.7.1 Allgemeines**

Eine Konfiguration ist ein Satz von Gruppen. Jede Konfiguration entspricht einem Schutzprofil und muss separat zertifiziert werden. Eine Konfiguration besitzt eine eigene Begründung.

#### **6.7.2 Regeln**

Aufgrund der Art der Gruppen gelten folgende Regeln:

— **Core**

Die „Core“-Gruppe ist obligatorisch.

— **KeyImp/KeyGen**

Eine Konfiguration muss mindestens die „KeyImp“-Gruppe oder die „KeyGen“-Gruppe umfassen. Sie kann auch beide Gruppen enthalten.

— **Admin**

Die „Admin“-Gruppe ist optional.

— **Trusted PersoAppli/Untrusted PersoAppli**

Eine Konfiguration muss entweder die „Trusted PersoAppli“-Gruppe oder die „Untrusted PersoAppli“-Gruppe umfassen. Sie kann nicht beide Gruppen enthalten.

— **Trusted AuthAppli/Untrusted AuthAppli**

Eine Konfiguration muss entweder die „Trusted AuthAppli“-Gruppe oder die „Untrusted AuthAppli“-Gruppe umfassen. Sie kann nicht beide Gruppen enthalten.

— **Trusted Verifier/Untrusted Verifier**

Eine Konfiguration muss entweder die „Trusted Verifier“-Gruppe oder die „Untrusted Verifier“-Gruppe umfassen. Sie kann nicht beide Gruppen enthalten.

— **Trusted CA/Untrusted CA**

Diese Gruppen sind mit der „KeyGen“-Gruppe verbunden.

Eine Konfiguration, die die „KeyGen“-Gruppe enthält, muss entweder die „Trusted CA“-Gruppe oder die „Untrusted CA“-Gruppe umfassen. Sie kann nicht beide Gruppen enthalten.

— **Trusted AdminAppli/Untrusted AdminAppli**

Diese Gruppen sind mit der „Admin“-Gruppe verbunden.

Eine Konfiguration, die die „Admin“-Gruppe enthält, muss entweder die „Trusted AdminAppli“-Gruppe oder die „Untrusted AdminAppli“-Gruppe umfassen. Sie kann nicht beide Gruppen enthalten.

### 6.7.3 Mögliche Konfigurationen

### 6.7.3.1 Allgemeines

Angesichts der oben beschriebenen Einschränkungen sind nur folgende Konfigurationen möglich:

### 6.7.3.2 Basiskonfigurationen

### Tabelle 1 — Basiskonfigurationen

| Basiskonfiguration | BC1 | BC2 | BC3 | BC4 | BC5 | BC6 |
|--------------------|-----|-----|-----|-----|-----|-----|
| Core               | 1   | 1   | 1   | 1   | 1   | 1   |
| KeyImp             | 1   | 0   | 1   | 1   | 0   | 1   |
| KeyGen             | 0   | 1   | 1   | 0   | 1   | 1   |
| Admin              | 0   | 0   | 0   | 1   | 1   | 1   |

Basiskonfigurationen sind mit BC1 bis BC6 bezeichnet.

### 6.7.3.3 Übertragungskonfigurationen

Übertragungskonfigurationen sind mit den Übertragungen sensibler Daten verbunden:

## Tabelle 2 — IDTrusted-Konfigurationen

[illegible]

IdTrusted kann alle Werte von 0 bis 1F annehmen.

Da es fünf unabhängige Möglichkeiten gibt, gilt:

IdTrusted besitzt  $2^5 = 32$  Möglichkeiten

Eine Konfiguration ist durch ihre Basiskonfiguration und ihre Übertragungskonfiguration bezeichnet: (IdBasic, IdTrusted).

Nicht alle Kombinationen dieser beiden Felder sind zulässig. Die einzigen Einschränkungen sind:

Die Gruppe („Trusted CA“ oder „Untrusted CA“) ist nur enthalten, wenn die Gruppe „KeyGen“ enthalten ist.

Die Gruppe („Trusted AdminApp“ oder „Untrusted AdminApp“) ist nur enthalten, wenn die Gruppe „Admin“ enthalten ist.

Somit gibt es  $6 * 32 * [1/2 * (1 + 2/3)] * [1/2 * (1 + 1/2)] = 120$  mögliche Konfigurationen.

In der Begründung wird auf jede Konfiguration eingegangen.

Der ST-Autor muss die Konfiguration des EVG festlegen.

