# Bestätigung
## von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 S. 1 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und § 11 Abs. 3 Signaturverordnung[2]

SRC Security Research & Consulting GmbH
Graurheindorfer Straße 149 A
53117 Bonn

**bestätigt hiermit gemäß**
**§§ 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §§ 15 Abs. 1 und 4, 11 Abs. 3 SigV,**
**dass die**

Signaturerstellungseinheit
„STARCOS 3.5 ID ECC C1R“

**den nachstehend genannten Anforderungen des SigG und der SigV entspricht.**

---

Die Dokumentation zu dieser Bestätigung ist registriert unter:

SRC.00021.TE.05.2013

Bonn, den 13.05.2013

Detlef Kraus  Thomas Hueske

Die SRC Security Research & Consulting GmbH ist gemäß der Veröffentlichung im Amtsblatt der Bundesnetzagentur Nr. 19 unter der Mitteilung Nr. 605/2008 zur Erteilung von Bestätigungen für Produkte gemäß §§ 17 Abs. 4 S. 1, 15 Abs. 7 S. 1 SigG ermächtigt.

---

[1] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542)

# Beschreibung des Produktes für qualifizierte elektronische Signaturen:

## 1. Handelsbezeichnung des Produktes und Lieferumfang

### 1.1 Handelsbezeichnung

Signaturerstellungseinheit STARCOS 3.5 ID ECC C1R der Giesecke & Devrient GmbH (im Folgenden kurz als „GD-Signaturkarte“ bezeichnet).

In Abhängigkeit der zugrundeliegenden Hardwarevariante wird das Produkt auch unter den Bezeichnungen STARCOS 3.5 ID ECC C1R/360, /800 oder /1280 vertrieben. Die Hardwarevarianten unterscheiden sich nur hinsichtlich der zur Verfügung stehenden Speicherplatzgrößen.

### 1.2 Auslieferung

Die „GD-Signaturkarte“ ist realisiert als sogenannte Dual Interface Karte, d.h. die Karte verfügt über eine kontaktbehaftete und eine kontaktlose Schnittstelle. Je nach Konfiguration kann die Karte als ausschließlich kontaktbehaftete, ausschließlich kontaktlose oder als Dual Interface Karte eingesetzt werden. Die Hardware der „GD-Signaturkarte“ besteht aus dem Chip Infineon M7820 A11, wobei die ebenfalls zur Verfügung gestellte Kryptobibliothek für Crypto@2304T nicht verwendet wird. Die Software besteht aus dem Betriebssystem STARCOS 3.5 ID (ROM, ggf. teilweise im EEPROM), welches auch die benötigten Kryptofunktionen beinhaltet, sowie aus der Anwendung zur Erzeugung qualifizierter elektronischer Signaturen, die im Weiteren als „SSCD-Anwendung“ bezeichnet wird (SSCD steht für Secure Signature Creation Device).

Die Smartcard Embedded Software enthält das Betriebssystem STARCOS 3.5 ID. Diese Plattform stellt eine ISO-7816 kompatible, multifunktionale Plattform zur Verfügung, die für Karten zum Einsatz in Anwendungen mit hohen Sicherheitsanforderungen geeignet ist. Die Karte verfügt über die *SSCD-Anwendung* und kann grundsätzlich mit weiteren Anwendungen versehen werden. Diese sind jedoch nicht Gegenstand der vorliegenden Bestätigung.

Die „GD-Signaturkarte“ wird als Karte mit *SSCD-Anwendung* vom Zertifizierungsdiensteanbieter (ZDA) an den Endkunden ausgeliefert. Hierzu bezieht der ZDA die Karten vom Chiphersteller und initialisiert sie mit den von der Giesecke & Devrient GmbH bereitgestellten Skripten. Dabei wird das durch den Hersteller vorbereitete Skript zur Initialisierung/Pre-Personalisierung gesichert an die Karte gesendet. Alternativ hierzu, kann der ZDA bereits initialisierte Karten beziehen.

Die Personalisierung der Karte erfolgt ebenfalls beim Zertifizierungsdiensteanbieter (bzw. bei einem beauftragten Dritten), der die spezifischen Daten in die Karte einbringt und sie anschließend an den Endkunden ausliefert. Als Transport-Schutz bei der Auslieferung zum Kunden wird eine spezifische Transport-PIN eingebracht oder das Leer-PIN-Verfahren verwendet. Die karteninterne Generierung des Signaturschlüsselpaars kann bereits mit der Personalisierung oder nach der Auslieferung durch den Kunden erfolgen. Möglich ist auch eine Kombination der beiden Verfahren, wobei das erste Schlüsselpaar während der Personalisierung und alle weiteren nach der Auslieferung durch den Kunden erzeugt werden.

Die Authentizität und Integrität der Module / Karten können wie folgt verifiziert werden:

Für die bestätigte Version der STARCOS 3.5 ID ECC C1R sind in [UG_Ini] die herstellerspezifischen Werte zu den Parametern „Chip Manufacturer Data“, „OS Manufacturer“, „OS Version number“ und „Version of ROM mask“ angegeben. Sie können während der Produktion mit dem Kommando „GET PROTOCOL DATA“ gemäß [UG_Ini], Kapitel 5.3.9 bzw. [UG_Pers], Kapitel 5.3.20 sowie während der Usage Phase aus der Karte ausgelesen werden. Während der Usage Phase können der Komplettierungsstand und die Version des Betriebssystems gelesen werden. Das Lesen von kartenindividuellen Informationen kann in dieser Phase unterbunden werden. Die ROM-Maske ist gekennzeichnet als CIF9DSCSR35-01c_V200.

## 1.3 Lieferumfang

Der Lieferumfang des Produktes besteht aus den folgenden Komponenten:

**Tabelle 1: Lieferumfang**

| Nr. | Typ | Bezeichnung | Version | Datum | Auslieferung |
|---|---|---|---|---|---|
| 1 | Hardware / Software | Infineon M7820 A11, inklusive dedizierter Test-Software<br><br>(SLE78CLX360P, SLE78CLX800P, SLE78CLX1280P)<br><br>(Zertifizierung unter BSI-DSZ-CC-0813-2012) | | | --- |
| 2 | Software (Betriebssystem) | Smartcard Embedded Software (Betriebssystem) STARCOS 3.5 ID (implementiert im ROM/EEPROM des Halbleiters)[3] | | | --- |
| 3 | Kryptographische Schlüssel | Kryptographische Schlüssel für die Initialisierung oder Personalisierung zum Schutz vor unberechtigter Modifikation | | | In elektronischer Form, zum Schutz vor Offenlegung bzw. Modifikation verschlüsselt und signiert |
| 4 | Software (Anwendungssoftware einschließlich Filesystem) | Smartcard Embedded Anwendung (als Initialisierungstabelle) zur Signaturerzeugung gemäß [UG_GenApp] | | | --- |
| 5 | Dokumentation | Guidance Documentation STARCOS 3.5 ID ECC C1 Main Document [UG_Main] | 0.6 | 19.10.2011 | Dokument in elektronischer Form |

[3] Hinweis: Es kann auch eine Auslieferung ohne Initialisierungstabelle erfolgen.

| Nr. | Typ | Bezeichnung | Version | Datum | Auslieferung |
|---|---|---|---|---|---|
| 6 | Dokumen-tation | Guidance Documentation for the Initialisation phase STARCOS 3.5 ID ECC C1 [UG_Ini] | 1.5 | 15.06.2012 | Dokument in elektronischer Form |
| 7 | Dokumen-tation | Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID ECC C1 [UG_Pers] | 0.8 | 15.06.2012 | Dokument in elektronischer Form |
| 8 | Dokumen-tation | Guidance Documentation for the Usage Phase STARCOS 3.5 ID ECC C1 [UG_Use] | 1.2 | 27.06.2012 | Dokument in elektronischer Form |
| 9 | Dokumentation | Generic Application of STARCOS 3.5 ID ECC C1R [UG_GenApp], Spezifikation des Filesystems | | Januar 2013 | Dokument in elektronischer Form |

## 1.4 Hersteller

Hersteller des Produktes ist die Giesecke & Devrient GmbH, Prinzregentenstrasse 159, Postfach 80 07 29, D-81607 München.

# 2. Funktionsbeschreibung

## Funktionalität und Architektur

Die „GD-Signaturkarte“ ist realisiert als sogenannte Dual Interface Karte, d.h. die Karte verfügt über eine kontaktbehaftete und eine kontaktlose Schnittstelle. Je nach Konfiguration kann die Karte als ausschließlich kontaktbehaftete, ausschließlich kontaktlose oder als Dual Interface Karte eingesetzt werden. Die Hardware der „GD-Signaturkarte“ besteht aus dem Chip Infineon M7820 A11, wobei die zugehörige Kryptobibliothek nicht verwendet wird. Der Chip Infineon M7820 A11 wurde nach CC 3.1 evaluiert und zertifiziert (BSI-DSZ-CC-0813-2012).