## 6.8 EVG-Umgebung

### 6.8.1 Allgemeiner Überblick

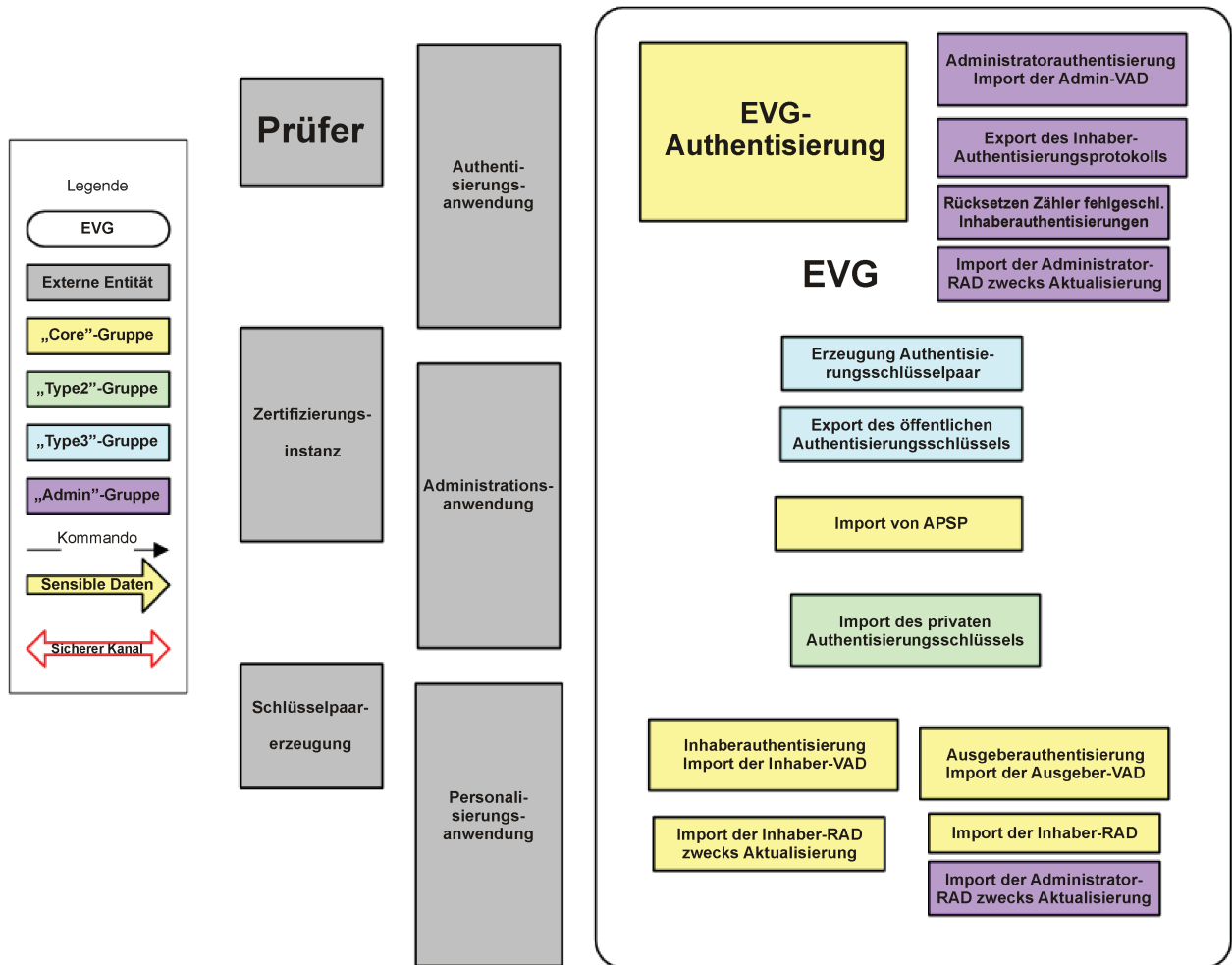


**Bild 1 — EVG Sicherheitsmerkmale**

Bild 1 zeigt alle Sicherheitsmerkmale des EVG in den Umgebungen Personalisierung und Nutzung.

In der Legende ist die farbliche Kennzeichnung der Sicherheitsmerkmale der Gruppen „Core“, „KeyImp“, „KeyGen“ und „Admin“ erläutert. Weitere Einzelheiten zu Gruppen können diesem Dokument entnommen werden.