Die Software besteht aus dem Betriebssystem STARCOS 3.5 ID (ROM, ggf. teilweise im EEPROM) sowie aus der *SSCD-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen.

Das Betriebssystem STARCOS 3.5 ID stellt eine interoperable, ISO 7816-konforme, multi-funktionale Plattform zur Verfügung, die für Karten zum Einsatz in Anwendungen mit hohen Sicherheitsanforderungen geeignet ist. Das umfangreiche Angebot verschiedener technischer und funktionaler Eigenschaften sowie von Sicherheitseigenschaften des STARCOS Betriebssystems unterstützt insbesondere die *SSCD-Anwendung*. Neben der dedizierten *SSCD-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen können sich grundsätzlich weitere Anwendungen auf der „GD-Signaturkarte“ befinden. Diese sind jedoch **nicht** Gegenstand der vorliegenden Bestätigung.

Darüber hinaus bietet das Betriebssystem u.a. die folgende Funktionalität:

- Dateisystem gemäß ISO 7816
- Zugriffskontrolle des Dateisystems
- Authentikation von Komponenten
- Secure Messaging zur sicheren Kommunikation mit der externen Welt
- Schlüssel- und PIN-Management
- PIN basierte Benutzerauthentikation
- Erzeugung von Elliptische Kurven Schlüsseln
- Erzeugung von RSA Schlüsseln
- Erzeugung von elektronischen Signaturen (Elliptische Kurven)
- Erzeugung von elektronischen Signaturen (RSA)

Zusammenfassend besteht die „GD-Signaturkarte“ insbesondere aus den folgenden Komponenten:

- Halbleiter (IC) von Infineon mit dedizierter Software,
- Betriebssystem STARCOS 3.5 und
- der *SSCD-Anwendung* mit den entsprechenden Datenstrukturen zur Speicherung und Verwaltung von Daten des Inhabers der Sicheren Signaturerstellungseinheit (Signatur-PIN, Signaturschlüssel) als auch den Daten für die Authentikation (Schlüssel für Authentikationsprotokolle).

Bevor die *SSCD-Anwendung* genutzt werden kann, ist diese noch zu vervollständigen. Dabei kann die noch ausstehende Generierung des Signaturschlüssels entweder

- vor der Auslieferung durch den Zertifizierungsdiensteanbieter (ZDA) (bzw. einen beauftragten Dritter), wobei auch direkt das Zertifikat erstellt werden kann, oder
- nach der Auslieferung an den Karteninhaber unter Kontrolle eines zertifikatsausstellenden ZDA

erfolgen. Wird das Signaturschlüsselpaar nach der Auslieferung erzeugt, muss für die Zertifikatserstellung der öffentliche Signaturschlüssel durch den ZDA sicher ausgelesen werden.

Optional kann das erstellte Zertifikat auch auf der „GD-Signaturkarte“ abgespeichert werden. Im Rahmen dieser Komplettierung der *SSCD-Anwendung* müssen, soweit nicht bereits vorhanden, noch die Transport-PIN und die Transport-PUK in der Karte gesetzt werden.

Um mit der komplettierten *SSCD-Anwendung* eine Signatur erzeugen zu können, muss der designierte Signaturschlüsselinhaber die „GD-Signaturkarte“ als sichere Signaturerstellungseinheit (SSEE) aktivieren. Dazu muss er die voreingestellte und maximal fünfstellige Transport-PIN durch eine gültige Signatur-PIN ersetzen. Weiterhin setzt der designierte Signaturschlüsselinhaber den Resetting-Code (im Folgenden auch als PUK bezeichnet). Zum Setzen der PUK muss er die voreingestellte und maximal fünfstellige Transport-PUK durch eine gültige PUK ersetzen. Das Setzen der PUK erfolgt einmalig. Sie kann nachträglich nicht mehr verändert werden. Die Verwendung der PUK ist optional.

Nach Aktivierung der *SSCD-Anwendung* kann die „GD-Signaturkarte“ zur Erzeugung qualifizierter Signaturen genutzt werden. Voraussetzung zur Erzeugung einer qualifizierten Signatur ist die erfolgreiche Benutzerauthentisierung des Signaturschlüsselinhabers mittels korrekter Eingabe der Signatur-PIN.

Die „GD-Signaturkarte“ unterstützt die optionale Verwendung von zwei Signaturschlüsseln (z.B. ein RSA-Signaturschlüssel und ein Signaturschlüssel für elliptische Kurven). Der Zugriff auf die Signaturschlüssel kann entweder durch eine gemeinsame Signatur-PIN geschützt werden oder jeder Signaturschlüssel verfügt über seine eigene Signatur-PIN. Im Falle eigener Signatur-PINs verfügt jede Signatur-PIN auch über eigene Sicherheitsattribute (z.B. Transport-PIN, Transport-PUK, PUK, Fehlbedienungszähler (FBZ)). Die „GD-Signaturkarte“ kann somit in den folgenden Varianten genutzt werden:

- Signaturkarte mit einem Signaturschlüssel (RSA oder elliptische Kurven) und einer Signatur-PIN,
- Signaturkarte mit einem optionalen zweiten Signaturschlüssel (RSA und elliptische Kurven) und einer gemeinsamen Signatur-PIN und
- Signaturkarte mit zwei Signaturschlüsseln (RSA und elliptische Kurven) und separaten Signatur-PINs für jeden Signaturschlüssel.

Die Variante wird im Rahmen der Initialisierung der Karte durch das verwendete Initialisierungsfile festgelegt und kann nachträglich nicht mehr verändert werden.

Die „GD-Signaturkarte“ ist eine sogenannte Multisignatur-fähige sichere Signaturerstellungseinheit (Multisignatur-SSEE) mit der nach einer erfolgreichen Eingabe der Signatur-PIN entweder genau eine, eine begrenzte Anzahl oder eine unbegrenzte Anzahl an qualifizierten Signaturen erzeugt werden können. Der Wert wird im Rahmen der Initialisierung festgelegt (Wert n des Signaturzählers) und kann anschließend nicht mehr verändert werden. Die „GD-

Signaturkarte“ kontrolliert die Einhaltung eines begrenzten Signaturzählers, d.h. nach Erzeugung von n Signaturen können keine weitere Signaturen ohne erneute Eingabe der Signatur-PIN generiert werden. Mit Ausführung eines Resets wird der Sicherheitszustand "Signatur-PIN erfolgreich eingegeben" in der „GD-Signaturkarte“ gelöscht. Anschließend muss die Signatur-PIN erneut eingegeben werden, um Signaturen erzeugen zu können (s.a. Sicherheitsfunktion "Prozesse der PIN-basierten Authentisierung (Signatur-PIN)"). Die Verwendung einer Multisignatur-SSEE bedingt spezifische Einsatzbedingungen (s. Einsatzbedingungen an die Nutzung des Signaturzählers in Kapitel 3.2).

Die *SSCD-Anwendung* kann durch den Signaturschlüsselinhaber administriert werden. Hierzu gehören die folgenden Funktionen

- Wechsel der Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der aktuell gültigen Signatur-PIN),
- Rücksetzen des Fehlbedienungszählers der Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der PUK) und
- Außerbetriebnahme eines Signaturschlüssels mit Terminieren der Signatur-PIN und des Signaturschlüssels.
- Zusätzlich erlaubt die „GD-Signaturkarte“ auch das Löschen eines Signaturschlüssels.

Nach einer Außerbetriebnahme kann eine erneute Aktivierung erfolgen, d.h. es kann eine neue Signatur-PIN nach dem nur in diesem Kartenzustand möglichen Leer-PIN-Verfahren gesetzt werden. Danach kann auch ein neuer Signaturschlüssel in der Karte generiert sowie ein qualifiziertes Zertifikat erzeugt und optional dieses in die Karte eingebracht werden. Die bei einer ersten Aktivierung einmalig gesetzte PUK kann jedoch nicht mehr verändert werden.

Für die Signaturanwendung relevanten Zugriffe unterstützt die „GD-Signaturkarte“ die Anwendung von Secure Messaging. Zur gegenseitigen Authentisierung von Terminal und Karte sowie zum Aufbau eines sicheren Kommunikationskanals werden die Authentisierungsprotokolle Password Authentication Connection Establishment (PACE), Terminal- und Chipauthentisierung sowie ein Authentisierungsprotokoll auf Basis symmetrischer Algorithmen gemäß [EN 14890-1], Kapitel 8.8 verwendet. Im Rahmen der Terminalauthentisierung werden Zugriffsrechte eines Terminals nachgewiesen. Hierzu gehört insbesondere auch das Recht eines ZDA zur Erzeugung eines Signaturschlüsselpaars auf der „GD-Signaturkarte“ und zum sicheren Auslesen des öffentlichen Signaturschlüssels.

Die Sicherheitseigenschaften der „GD-Signaturkarte“ werden mit der Beschreibung der Sicherheitsfunktionen weiter erläutert (s. Kapitel 3.2).

Das STARCOS Betriebssystem erlaubt dem Kartenhersteller eine Reihe von Konfigurationsmöglichkeiten. Vor der Initialisierung hat der Kartenhersteller die Konfiguration insbesondere durch die Erstellung des Filesystems festgelegt. Die Installationsdaten zum Laden des Filesystems werden vom Kartenhersteller an den Initialisierer der Karte ausgeliefert. Vertraulichkeit und Integrität der Daten sowie deren authentischer Ursprung werden durch kryptographische Verfahren sichergestellt.

Die Installation des Filesystems erfolgt während der Initialisierung des Chips (Komplettierung des OS-Code und Laden des Filesystems) durch den Initialisierer. Die Installation des Filesystems kann nur nach einer Authentisierung des Initialisierungssystems gegenüber der Karte erfolgen. Die zur kryptographischen Absicherung der Ladedaten verwendeten Schlüssel sind lediglich dem Kartenhersteller bekannt. In diesem Sinn kann man von einer Ende-zu-Ende-Sicherung zwischen Kartenhersteller und Chip sprechen. Das Laden von unautorisiert geänderten Initialisierungsdaten kann hierdurch verhindert werden. Ein nachträgliches Einbringen weiterer Software wird durch die „GD-Signaturkarte“ nicht unterstützt.

Zur Erzeugung von Signaturschlüsselpaaren sowie von qualifizierten elektronischen Signaturen werden durch die „GD-Signaturkarte“ die folgenden kryptographischen Algorithmen unterstützt:

- DSA auf Basis elliptischer Kurven (ECDSA) basierend auf Gruppen $E(F_p)$ (vgl. [TR-03111]),
- Asymmetrischer RSA Algorithmus gemäß [PKCS#1] mit einer Schlüssellänge von 2048 Bit bis 4096 Bit,
- Hashfunktion SHA-2 (224, 256, 384 oder 512 Bit) gemäß [FIPS 180-2], sowie
- Zufallszahlenerzeugung auf Basis eines deterministischen Zufallszahlengenerators (DRNG), dessen Seed durch die zugrundeliegende Hardware generiert wird. Der DRNG wurde im Rahmen der Evaluierung als DRG.4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet.
- Der Zufallszahlengenerator der zugrundeliegenden Hardware von Infineon ist ein True Random Number Generator mit einer PTG.2 Klassifizierung gemäß [AIS 31]. Die Zufallszahlen werden im laufenden Betrieb statistischen Tests unterzogen („Onlinetests“). Diese Eigenschaften wurden im Rahmen der CC Evaluierung der Hardware von Infineon geprüft (vgl. [STHW] und [IFX_Cert]).

Die „GD-Signaturkarte“ unterstützt die ECC Brainpool Kurven P224r1[4], P256r1, P320r1, P384r1 und P512r1 gemäß [TR-03111] sowie die NIST Kurven secp256r1, secp384r1 und secp521r1 gemäß [SEC 2].

Die Erzeugung von Hashwerten kann entweder innerhalb der „GD-Signaturkarte“ mit dem Kommando PSO: HASH durchgeführt oder vollständig außerhalb der Karte vorgenommen werden. Das Kommando PSO: HASH kann zudem für einen gemischten Mode verwendet werden. Hierzu wird der erste Teil der zu signierenden Daten zunächst außerhalb der Karte gehasht und anschließend der so berechnete Zwischenwert und der Rest der Daten an die Karte übergeben, um den endgültigen Hashwert in der Karte zu berechnen. Grundsätzlich lässt das Kommando PSO: HASH ein sogenanntes Chaining zu, um den Hashwert zu signierender Daten, deren Länge die maximal mögliche Inputlänge des Kommandos übersteigt, durch ein iteratives Anwenden des Kommandos PSO: HASH zu berechnen. Grundsätzlich muss jeder an die „GD-Signaturkarte“ übergebene Hashwert mit einem Message Authentication Code (MAC) gesichert werden.

[4] Wird nur zur Authentikation und nicht zur Signaturerzeugung verwendet.

Weiterhin werden die folgenden Algorithmen unterstützt. Diese werden jedoch bei der Erstellung von qualifizierten elektronischen Signaturen sowie bei der Erzeugung von Signaturschlüsselpaaren nicht verwendet.

- Diffie-Hellman gemäß [TR-03110] zur Authentisierung (PACE, Terminal- und Chipauthentisierung) und Schlüsselvereinbarung für den Secure Messaging Kanal.
- Symmetrischer AES Algorithmus gemäß [FIPS 197] mit einer effektiven Schlüssellänge von 128, 192 oder 256 Bit.

Die „GD-Signaturkarte“ wurde auf Basis der Common Criteria in der Version 3.1 erfolgreich evaluiert [ETR]. Die Zertifizierung des Produktes erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem Sicherheitszertifikat BSI-DSZ-CC-0880. Die Prüftiefe beträgt EAL 4+ mit der Augmentierung AVA_VAN.5.

Weiterhin berücksichtigt die „GD-Signaturkarte“ das Protection Profile „Protection profiles for Secure signature creation device – Part 2: Device with key generation", prEN 14169-2:2012, Version 2.0.1; 2012-01, BSI-CC-PP-0059-2009-MA-01 [BSI-CC-PP-0059].

## Sicherheitsfunktionen bzw. –eigenschaften der „GD-Signaturkarte“

Die „GD-Signaturkarte“ stellt u.a. die nachfolgend aufgeführten Sicherheitsfunktionen und Sicherheitseigenschaften zur Verfügung. Sie sind im Security Target [ST] beschrieben und wurden im Rahmen der Evaluierung verifiziert.

### „Zugriffskontrolle“

Die „GD-Signaturkarte“ verwendet eine rollenbasierte Zugriffskontrolle. Diese unterscheidet u.a. zwischen den Rollen „Administrator“ (Administrator bzw. „R.Admin“) und „Signierer“ (Signatory bzw. „R.Sigy“). Weiterhin werden die folgenden Sicherheitsattribute verwendet:

- Für eine authentisierte Rolle: „SCD / SVD Management“ (Werte: „authorized“, „not authorized“)
- Für das Datenobjekt Secure Creation Data (SCD, der Signaturschlüssel): „SCD operational“ (Werte: „no“, „yes“)

Ein Anwender authentisiert sich gegenüber der „GD-Signaturkarte“ durch die Kenntnis eines geheimen Schlüssels als Administrator (wie bspw. Initialisierer oder Personalisierer) bzw. durch Eingabe der Signatur-PIN als Signierer. Der Zertifizierungsdiensteanbieter (ZDA), der insbesondere die Zertifikatserstellung durchführt und hierzu über Zugriffsrechte verfügt, agiert ebenfalls in der Rolle des Administrators.

In der Nutzungsphase wird die Anwendung eines sicheren Kanals sowohl bei Verwendung der kontaktbehafteten als auch der kontaktlosen Schnittstelle durch die „GD-Signaturkarte“ unterstützt. Bei der Nutzung der kontaktbehafteten Schnittstelle in einer sicheren Umgebung kann die Verbindung zwischen der „GD-Signaturkarte“ und der Signaturanwendung optional kryptographisch abgesichert werden. In einer unsicheren Umgebung sowie bei jeder Kommunikation mit der zertifikaterzeugenden Anwendung des ZDA muss die Verbindung mit

Secure Messaging abgesichert werden. Eine Nutzung der kontaktlosen Schnittstelle kann ausschließlich unter Anwendung eines sicheren Kanals erfolgen.

Dabei können die Sitzungsschlüssel durch verschiedene Verfahren ausgehandelt werden. Über die kontaktbasierte Schnittstelle stellt die „GD-Signaturkarte“ sowohl eine symmetrische als auch eine asymmetrische (Chip- und Terminal-) Authentisierung zur Verfügung. Im Fall der kontaktlosen Schnittstelle sind es PACE, Chip- und Terminalauthentisierung bzw. PACE mit AES-Schlüsseln. Zusammenfassend werden zur gegenseitigen Authentisierung und zum Aufbau eines sicheren Kommunikationskanals die folgenden Authentisierungen verwendet:

- **PACE Protokoll** zur gegenseitigen Authentisierung und Aufbau eines sicheren Kanals insbesondere zur Absicherung der Luftschnittstelle zwischen Karte und Terminal.
- **Terminalauthentisierung** zur Authentisierung des Terminals gegenüber der Karte und zum Nachweis der damit für das Terminal verbundenen Zugriffsrechte (z.B. das Recht zum Erzeugen einer qualifizierten Signatur).
- **Chipauthentisierung** zur Authentisierung des Chips gegenüber dem Terminal sowie Aufbau eines sicheren Kanals zur verschlüsselten und integritätsgesicherten Kommunikation zwischen Karte und Terminal.
- **Authentisierung mit symmetrischen Schlüsseln** zur gegenseitigen Authentisierung und Aufbau eines sicheren Kanals.