## 6.8.2 Personalisierungsanwendung

### 6.8.2.1 Allgemeines

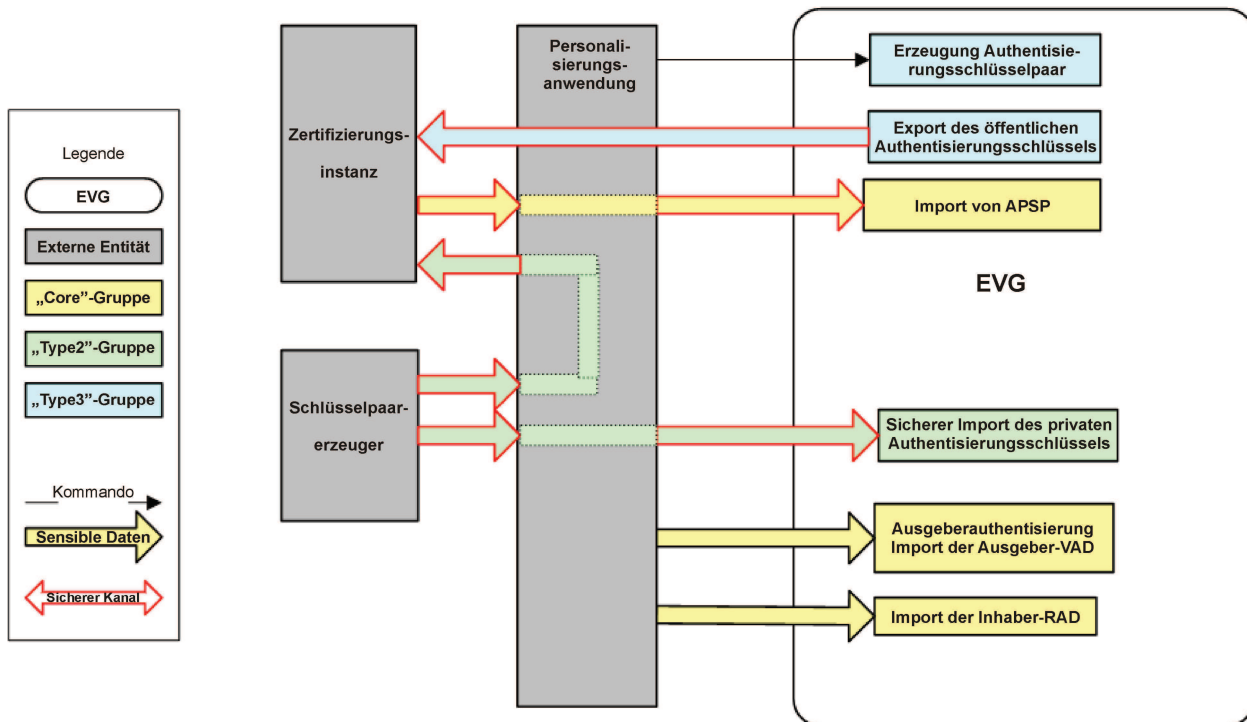


Bild 2 — Umgebung der Personalisierungsanwendung

### 6.8.2.2 Funktionalitäten

Die Personalisierungsanwendung stellt eine Schnittstelle für den EVG an der Personalisierungseinrichtung bereit. Diese Operationen finden vor Ausgabe des EVG statt.

Nach der Ausgabe des EVG, wenn dieser sich in der Einsatzphase befindet, können administrative Funktionen mit Hilfe der Administrationsanwendung, siehe 6.8.3, von einem Administrator ausgeführt werden.

Diese Anwendung initialisiert alle für den Endbenutzer spezifischen Daten. Dazu können gehören:

- APrK;
- Benutzer-RAD;
- Administrator-RAD.

Wenn der EVG den APrK erzeugt, ruft die Anwendung den APuK ab und sendet ihn an die CA, die das Zertifikat erzeugt.

Wenn der EVG den APrK importiert, ruft die Anwendung den APuK ab und sendet ihn an den EVG. Die Anwendung stellt außerdem sicher, dass der APuK sicher, d. h. in seiner Integrität geschützt, vom Schlüsselpaarerzeuger an die CA, die das Zertifikat erzeugt, gesendet wird.

### 6.8.2.3 Kommunikation

Je nach der in der Konfiguration ausgewählten Gruppe, d. h. „Untrusted PersoAppli“ oder „Trusted PersoAppli“, muss die Übertragung sensibler Daten durch die Umgebung oder durch einen vertrauenswürdigen Kanal entweder geschützt werden oder nicht.

Da der APrK jedoch besonders schützenswert ist, ist zum Laden immer ein vertrauenswürdiger Kanal erforderlich.

## 6.8.3 Administrationsanwendung

### 6.8.3.1 Allgemeines

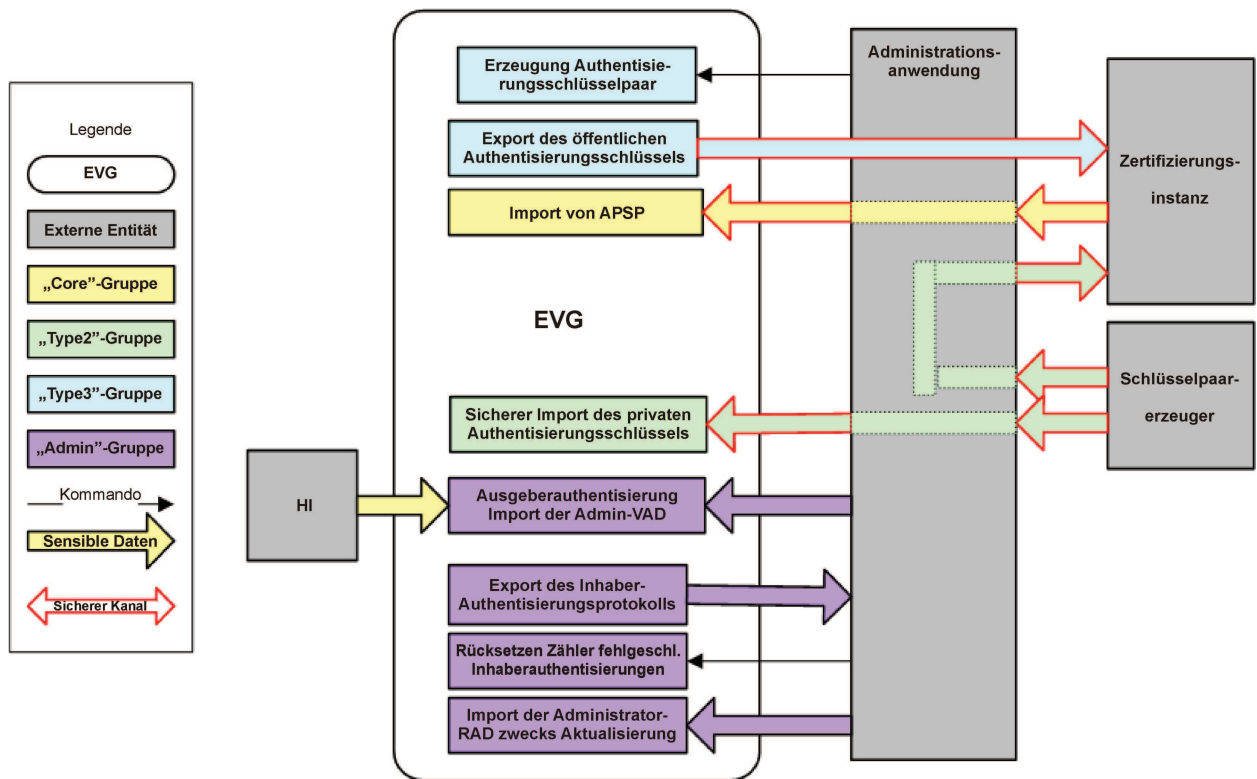


Bild 3 — Umgebung der Administrationsanwendung

### 6.8.3.2 Funktionalitäten

Die Administrationsanwendung stellt eine Schnittstelle für den EVG bei der Administrationseinrichtung bereit. Die Verbindung zu der Einrichtung kann eine Online-Verbindung sein.

Diese Anwendung führt die Administrationsoperationen des EVG aus. Dies sind:

- Abrufen von Authentisierungsprotokollen;
- Rücksetzen des Wiederholungszählers für die Benutzer-RAD.

Vor der Ausführung dieser Operationen muss sich der Administrator mit Hilfe der Administrator-RAD gegenüber dem EVG authentisieren.

### 6.8.3.3 Kommunikation

Je nach der in der Konfiguration ausgewählten Gruppe, d. h. „Untrusted AdminAppli“ oder „Trusted AdminAppli“, muss die Übertragung sensibler Daten durch die Umgebung oder durch einen vertrauenswürdigen Kanal entweder geschützt werden oder nicht.