Weiterhin ist die Zugriffskontrolle realisiert unter Anwendung von Zugriffsbedingungen, die als Sicherheitsattribute in der „GD-Signaturkarte“ hinterlegt sind. Zugriff auf ein DF, EF, einen Schlüssel oder eine PIN ist nur erlaubt, sofern die entsprechenden Zugriffsbedingungen erfüllt sind. Dazu prüft die Sicherheitsfunktion vor Ausführung des Kommandos, ob insbesondere die spezifischen Anforderungen hinsichtlich Benutzerauthentisierung und sicherer Kommunikation erfüllt sind.

Es gelten in der Nutzungsphase u.a. die folgenden Regeln:

- Eine Schlüsselgenerierung ist nur dann möglich, wenn das Sicherheitsattribut „SCD/SVD Management” den Wert „authorized“ besitzt.
- Die PIN für den Transport-Schutz kann nur im Rahmen der Personalisierung gesetzt werden.
- Ein Export sensitiver Informationen (z.B. Signaturschlüssel, Transport-PIN, Signatur-PIN) über die Betriebssystem-Kommandos ist aufgrund der gesetzten Zugriffsregeln nicht möglich.
- Das Ersetzen der Transport- durch eine Signatur-PIN durch den designierten Signaturschlüsselinhaber kann nur im initialen bzw. im terminierten Zustand (für das Datenobjekt SCD hat das Attribut „SCD operational“ den Wert „no“, d.h. insbesondere ist der Signaturschlüssel auf der Karte nicht nutzbar) der „GD-Signaturkarte“ nach einer erfolgreichen Benutzerauthentisierung erfolgen.
- Das Wechseln einer bestehenden Signatur-PIN in eine neue Signatur-PIN durch den Signaturschlüsselinhaber kann nur nach einer erfolgreichen Benutzerauthentisierung mit der alten Signatur-PIN erfolgen.
- Die PUK kann durch den designierten Signaturschlüsselinhaber bei einer ersten Aktivierung des Signaturschlüssels gesetzt werden. Hierzu muss die PUK im

Transportstatus sein. Nach Setzen der PUK ist die PUK im Status "activated". Ein Rücksetzen des Status ist dann nicht mehr möglich, d.h. die PUK kann nur einmal gesetzt werden und kann nachträglich nicht mehr verändert werden.

- Die Außerbetriebnahme der Signaturfunktion setzt eine erfolgreiche Benutzerauthentisierung voraus. Nach einer erfolgreichen Außerbetriebnahme eines Signaturschlüssels kann dieser nicht mehr zur Erzeugung qualifizierter Signaturen verwendet werden.
- Signaturen können nur durch den Signaturschlüsselinhaber generiert werden. Hierzu ist eine vorherige erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erforderlich.

**„Password Authenticated Connection Establishment (PACE) Protokoll“**

Die „GD-Signaturkarte“ unterstützt die Durchführung des Password Authenticated Connection Establishment (PACE) Protokolls. Das PACE Protokoll ist ein Passwort basiertes Protokoll zur Vereinbarung von Schlüsseln auf der Basis von Diffie-Hellman (DH). Es beinhaltet den Nachweis, dass die „GD-Signaturkarte“ und das Terminal über einen gleichen Ausgangswert verfügen (Speicherung in der Karte und Eingabe durch den Karteninhaber in das Terminal) und etabliert einen sicheren Kanal zwischen „GD-Signaturkarte“ und Terminal insbesondere zur Absicherung der kontaktlosen Schnittstelle (Luftschnittstelle). Durch die Verwendung spezifischer Geheimnisse als Ausgangswert kann zusätzlich eine Bindung an den Karteninhaber erfolgen.

Die erfolgreiche Durchführung des PACE Protokolls als notwendige Voraussetzung zur Nutzung der „GD-Signaturkarte“ unterstützt die Kontrolle des Signaturschlüsselinhabers über die sichere Signaturerstellungseinheit bei Anwendung der Karte über die Luftschnittstelle.

In Abhängigkeit der durchzuführenden Funktion können für das PACE Protokoll eine Card Access Number (CAN) oder eine Pairing Card Access Number (PCAN) genutzt werden. Dabei ist die CAN auf der Vorderseite des Kartenkörpers aufgedruckt und damit kein Geheimnis für jeden, der physischen Zugriff auf die „GD-Signaturkarte“ hat. Durch Eingabe einer CAN wird vom Karteninhaber die Kommunikation mit einer kontaktlosen Karte begonnen und ist damit ein Äquivalent zum Einführen einer kontaktbehafteten Karte in ein Lesegerät. Dadurch wird eine unbeaufsichtigte Kommunikation mit der „GD-Signaturkarte“ erschwert.

Durch Eingabe der globalen PIN kann der Signaturkarteninhaber die im EF.PCAN gespeicherte PCAN für ein Terminal auslesbar machen. Das Terminal speichert die PCAN und setzt diese bei zukünftigen Authentisierungen anstelle der CAN ein. Alternativ zu dem Einsatz der PCAN kann die zertifikaterzeugende Anwendung des ZDA auch einen AES-Schlüssel aus CAN und einem Master-Schlüssel ableiten, welcher für die Authentisierung verwendet wird.

Die Durchführung der jeweiligen Funktion ist ggf. von zusätzlichen Sicherheitsfunktionen abhängig (z.B. erfolgreiche Eingabe der Signatur-PIN beim Wechsel der Signatur-PIN).

**„Terminalauthentisierung“**

Die „GD-Signaturkarte“ unterstützt die Durchführung der Terminalauthentisierung. Dieses Protokoll wird zur Authentisierung des Terminals (Challenge-and-Response Protokoll) gegenüber der „GD-Signaturkarte“ genutzt. Weiterhin erfolgt mit dem Protokoll der Nachweis

der Zugriffsrechte des Signaturterminals gegenüber der „GD-Signaturkarte“. Diese Rechte werden an den sicheren Kanal, der anschließend mit der Chipauthentisierung aufgebaut wird, gebunden.

Zur Authentisierung erzeugt das Terminal mit seinem privaten Schlüssel ein Authentikations-token über eine Zufallszahl der „GD-Signaturkarte“ sowie über weitere Daten (z.B. Identität der „GD-Signaturkarte“, ephemeralen öffentlichen Terminalschlüssel). Das Authentikationstoken wird durch die „GD-Signaturkarte“ mit dem öffentlichen Schlüssel des Terminals geprüft. Kryptographische Grundlage bildet das Verfahren ECDSA.

Die Zugriffsrechte des ZDA beinhalten insbesondere das Lesen von Daten der *SSCD-Anwendung* sowie das Recht zur Installation von qualifizierten Signaturschlüsselzertifikaten.

Die Zugriffsrechte eines Signaturterminals zur Erstellung qualifizierter Signaturen beinhaltet das Recht zum Erstellen qualifizierter Signaturen sowie zur Verwaltung der Signatur-PIN. Dieses Recht autorisiert Zugriffe auf die *SSCD-Anwendung* der „GD-Signaturkarte“.

**„Chipauthentisierung“**

Die „GD-Signaturkarte“ unterstützt die Durchführung der Chipauthentisierung. Dieses Protokoll wird zur Authentisierung des Chips gegenüber dem Terminal sowie zum Aufbau eines sicheren Kanals für die verschlüsselte und integritätsgesicherte Kommunikation zwischen Terminal und Karte genutzt.

Das Protokoll basiert auf der Grundlage des Diffie-Hellman Protokolls zur Schlüssel-vereinbarung. Dabei werden das ephemeral DH Schlüsselpaar des Terminals (aus der Terminalauthentisierung) sowie das statische DH Schlüsselpaar der „GD-Signaturkarte“ verwendet. Die Berechnung der Authentikationstoken erfolgt jedoch mit Message Authentication Codes (MAC) auf der Basis der mit DH vereinbarten symmetrischen Schlüssel. Kryptographische Grundlage bildet das Diffie-Hellman Verfahren gemäß [TR-03110].

Zur Chipauthentisierung besitzt die „GD-Signaturkarte“ einen Chipauthentisierungsschlüssel. Der öffentliche Schlüssel wird in der „GD-Signaturkarte“ in der Karte gespeichert und kann nach der Personalisierung nicht mehr geändert werden.

**„Symmetrische Authentisierung“**

Für die Durchführung einer symmetrischen Authentisierung gemäß [EN 14890-1] werden bereits vor der Auslieferung an den Signaturkarteninhaber symmetrische Schlüssel in der „GD-Signaturkarte“ gespeichert. Zur Vorbereitung der Authentisierung ist eine Zufallszahl in der „GD-Signaturkarte“ zu erzeugen, welche im Rahmen der gegenseitigen Authentisierung eingesetzt wird.

**„Administration der „GD-Signaturkarte“ bzw. der Signaturanwendung“**

Diese Sicherheitsfunktion findet Anwendung innerhalb der Prozesse zur Initialisierung und Personalisierung der „GD-Signaturkarte“. Für die Initialisierung und Personalisierung der „GD-

Signaturkarte“ sind die zugehörigen Anforderungen des Herstellers zu berücksichtigen (s. Kapitel 3.2).