## 6.8.4 Authentisierungsanwendung

### 6.8.4.1 Allgemeines

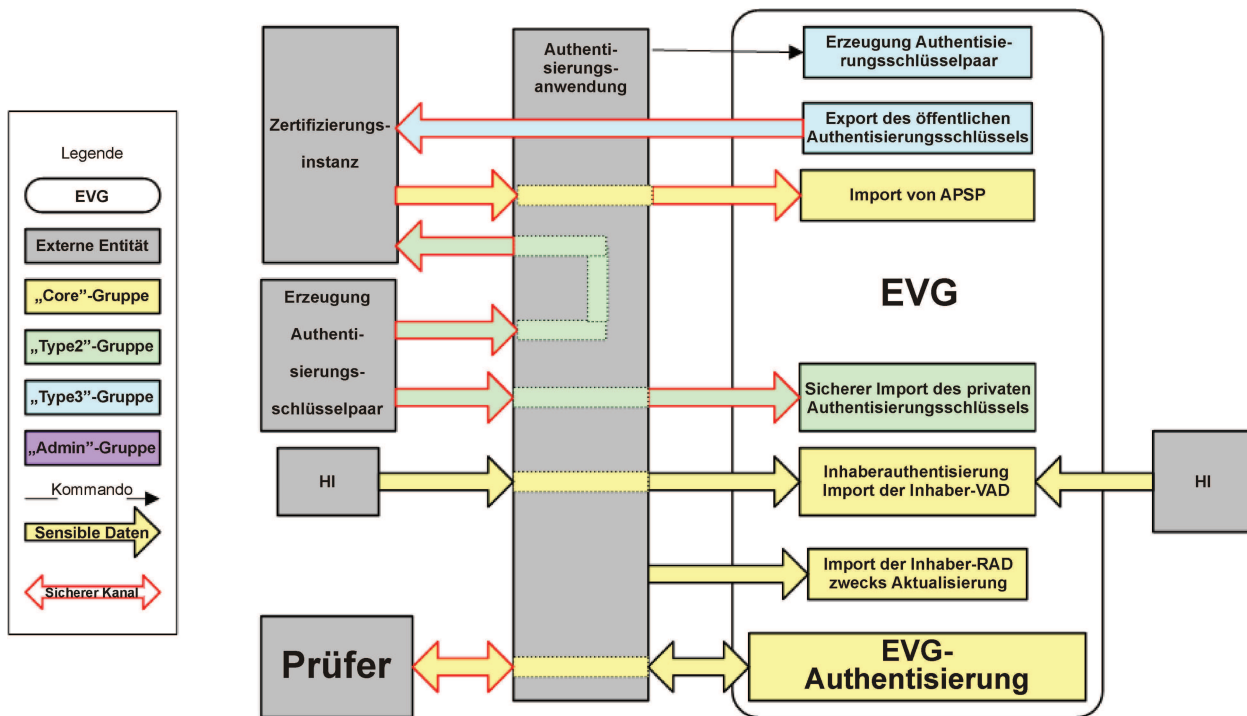


Bild 4 — Umgebung der Authentisierungsanwendung

### 6.8.4.2 Funktionalitäten

Die Authentisierungsanwendung stellt eine Schnittstelle für den EVG bereit, wenn der Inhaber vom Prüfer authentisiert werden muss. Sie kann auf verschiedenen Einrichtungen laufen:

- auf einem Heim-PC, um auf Online-Dienste zugreifen zu können (E-Administration, E-Commerce usw.);
- auf einem speziellen Gerät, um einen Karteninhaber zu authentisieren und zu identifizieren (Polizeikontrolle usw.).

Der EVG darf mehrere Authentisierungsschlüssel enthalten. Er darf außerdem Signaturschlüssel enthalten. Daher muss die Authentisierungsanwendung eine klare und sichere Benutzerschnittstelle (HI) sicherstellen, um Verwechslungen bei der Wahl des Prüfers und des Authentisierungsschlüssels zu vermeiden.

Die VAD können auch über eine separate Benutzerschnittstelle eingegeben werden.

### 6.8.4.3 Kommunikation

Je nach der in der Konfiguration ausgewählten Gruppe, d. h. „Untrusted AuthAppli“ oder „Trusted AuthAppli“, muss die Übertragung sensibler Daten durch die Umgebung oder durch einen vertrauenswürdigen Kanal entweder geschützt werden oder nicht.

Der EVG und die Authentisierungsanwendung tauschen folgende sensible Daten aus:

- Import der Inhaber-VAD zwecks Authentisierung;
- Import der Inhaber RAD für Aktualisierung;
- Anforderung der Authentisierung durch einen bestimmten Prüfer.

## 6.8.5 Prüfer

### 6.8.5.1 Funktionalitäten

Der Prüfer will den Karteninhaber authentisieren.

Der Inhaber aktiviert auf dem PC eine „Authentisierungsanwendung“.

Die „Authentisierungsanwendung“ wählt einen Online-Server (E-Administration, E-Commerce usw.), der die Authentisierung und den Authentisierungsschlüssel anfordert.

Je nach dem vom Inhaber gewählten Prüfer muss die „Authentisierungsanwendung“ zulassen, dass das Authentisierungsprotokoll mit dem gewählten Authentisierungsschlüssel und den entsprechenden APSD initialisiert wird.

Sind auf der Karte mehrere unterschiedliche Authentisierungsschlüssel gleichzeitig vorhanden, muss der Inhaber einen auswählen, je nachdem, von welchem Prüfer er authentisiert werden will. Die IT-Umgebung, hauptsächlich die Authentisierungsanwendung, hilft dem Inhaber dabei, den richtigen Authentisierungsschlüssel sicher zu wählen. Es bleibt der IT-Umgebung überlassen, die Verknüpfung zwischen dem gewählten Authentisierungsschlüssel und dem Zertifikat des jeweiligen Schlüssels anzuzeigen. Dazu sowie auch zur Ermöglichung von Mobilität kann es sinnvoll sein, das Zertifikat bzw. die Zertifikatinformationen auf der Karte zu speichern; dies ist jedoch keine verpflichtende Anforderung.

### 6.8.5.2 Kommunikation

Die Kommunikation zwischen dem EVG und dem Prüfer ist das Authentisierungsprotokoll.

Ein Datenaustausch, der möglicherweise nach dieser Authentisierung stattfindet, wird durch das vorliegende Schutzprofil nicht abgedeckt.

Diese Authentisierung darf in einer nicht vertrauenswürdigen Umgebung stattfinden. Daher muss der EVG den in ISO/IEC 10181-2 genannten Bedrohungen durch Relay- und Replay-Angriffe über das Authentisierungsprotokoll entgegenwirken.

Das Kommunikationsprotokoll kann auch Bedrohungen entgegenwirken, die durch eine fehlerhafte CA entstehen, welche Zertifikate liefert, ohne die korrekte Herkunft des öffentlichen Schlüssels durch einen Besitznachweis („Proof of Possession“) zu überprüfen. In diesem Fall kann durch ein Authentisierungsprotokoll, das ein an den EVG geliefertes signiertes Zertifikat verwendet, eine korrekte Authentisierung dennoch sichergestellt werden.

## 6.8.6 Schlüsselerzeuger

### 6.8.6.1 Funktionalitäten

Der Schlüsselerzeuger erzeugt ein öffentliches Schlüsselpaar. Der private Schlüssel wird sicher an den EVG gesendet.

Die Umgebung muss sicherstellen, dass der öffentliche Schlüssel für die Zertifikaterzeugung sicher an die CA gesendet wird.

### 6.8.6.2 Kommunikation

Die Kommunikation zwischen dem Schlüsselerzeuger und dem EVG muss gesichert sein.

Während der Personalisierungsphase, die in einer vertrauenswürdigen Umgebung abläuft, kann diese Kommunikation in zwei Phasen unterteilt werden:

- Übertragung vom Schlüsselerzeuger an die Personalisierungsanwendung, anschließend
- Übertragung von der Personalisierungsanwendung an den EVG.

Die Übertragung von der Personalisierungsanwendung an den EVG muss durch den EVG geschützt sein.

## **6.8.7 Zertifizierungsinstanz**

### **6.8.7.1 Funktionalitäten**

Auf der Grundlage des empfangenen öffentlichen Schlüssels erzeugt die Zertifizierungsinstanz ein Zertifikat. Wenn das Schlüsselpaar auf dem EVG erzeugt wird, muss der öffentliche Schlüssel vom EVG gesendet werden.

Der ST-Autor muss die Identifikationsdaten festlegen und angeben, wie diese sicher an die CA zu übertragen und mit dem korrekten öffentlichen Schlüssel zu assoziieren sind.

Wenn der Schlüssel außerhalb des EVG erzeugt wird, muss die Umgebung sicherstellen, dass der öffentliche Schlüssel sicher an die CA übertragen wird.

Der öffentliche Schlüssel muss mit den richtigen Identitätsdaten übertragen werden, um sicherzustellen, dass kein falsches Zertifikat erstellt werden kann. Die CA muss die Erzeugung von Zertifikaten mit falscher Identität verhindern. Ein mögliches Mittel dazu ist der Besitznachweis („Proof of Possession“).

Das Zertifikat darf dann an die Karte gesendet werden. Es kann einige Angriffe auf Authentisierungsprotokolle verhindern.

### **6.8.7.2 Kommunikation**

Die Kommunikation zwischen dem EVG und der CA dient dazu, den öffentlichen Schlüssel zu übertragen.

Diese Authentisierung kann in einer vertrauenswürdigen oder einer nicht vertrauenswürdigen Umgebung stattfinden.

Die Kommunikation kann durch eine CGA gehen.

Ist die Gruppe „Trusted CA“ in der Konfiguration enthalten, dann muss die gesamte Umgebung zwischen EVG und CA durch die CGA vertrauenswürdig sein.

Der vertrauenswürdige Kanal muss zwischen dem EVG und der CA eingerichtet werden.

## **6.8.8 Anwendungsbeispiele**

### **6.8.8.1 Allgemeines**

Dies in diesem Abschnitt allgemein beschriebene EVG-Umgebung deckt sehr unterschiedliche Umgebungen ab.

### **6.8.8.2 Einfache Zugriffskontrolle**

Der einfachste Fall ist eine Zugriffskontrollanwendung innerhalb eines Unternehmens, bei der das PKI-Management innerhalb des Unternehmens erfolgt und die IT-Umgebung sicher, d. h. gegen Angriffe von außen geschützt ist.

Bei dieser einfachen Anwendung ist die Kommunikation zwischen EVG und Prüfer durch die IT-Umgebung geschützt.

Die PKI wird intern verwaltet. Sie generiert und verwaltet Zertifikate und aktualisiert regelmäßig die Liste der vom Prüfer verwendeten gültigen Zertifikate.

Ausgeber und Administration gehören zum Unternehmen und verwenden die sichere interne IT.