Die Sicherheitsfunktion erzwingt insbesondere die folgenden Regeln:

- Initialisierung und Personalisierung der „GD-Signaturkarte“ können nur erfolgen nachdem eine erfolgreiche Authentikation gegenüber der „GD-Signaturkarte“ mit einem geheimen Schlüssel stattgefunden hat.
- Am Ende der Initialisierungs- und Personalisierungsphase wird der Zugriff für eine weitere Initialisierung bzw. Personalisierung gesperrt.
- Die Initialisierung mit dem Laden der Initialisierungsskripte sowie der anschließenden Prüfung der geladenen Daten erfolgt gemäß der Guidance-Dokumentation [UG_Ini]. Das Laden des Initialisierungsskripts ist durch Sicherheitsmaßnahmen zur Wahrung von Sicherheit und Vertraulichkeit geschützt.

**„Prozesse der PIN-basierten Authentisierung (Signatur-PIN)“**

Die Sicherheitsfunktion beinhaltet die PIN-basierte Benutzerauthentisierung der Rolle Signierer. Sie steht erst nach dem erfolgreichen Setzen der Signatur-PIN zur Verfügung. Die Authentisierung des Benutzers erfolgt durch den Vergleich der vom Benutzer eingegebenen Signatur-PIN mit dem in der „GD-Signaturkarte“ (in der *SSCD-Anwendung*) geheim gespeicherten Referenzwert (RAD).

Nach erfolgreich abgeschlossener Personalisierung ist die „GD-Signaturkarte“ mit einer Transport-PIN (Leer-PIN oder spezifische PIN), die ausschließlich dem Transport-Schutz dient, ausgestattet. Vor Erzeugung einer Signatur muss eine Signatur-PIN gesetzt werden, die über mindestens sechs Stellen verfügt. Hierzu muss sich der Benutzer durch eine erfolgreiche Eingabe der Transport-PIN gegenüber der „GD-Signaturkarte“ authentisieren. Die Erzeugung einer Signatur nach Eingabe der Transport-PIN ist nicht möglich, dies wird durch die „GD-Signaturkarte“ verhindert. Die Signatur-PIN mit einer Mindestlänge von sechs Stellen ist vor der Aktivierung der *SSCD-Anwendung* bzw. eines Signaturschlüssels durch den designierten Signaturschlüsselinhaber zu setzen (Kommando CHANGE REFERENCE DATA mit einer PIN).

Sofern die „GD-Signaturkarte“ in der Variante mit zwei Signaturschlüsseln mit eigenen Signatur-PINs verwendet wird, verfügt die Karte nach der Personalisierung über zwei spezifische Transport-PINs. In diesem Fall muss vor der Erzeugung einer Signatur mit einem Signaturschlüssel die zugeordnete Signatur-PIN gesetzt werden. Die Sicherheitseigenschaften hinsichtlich des Transportschutzes bleiben für jede Signatur-PIN bestehen.

Eine Signatur-PIN besitzt einen Fehlbedienungszähler (FBZ), welcher während der Initialisierung auf maximal drei gesetzt werden kann und der nach Eingabe einer falschen PIN um eins erniedrigt wird. D.h. nach konfigurationsabhängiger und ggf. mehrfach aufeinanderfolgender Eingabe einer falschen PIN hat der FBZ den Wert Null und diese Signatur-PIN ist blockiert. In diesem Zustand kann weder eine weitere Prüfung der Signatur-PIN erfolgen, noch eine qualifizierte elektronische Signatur mit einem Signaturschlüssel erzeugt werden, der unter dieser Signatur-PIN geschützt wird. Nach einer erfolgreichen Eingabe der Signatur-PIN wird der FBZ zurück auf den konfigurierten Initialwert gesetzt, jedoch nur dann wenn diese Signatur-PIN nicht blockiert ist.

Der FBZ einer blockierten Signatur-PIN kann unter Anwendung eines Resetting Codes (PUK) zurückgesetzt werden. Die „GD-Signaturkarte“ unterstützt Resetting Codes mit einer Länge von mindestens sechs bis maximal 32 Stellen, wobei ein Resetting Code maximal zwanzigmal genutzt werden kann. D.h. der Nutzungszähler (Use counter) eines Resetting Codes ist maximal 20. Nach maximal zwanzigmaliger Eingabe des Resetting Codes (falsch oder korrekt) kann dieser nicht mehr verwendet werden und das Zurücksetzen einer blockierten Signatur-PIN ist nicht mehr möglich. Der Resetting-Code mit einer Mindestlänge von sechs Stellen ist vor der Aktivierung der *SSCD-Anwendung* durch den designierten Signaturschlüsselinhaber zu setzen (Kommando CHANGE REFERENCE DATA mit einer PUK). Das Setzen der PUK kann nur einmalig bei der ersten Aktivierung des Signaturschlüssels erfolgen. Anschließend kann die PUK nicht mehr verändert werden. Zum Setzen der PUK muss sich der Benutzer durch eine erfolgreiche Eingabe der Transport-PUK gegenüber der „GD-Signaturkarte“ authentisieren. Die Verwendung der PUK ist optional.

Zum Zurücksetzen des FBZ ist das Kommando RESET RETRY COUNTER zu verwenden. Ein Wechsel einer Signatur-PIN ist dabei nicht möglich. Es erfolgt kein Setzen des Sicherheitszustandes einer Signatur-PIN, d.h. das Zurücksetzen einer blockierten Signatur-PIN ermöglicht nicht die Erzeugung einer qualifizierten Signatur.

Eine Signatur-PIN kann durch den Signaturschlüsselinhaber geändert werden. Hierzu muss er sich durch die erfolgreiche Eingabe der aktuellen Signatur-PIN gegenüber der „GD-Signaturkarte“ authentisieren, d.h. das Ändern einer Signatur-PIN in eine neue Signatur-PIN ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der aktuellen Signatur-PIN (Kommando CHANGE REFERENCE DATA mit alter und neuer PIN) möglich.

Die Anzahl der Signaturen, die nach einer erfolgreichen Eingabe einer Signatur-PIN erzeugt werden können, ist konfigurierbar. Es sind die Werte von 1 bis 254 oder auch der Wert „unbegrenzt“ konfigurierbar. Die „GD-Signaturkarte“ prüft intern, ob der Maximalwert erreicht bzw. überschritten wurde. Anschließend muss die Signatur-PIN erneut eingegeben werden, um Signaturen erzeugen zu können.

Mit Außerbetriebnahme eines Signaturschlüssels kann die zugehörige Signatur-PIN und der Signaturschlüssel „terminiert“ werden. Voraussetzung für die Terminierung ist eine erfolgreiche Benutzerauthentisierung mit einer globalen Karteninhaber-PIN. Nach dem Terminieren der Signatur-PIN kann weder eine erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erfolgen, noch kann eine qualifizierte Signatur mit dem terminierten Signaturschlüssel erzeugt werden. Darüber hinaus erlaubt die „GD-Signaturkarte“ auch das Löschen des Signaturschlüssels nach einer erfolgreichen Benutzerauthentisierung mit einer globalen Karteninhaber-PIN.

Die „GD-Signaturkarte“ unterstützt die optionale Verwendung von zwei Signaturschlüsseln (z.B. ein RSA-Signaturschlüssel und ein Signaturschlüssel für elliptische Kurven). Der Zugriff auf die Signaturschlüssel kann entweder durch eine gemeinsame Signatur-PIN geschützt werden oder jeder Signaturschlüssel verfügt über seine eigene Signatur-PIN. Im Falle eigener Signatur-PINs verfügt jede Signatur-PIN auch über eigene Sicherheitsattribute (z.B. Transport-PIN, Transport-PUK, PUK, FBZ). Die beschriebenen Sicherheitseigenschaften gelten für jede Signatur-PIN.

**„Integrität gespeicherter Daten“**

Diese Sicherheitsfunktion dient zur Überwachung der Integrität von gespeicherten Daten. Dies betrifft alle DFs, EFs sowie sicherheitskritische Daten im RAM, die zur Erzeugung von qualifizierten Signaturen genutzt werden. Hierzu gehören insbesondere auch der Signaturschlüssel und der Signaturprüfschlüssel sowie der Referenzwert zur Prüfung der Signatur-PIN.

Die technische Umsetzung erfolgt auf Basis eines Prüfwerts. Beim Zugriff auf ein Datenobjekt wird der Wert berechnet und mit dem Wert, der bei Speicherung des Datenobjektes generiert und gespeichert wurde, verglichen. Im Falle einer Abweichung wird das betreffende Datenobjekt nicht verarbeitet und das aktuelle Kommando wird abgebrochen.

**„Sicherer Datenaustausch“**

Die „GD-Signaturkarte“ unterstützt den verschlüsselten und integritätsgesicherten Datenaustausch mit der externen Welt auf Basis des Secure Messaging gemäß dem ISO Standard [ISO 7816-4].