Bei einer derartigen einfachen Anwendung benötigt der EVG nur seinen privaten Authentisierungsschlüssel. Das prüferbezogene Authentisierungsprotokoll darf sehr einfach sein. Der Prüfer erzeugt eine Zufallsnachricht, sendet diese an den EVG, der sie signiert und an den Prüfer zurücksendet.

Jegliche Kommunikation im sicheren IT-Netz ist geschützt.

### **6.8.8.3 E-Government**

E-Government-Anwendungen, die einem Inhaber den Zugriff auf persönliche Daten über einen Heim-PC erlauben, z. B. Punktestand im Zusammenhang mit Verkehrsverstößen

Die E-Government-Anwendung kann das Zertifikat aus der PKI beziehen. Sie kann jedoch auch darauf angewiesen sein, dass das Authentisierungsprotokoll den öffentlichen Schlüssel bereitstellt, z. B. mit in einem signierten Zertifikat.

Die Kommunikation zwischen der Authentisierungsanwendung und dem EVG darf für Folgendes als sicher angesehen werden:

- die Inhaberauthentisierung;
- die Annahme der Authentisierung des EVG mit dem Authentisierungsschlüsselpaar.

### **6.8.8.4 Sonstige Anwendungen**

E-Administration für Steuerzahlung mit erforderlicher Signatur + E-Commerce nur mit Authentisierung

Das E-Administration- und das E-Commerce-Center können das Zertifikat aus der PKI beziehen. Sie können sich aber auch darauf verlassen, dass das Authentisierungsprotokoll den öffentlichen Schlüssel sicher bereitstellt, z. B. in einem signierten Zertifikat.

Die Kommunikation zwischen der Authentisierungsanwendung und dem EVG kann für Folgendes als sicher angesehen werden:

- Inhaberauthentisierung;
- Auswahl des Online-Servers;
- Auswahl eines bestimmten Authentisierungsschlüsselpaars;
- Annahme der Authentisierung des EVG.

## 6.9 Lebenszyklus

### 6.9.1 Überblick

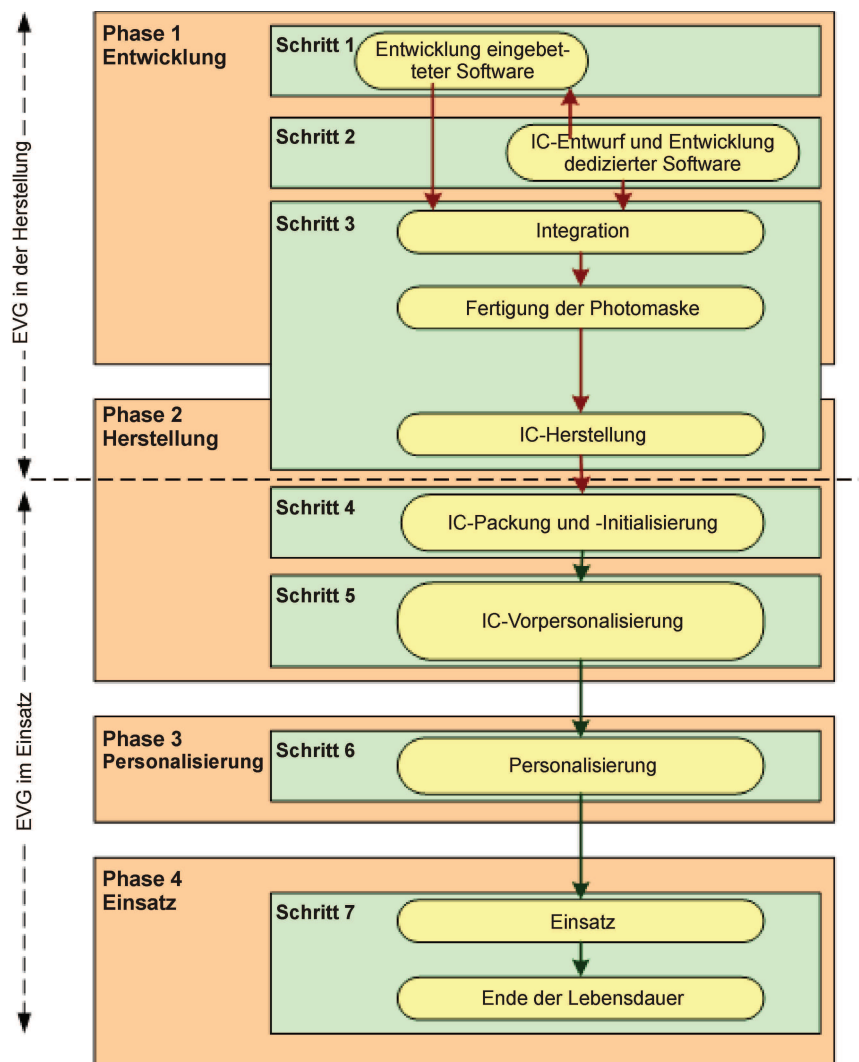


**Bild 5 — EVG Lebenszyklus**

Dieses Bild zeigt zwei Sichten des Lebenszyklus:

- eine aus 4 Phasen bestehende „Endbenutzer“-Sicht, unter besonderer Konzentration auf die folgenden wesentlichen logischen Phasen:
  - Entwicklungsphase: IC-Planung und Entwicklung eingebetteter Software;
  - Herstellungsphase: von der IC-Herstellung bis zur Herstellung der Karte bzw. des Tokens, einschließlich des Ladens von Patches, der Anwendungserzeugung und der Vorpersonalisierung;
  - Personalisierungsphase: Laden aller mit dem EVG-Inhaber zusammenhängenden Daten;
  - Einsatzphase: Nutzung des EVG durch seinen rechtmäßigen Inhaber zur Authentisierung gegenüber einem Prüfer;

- b) eine aus 7 Schritten bestehende geschäftsbezogene Sicht, die sich stärker auf die unterschiedlichen Branchen und Akteure konzentriert, welche an der Herstellung und Verwendung von Chipkarten beteiligt sind. Zum Beispiel kann das Unternehmen, das für die IC-Herstellung verantwortlich ist, ein anderes sein als das, das für die Packung zuständig ist; und auch mit Packung, Initialisierung und Vorpersonalisierung kann wiederum ein anderes Unternehmen betraut sein, ganz abgesehen von den an dieser Phase beteiligten übrigen Akteuren: Antennenlieferanten, Broschürenlieferanten. Die Definition des Inhalts jedes Schritts und die zugehörige Lieferkette variieren von Anbieter zu Anbieter, Bild 4 ist daher nur als Beispiel zu verstehen.

Das **evaluierte Produkt** ist im Lebenszyklus das Produkt, das das Ergebnis der IC-Herstellung, der Prüfung und einer eventuellen Vorpersonalisierung ist (**Schritt 3**).

An dieser Stelle muss das Produkt bereits über einen Selbstschutz verfügen, bevor es an Schritt 4 und alle anschließenden Schritte übergeben wird. Das bedeutet, dass, wenn zum Schließen einer Sicherheitslücke ein Patch in das Produkt zu laden ist, dies während des Schritts der IC-Herstellung erfolgen muss, d. h. in einer Umgebung, die der Evaluierung unterliegt und nach einer CC-Vertrauenswürdigkeitsklasse bewertet wird, die sich auf die Entwicklungsumgebung bezieht (ALC).

Die Berücksichtigung folgender Optionen ist ebenfalls wichtig:

- Erzeugung der Anwendung;
- Applet-Installation für JavaCard;
- Laden der *Vorpersonalisierungsdaten* in den Chip.

Diese Operationen können, je nach Betriebsorganisation für die EVG-Produktion, auf dem durch den Evaluationsbereich abgedeckten sicheren Gelände des IC-Herstellers ausgeführt werden oder auch nicht. Sie können sogar während der Personalisierungsphase (Schritt 6) unter Kontrolle des Ausgeberstaates erfolgen.

Wenn diese Operationen jedoch nicht auf dem sicheren Gelände des IC-Herstellers ausgeführt werden, müssen die Vorgehensweisen zur Ausführung dieser Operationen genau definiert und durch CC-Vertrauenswürdigkeitsaufgaben im Zusammenhang mit der Handbuchanalyse (Klasse AGD) erfolgreich evaluiert sein.

Allgemeiner lässt sich festhalten, dass alle Schritte im Anschluss an Schritt 3 durch die Klasse „Handbücher“ abgedeckt sein müssen (sichere Übergabe, sichere Handhabung usw.).

Der Autor des Sicherheitsziels kann sich dafür entscheiden, Schritt 4 und auch Schritt 5 in den Evaluationsumfang mit aufzunehmen. In diesem Fall wird das Gelände, auf dem diese Operationen stattfinden, nicht durch AGD, sondern durch ACL abgedeckt, und sensible Operationen wie das Laden von Patches mit Auswirkung auf Sicherheitsfunktionen können in den entsprechend aufgenommenen Schritten ausgeführt werden.

## 6.9.2 Vorpersonalisierungsphase

Die Vorpersonalisierung ist die letzte Phase, die der Kontrolle des Chipkartenherstellers unterliegt.

### — Anwendungsinitialisierung

Während der Vorpersonalisierung initialisiert der Chipkartenhersteller die Anwendung.

### — Import der Ausgeber-RAD

Der Hersteller importiert die Ausgeber-RAD, die in der nächsten Phase zur Authentisierung des Ausgebers verwendet werden.

## 6.9.3 Personalisierungsphase

### 6.9.3.1 Allgemeines

Die Personalisierungsphase findet unter der Kontrolle des Ausgebers statt.