Hierzu werden voreingestellte oder durch eine gegenseitige Authentisierung (PACE, Terminal- und Chipauthentisierung) mit der externen Welt vereinbarte symmetrische Schlüssel eingesetzt.

**„Speicheraufbereitung“**

Die „GD-Signaturkarte“ stellt sicher, dass mit der Freigabe eines Speicherbereichs sicherheitskritische Informationen (z.B. Signaturschlüssel, Signatur-PIN) gelöscht werden. Hierzu gehören alle flüchtigen und permanenten Speicherbereiche, in denen sicherheitskritische Daten zwischengespeichert werden. Zur Wiederaufbereitung der Speicherbereiche werden diese überschrieben.

**„Schutz bei Fehlersituationen der Hard- oder Software“**

Diese Sicherheitsfunktion dient zur Wahrung eines sicheren Betriebszustandes im Falle eines Hard- oder Softwarefehlers. Hierzu gehören beispielsweise die folgenden Fehlersituationen oder Angriffe:

- Inkonsistenzen bei der Erzeugung von Signaturen
- Angriffe durch Fehlereinstreuung (Fault injection attacks)

Stellt die „GD-Signaturkarte“ eine Fehlersituation fest, geht sie in einen sicheren Betriebszustand über. Dabei werden mindestens alle diejenigen Prozesse abgebrochen, die mit der Fehlersituation in Verbindung stehen. In schwerwiegenden Fehlersituationen schließt die „GD-Signaturkarte“ die Session. In Abhängigkeit des Fehlers ist die „GD-Signaturkarte“ entweder blockiert oder kann nach Ausführung eines Resets in weiteren Sessions genutzt werden.

**„Resistenz gegen Seitenkanalangriffe“**

Die „GD-Signaturkarte“ stellt geeignete Hard- und Softwaremechanismen zum Widerstand von Seitenkanalangriffen wie

- Simple Power Analysis (SPA),
- Differential Power Analysis (DPA),
- Differential Fault Analysis (DFA) und
- Timing Analysis (TA)

zur Verfügung. Alle sicherheitskritischen Operationen der „GD-Signaturkarte“, insbesondere die kryptographischen Funktionen, sind durch diese Hard- und Softwaremechanismen geschützt. Informationen über Leistungsaufnahme sowie Ausführungszeiten von Kommandos lassen keine Rückschlüsse auf sicherheitsrelevante Daten wie Signaturschlüssel oder Signatur-PIN zu.

Diese Sicherheitsfunktion ist in allen Betriebsphasen (Initialisierung, Personalisierung und Nutzung) der „GD-Signaturkarte“ aktiv.

**„Selbsttest“**

Die „GD-Signaturkarte“ stellt verschiedene Arten von Selbsttests zur Verfügung. Nach jedem Reset sowie in periodischen Abständen während der Laufzeit wird automatisch ein Selbsttest durchgeführt.

Weiterhin wird im laufenden Betrieb die Integrität gespeicherter Daten verifiziert. Dies ist in der Sicherheitsfunktion „Integrität gespeicherter Daten“ beschrieben.

**„Kryptographische Algorithmen“**

Diese Sicherheitsfunktion der „GD-Signaturkarte“ stellt die kryptographischen Funktionen zur Verfügung.

Die „GD-Signaturkarte“ unterstützt die in „Funktionalität und Architektur“ gelisteten Algorithmen.

**„Erzeugung von Schlüsselpaaren“**

Die „GD-Signaturkarte“ unterstützt die karteninterne Erzeugung von ECDSA- bzw. RSA-Schlüsselpaaren zur Erzeugung von qualifizierten Signaturen mit einer Länge von 256 Bit, 320 Bit, 384 Bit, 512 Bit oder 521 Bit bei ECDSA-Schlüsseln bzw. von 2048 Bit bis zu 4096 Bit bei RSA-Schlüsseln.

Die Sicherheitsfunktion stellt sicher, dass u.a. die folgenden Anforderungen eingehalten werden:

- Es können Schlüssel für das ECDSA Verfahren auf Basis von $E(F_p)$ generiert werden. Die Länge der Parameter p und q beträgt 256 Bit, 320 Bit, 384 Bit, 512 Bit oder 521 Bit.
- Es können RSA-Schlüsselpaare mit einer Länge von 2048 Bit bis zu 4096 Bit generiert werden.
- Die Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2013], Kapitel 3.1) RSA-Verfahren sowie Kapitel 3.2.a) DSA-Varianten basierend auf Gruppen $E(F_p)$.
- Die hohe Qualität der Zufallszahlenerzeugung zur Erzeugung der Primzahlen stellt sicher, dass der Signaturschlüssel und der Signaturprüfschlüssel nicht vorhersagbar und mit hoher Wahrscheinlichkeit eindeutig sind. Die Primzahlen werden unabhängig voneinander erzeugt und erfüllen die Anforderungen gemäß [Alg_Kat 2013], Kapitel 3.1 und 4.
- Zur Schlüsselerzeugung werden der deterministische Zufallszahlengenerator (DRNG) sowie der Zufallszahlengenerator der Hardware (TRNG) der „GD-Signaturkarte“ verwendet.
- Die Schlüsselerzeugung stellt sicher, dass der Signaturschlüssel nicht aus dem Signaturprüfschlüssel ableitbar ist.
- Nach der Schlüsselgenerierung verifiziert die „GD-Signaturkarte“, ob der Signaturschlüssel und der Signaturprüfschlüssel zusammenpassen. Es werden nur gültige Schlüsselpaare zugelassen.
- Ein Import von ECDSA- bzw. RSA-Signaturschlüsselpaaren ist nicht möglich.
- Die Schlüsselerzeugung beinhaltet ein physikalisches Löschen des alten privaten Schlüssels bevor das neue Schlüsselpaar erzeugt wird.
- Die Schlüsselerzeugung ist resistent gegen Seitenkanalangriffe.
- Die Schlüsselerzeugung ist nur möglich, sofern das Sicherheitsattribut „SCD operational“ des Datenobjekts SCD den Wert „no“ hat.
- Die Schlüsselerzeugung durch den ZDA ist nur möglich, sofern sich dieser gegenüber der „GD-Signaturkarte“ authentisiert hat.

Bei der karteninternen Erzeugung des Signaturschlüssels werden durch die „GD-Signaturkarte“ die genannten Sicherheitsanforderungen zur Erzeugung von ECDSA- bzw. RSA-Schlüsselpaaren eingehalten.

In der Nutzungsphase kann das Kommando GENERATE ASYMMETRIC KEY PAIR zur karteninternen Erzeugung von Schlüsselpaaren durch einen authentisierten ZDA aufgerufen werden. Die für die Schlüsselgenerierung zu verwendende Schlüssellänge wird durch den Kartenhersteller in die Initialisierungsdaten eingetragen und mit der Initialisierung der „GD-Signaturkarte“ in der Karte unveränderbar gespeichert. Das Kommando GENERATE ASYMMETRIC KEY PAIR wertet zur Erzeugung des Signaturschlüssels die in der Karte gespeicherte Schlüssellänge aus.

Die Initialisierungsdaten (Filesystem und weitere Parameter) werden durch die Giesecke & Devrient GmbH erzeugt. Sie unterliegen einer Ende-zu-Ende Sicherung zwischen Kartenhersteller und Karte. Nachträgliche Änderungen an den Initialisierungsdaten können somit

durch die Karte erkannt werden. Daher kann die in der Karte gespeicherte Schlüssellänge weder vom Signaturschlüsselinhaber noch vom ZDA verändert werden.

**„Erzeugung von qualifizierten Signaturen“**

Die „GD-Signaturkarte“ unterstützt die Erzeugung von qualifizierten elektronischen Signaturen mit dem

- ECDSA Signaturschlüssel mit einer Schlüssellänge von 256 Bit, 320 Bit, 384 Bit, 512 Bit oder 521 Bit bzw.
- RSA Signaturschlüssel mit einer Schlüssellänge von 2048 Bit bis zu 4096 Bit.

Die Sicherheitsfunktion hat die folgenden Eigenschaften:

- Empfang von Daten (Data to be signed, DTBS) zur Erzeugung von qualifizierten elektronischen Signaturen (Hashen außerhalb der Karte).
- Empfang von Zwischenwerten einer Hashwertberechnung oder vollständig in der Karte zu hashenden Daten mit der abschließenden Berechnung des Hashwerts zur Erzeugung einer qualifizierten elektronischen Signatur.
- Bei Nutzung der kontaktlosen Schnittstelle muss jeder an die „GD-Signaturkarte“ übergebene Hashwert mit einem MAC gesichert werden.
- Berechnungen von ECDSA Signaturen gemäß [EN 14890-1].
- Erzeugung von digitalen Signaturen mit dem RSA gemäß dem Standard PKCS #1 in der Version 2.1 [PKCS#1] mit dem Formatierungsverfahren RSASSA-PSS und PKCS#1-v1_5.
- Zur Erzeugung von Zufallszahlen für die Generierung von Signaturen mit ECDSA werden der deterministische Zufallszahlengenerator (DRNG) sowie der Zufallszahlengenerator der Hardware (TRNG) der „GD-Signaturkarte“ verwendet.
- Die Signaturerzeugung ist resistent gegen Seitenkanalangriffe.
- Die Signaturerzeugung erfolgt in der Art und Weise, dass der Signaturschlüssel nicht aus der erzeugten Signatur abgeleitet werden kann und während der Signaturerzeugung keine Informationen über den Signaturschlüssel ermittelt werden können.
- Eine Signaturerzeugung kann nur durchgeführt werden, wenn eine erfolgreiche Benutzerauthentisierung mit der zugehörigen Signatur-PIN (Kommando VERIFY) stattgefunden und das Sicherheitsattribut „SCD operational“ des Datenobjekts SCD den Wert „yes“ hat.
- Verfügt die „GD-Signaturkarte“ über zwei Signaturschlüssel (ein RSA- und ein ECC-Signaturschlüssel) kann der Zugriff auf diese durch verschiedene Signatur-PINs geschützt werden.

# 3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

## 3.1 Erfüllte Anforderungen

Das Produkt erfüllt die folgenden Anforderungen gemäß Signaturgesetz [SigG] und Signaturverordnung [SigV].

**Tabelle 2: Erfüllung der Anforderungen des Signaturgesetzes**

| Referenz | Anforderung / Erläuterung / Ergebnis |
|---|---|
| **§ 17** | **Produkte für qualifizierte elektronische Signaturen** |
| Abs. (1) | **Anforderung**<br><br>Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend. |
| Abs. (3)<br><br>Nr. 1 | **Anforderung**<br><br>Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um<br><br>bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ... |

**Tabelle 3: Erfüllung der Anforderungen der Signaturverordnung**

| Referenz | Anforderung / Erläuterung / Ergebnis |
|---|---|
| **§ 15** | **Anforderungen an Produkte für qualifizierte elektronische Signaturen** |
| Abs. (1) | **Anforderung**<br><br>Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein. Die |

| Referenz | Anforderung / Erläuterung / Ergebnis |
|---|---|
| | zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfschlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können. |
| Abs. (4) | **Anforderung**<br><br>Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden. |
| **Anl. 1, I, 1.1**<br><br><br><br><br><br><br><br><br><br>b) | **Anforderung**<br><br>Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des § 15 Abs. 7 und des § 17 Abs. 4 des Signaturgesetzes hat nach den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, - ISO/IEC 15408) oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC - GMBl vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen.<br><br>Die Prüfung muss<br><br>bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen. |
| **Anl. 1, I, 1.2** | **Anforderung**<br><br>Bei den Prüfstufen "EAL 4" und bei "EAL 3" gemäß Abschnitt I Nr. 1.1 Buchstabe a bis c i) und Buchstabe d ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen.<br><br>Die Stärke der Sicherheitsmechanismen muss bei allen Produkten gemäß Abschnitt I Nr. 1.1 Buchstabe a bis d im Fall "E 3" und "E 2" mit "hoch" bewertet werden.<br><br>Abweichend hiervon genügt für den Mechanismus zur Identifikation durch biometrische Merkmale eine Bewertung der Sicherheitsmechanismen mit "mittel", wenn diese zusätzlich zur Identifikation durch Wissensdaten genutzt werden. |
| **Anl. 1, I, 1.3** | **Anforderung**<br><br>Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein. |

## 3.2 Einsatzbedingungen

**Anforderungen an den Initialisierer**

- Die durch Giesecke & Devrient GmbH ausgelieferten Initialisierungsdaten (Filesystem und weitere Parameter) müssen in einer sicheren Art und Weise behandelt werden.
- Bei der Handhabung der Initialisierungsdaten sind Datenintegrität und -authentizität sicherzustellen.
- Die Vorgaben des Kartenherstellers an die Initialisierung gemäß [UG_Ini] sind zu berücksichtigen.

**Einsatzbedingungen an die Nutzung des Signaturzählers**

Im Rahmen der Initialisierung wird festgelegt, wie viele Signaturen n (Wert des Signaturzählers) nach einmaliger Eingabe der Signatur-PIN erstellt werden können. Dabei gilt generell, dass eine Anzahl größer als Eins nur unter den folgenden Bedingungen erlaubt ist:

Der Zertifizierungsdiensteanbieter ist verpflichtet, den Antragsteller über die besonderen Sicherheitsanforderungen für die Einsatzumgebung der SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit (Multisignatur-SSEE) im Rahmen des § 6 Abs. 1 SigG zu unterrichten. Die Unterrichtung muss vor Ausstellung des qualifizierten Zertifikats erfolgen und soll die besonderen Sicherheitsanforderungen, die sich aus dem hohen Angriffspotenzial ergeben, im Einzelnen auflisten. Insbesondere, jedoch nicht ausschließlich, sind alle Sicherheitsanforderungen an die Umgebung anzugeben, die in der Bestätigung genannt sind.

Die Einsatzumgebung muss durch den Signaturschlüssel-Inhaber unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität der Multisignatur-SSEE und die Ausspähung der zugehörigen Identifikationsdaten (Signatur-PIN) durch Angreifer mit hohem Angriffspotential praktisch ausgeschlossen sind und damit die alleinige Kontrolle des Signaturschlüssel-Inhabers über den Prozess der Signaturerzeugung gegeben ist. Der Zertifizierungsdiensteanbieter ist verpflichtet, mindestens eine Einsatzumgebung anzugeben, die diese Anforderungen erfüllt.

Zu den physischen Sicherungsmaßnahmen gehört der physikalische Schutz gegen unbefugten Zugriff auf die SSEE, insbesondere bei einem unbeaufsichtigten Betrieb. In der Unterrichtung des Zertifizierungsdiensteanbieters gemäß § 6 Abs. 2 SigG soll in diesem Zusammenhang auf die Zurechnung der qualifizierten elektronischen Signaturen besonders hingewiesen werden.

Zu den logischen Sicherungsmaßnahmen gehören die Sicherstellung, dass ausschließlich bestätigte Produkte gemäß §§ 15 Abs. 7 Satz 1 oder 17 Abs. 4 Satz 1 SigG oder hinreichend geprüfte Produkte mit Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG zur Signaturanwendung eingesetzt werden, sowie zusätzlich die folgenden Punkte:

- Ordnungsgemäße Installation des Produktes und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,

- regelmäßige Überprüfung der Integrität des Produktes und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur, falls der Einsatz der SSEE in einem IT-Netz erfolgt,
- vertrauenswürdige Anbindung an externe Kommunikationsnetze, falls die SSEE in einem IT-Netz mit Anbindung an externe Kommunikationsschnittstellen eingesetzt wird.

Der Zertifizierungsdiensteanbieter sollte den Signaturschlüssel-Inhaber einer Multisignatur-SSEE darauf hinweisen, dass er bei Zweifeln an der ausreichenden Sicherheit seiner Einsatzumgebung eine anerkannte Prüf- und Bestätigungsstelle gemäß § 18 SigG kontaktieren möge.

**Anforderungen an den Personalisierer**

- Der Personalisierer muss sicherstellen, dass die Personalisierungsdaten (insbesondere der *SSCD-Anwendung*) in einer sicheren Art und Weise behandelt werden. Die Personalisierungsdaten müssen hinsichtlich Integrität, Authentizität und Vertraulichkeit geschützt werden.
- Die Vorgaben des Kartenherstellers an die Personalisierung gemäß [UG_Pers] sind zu berücksichtigen.

**Anforderungen an den Zertifizierungsdiensteanbieter**

- Die eingesetzte Zertifizierungskomponente (Anwendung) zur Erzeugung von qualifizierten Zertifikaten (Signature generation Application, CGA) sollte die Sicherheitsanforderungen von [UG_Use], Kapitel 5.5.2 erfüllen.
- Der ZDA muss den Prozess zur Aktivierung der *SSCD-Anwendung* in seinem Sicherheitskonzept beschreiben. Es ist darzulegen, wie der ZDA sich in geeigneter Weise davon überzeugen kann, dass der designierte Signaturschlüsselinhaber eine sichere Signaturerstellungseinheit besitzt und diese vollständig unter seiner alleinigen Kontrolle steht.
- Wenn ein ZDA ein Produkt für qualifizierte elektronische Signaturen vertreibt und der Produktname vom Namen des Produkts in der Bestätigung abweicht, dann muss der ZDA in einer Unterlage zum vertriebenen Produkt auf das eigentliche bestätigte Produkt hinweisen.

  Der ZDA hat in diesem Fall bei der Bundesnetzagentur einen Nachtrag zum bestätigten Produkt zu hinterlegen. Im Nachtrag sind mindestens der ZDA, der Name des bestätigten Produkts sowie der Vertriebsname des Produktes anzugeben.
- Der akkreditierte ZDA hat den Signaturschlüsselinhaber über bestätigte Kartenterminals und zugehörige Signaturanwendungskomponenten zu unterrichten, mit denen er die Signatur-PIN setzen kann.

  Dies ist auch im Sicherheitskonzept des ZDAs zu berücksichtigen.

- Programme, die ein ZDA seinen Kunden i.S.v. § 5 Abs. 1 Satz 2 SigV zur Übertragung von Referenzdaten auf die „GD-Signaturkarte“ zur Verfügung stellt (d.h. mit denen der Signaturschlüsselinhaber seine Signatur-PIN setzen oder ändern kann), müssen derart voreingestellt sein, dass die Eingabe der Referenzdaten standardmäßig über die Tastatur des Chipkartenlesers erfolgen muss. Für den Fall, dass das Programm optional die Deaktivierung der Tastatur des Chipkartenlesers erlaubt und stattdessen die PC-Tastatur zur Eingabe vorsieht, muss das Programm beim Wechsel auf diese Eingabeart einen Warnhinweis auf den damit verbundenen möglichen Sicherheitsverlust anzeigen.

**Anforderungen an den Signaturschlüssel- bzw. Karteninhaber**

- Der Signaturschlüsselinhaber soll zum Ersetzen der Transport-PIN und Setzen der Signatur-PIN sowie zum Ersetzen der Transport-PUK und Setzen der PUK einen Kartenleser mit sicherer PIN-Eingabe (d.h. mind. Klasse 2) und einer sicheren Signaturanwendungskomponente verwenden.
- Der Signaturschlüsselinhaber muss verifizieren, dass eine maximal fünfstellige Transport-PIN (Transport-PUK) noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte Signatur-PIN (PUK) setzt, die über mindestens eine Länge von sechs Stellen verfügt. Ist die Transport-PIN nicht gültig, so muss sich der Signaturschlüsselinhaber mit dem ausgebenden ZDA in Verbindung setzen.
- Der Signaturschlüsselinhaber muss die von ihm selbst gewählte Signatur-PIN und PUK vertraulich behandeln. Der Signaturschlüsselinhaber darf die Signatur-PIN sowie die PUK niemandem anvertrauen und muss sie sicher verwahren.
- Der Signaturschlüsselinhaber muss seine Signatur-PIN in regelmäßigen Abständen ändern.
- Der Signaturschlüsselinhaber muss die „GD-Signaturkarte“ so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Zur Erzeugung von qualifizierten Signaturen verwendet der Signaturschlüsselinhaber die „GD-Signaturkarte“ nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

**Anforderungen an Hersteller von Signaturanwendungskomponenten**

- Der Hersteller einer Signaturanwendungskomponente muss die Schnittstellen des Betriebssystems STARCOS 3.5 sowie der *SSCD-Anwendung* geeignet berücksichtigen.
- Bei der Erzeugung einer qualifizierten Signatur mit Übergabe eines extern berechneten Hashwerts sowie bei Nutzung der durch die „GD-Signaturkarte“ zur Verfügung gestellten Hashfunktionen ist die Auswahl einer geeigneten Hashfunktion durch die Signaturanwendungskomponente sicherzustellen.
- Der Hersteller einer Signaturanwendungskomponente zur Erzeugung von qualifizierten elektronischen Signaturen (Signature Creation Application, SCA) sollte die Sicherheitsanforderungen von [UG_Use], Kapitel 5.5.3 berücksichtigen.

- Verfügt die „GD-Signaturkarte“ über einen zweiten Signaturschlüssel muss die Signaturanwendungskomponente bei einer Erzeugung von qualifizierten Signaturen dem Karteninhaber den zur Signaturerzeugung ausgewählten Signaturschlüssel (z.B. RSA oder ECC) identifizieren.
- Verfügt die „GD-Signaturkarte“ über einen zweiten Signaturschlüssel und jeder Signaturschlüssel über eine eigene Signatur-PIN muss die Signaturanwendungs-komponente bei einer Erzeugung von qualifizierten Signaturen dem Karteninhaber die einzugebende Signatur-PIN identifizieren (z.B. RSA oder ECC).

## 3.3 Algorithmen und zugehörige Parameter

Die „GD-Signaturkarte“ stellt zur Erstellung von elektronischen Signaturen sowohl das ECDSA- als auch das RSA-Verfahren bereit. Das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ mit einer Länge von 256 Bit, 320 Bit, 384 Bit, 512 Bit oder 521 Bit für die Parameter p und q. Auf der Grundlage dieser Berechnungen können mit der „GD-Signaturkarte“ ECDSA Signaturen gemäß [EN 14890-1] erzeugt werden. Das RSA-Verfahren basiert auf dem RSA-Algorithmus mit einer Schlüssellänge von 2048 Bit bis zu 4096 Bit. Die konkrete Schlüssel-länge wird durch die berücksichtigten Initialisierungsskripte während der Initialisierung gesetzt und kann nachträglich nicht mehr geändert werden. Als Formatierungsverfahren werden RSASSA-PSS und PKCS#1-v1_5 gemäß [PKCS#1] unterstützt.

Zur Erzeugung von elektronischen Signaturen kann eine karteninterne bzw. eine teilweise karteninterne Hashwertberechnung mit der Hashfunktion SHA-2 (224, 256, 384 oder 512 Bit) gemäß [FIPS 180-2] oder eine ausschließlich externe Hashwertberechnung genutzt werden. Für die Anwendung von Hashfunktionen sind insbesondere die Einsatzbedingungen an die Hersteller von Signaturanwendungskomponenten zu berücksichtigen.

Es wird eine Zufallszahlenerzeugung auf Basis eines deterministischen Zufallszahlengenera-tors (DRNG) und eines Zufallszahlengenerators (TRNG) der zugrundeliegenden Hardware unterstützt. Der DRNG wurde im Rahmen der Evaluierung als DRG.4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet. Die Seed des DRG.4-Generators wird durch die zugrundeliegende Hardware generiert. Die Anforderungen gemäß [Alg_Kat 2013] an die erforderliche Entropie der Seed werden erfüllt.

Der TRNG der zugrundeliegenden Hardware von Infineon Technologies ist ein Zufallszahlen-generator mit einer PTG.2-Klassifizierung gemäß [AIS 31]. Die Zufallszahlen werden im laufenden Betrieb statistischen Tests unterzogen („Onlinetests“). Diese Eigenschaften wurden im Rahmen der CC Evaluierung der Hardware von Infineon nachgewiesen (vgl. [STHW] und [IFX_Cert]).

Die verwendeten kryptographischen Algorithmen sind gemäß dem Algorithmenkatalog der Bundesnetzagentur [Alg_Kat 2013] als geeignet eingestuft.

Für die Hashfunktion SHA-2 gelten die folgenden Hashwert-Längen als geeignet für die Anwendung bei qualifizierten elektronischen Signaturen:

**Tabelle 4: Mindest-Hashwert-Längen für SHA-2 Hashfunktionen**

| Geeignet bis Ende 2015 | Geeignet bis Ende 2019 |
|---|---|
| SHA-224 | SHA-256, SHA-384, SHA-512 |

Für das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ gelten die folgenden Mindest-Schlüssellängen als geeignet:

**Tabelle 5: Mindest-Schlüssellängen für das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$**

| Parameter \ Zeitraum | Bis Ende 2015 | Bis Ende 2019 |
|---|---|---|
| *p* | Keine Einschränkung | Keine Einschränkung |
| *q* | 224 Bit | 250 Bit |

Für den RSA-Algorithmus gelten die folgenden Mindest-Schlüssellängen als geeignet:

**Tabelle 6: Mindest-Schlüssellängen für den RSA Algorithmus**

| Parameter | Bis Ende 2019 |
|---|---|
| Schlüssellänge | 1976 Bit |

Für das Formatierungsverfahren RSASSA-PSS sind keine zeitlichen Restriktionen hinsichtlich dessen Eignung festgelegt. Das Formatierungsverfahren PKCS#1-v1_5 ist noch bis Ende 2015 geeignet.

Diese Bestätigung der „GD-Signaturkarte“ ist somit **maximal** gültig bis **31.12.2019**.

Die durch die Karte zur Verfügung gestellte Hashfunktion SHA-224 darf gemäß [Alg_Kat 2013] nur noch bis **Ende 2015** zur Erzeugung von qualifizierten Signaturen verwendet werden. Dies muss durch die Signaturanwendungskomponente sichergestellt werden.

Die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen und Parameter vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

## 3.4 Prüfstufe und Mechanismenstärke

Das Produkt STARCOS 3.5 ID ECC C1R wurde erfolgreich nach den Common Criteria (CC) Version 3.1 mit der Prüfstufe **EAL4+** (EAL4 mit den Augmentierung AVA_VAN.5) evaluiert.

Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential (Augmentierung AVA_VAN.5).

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0880 vom 19. April 2013 vor.

Die Evaluierung wurde in Form einer sogenannten „Composition Evaluation“ durchgeführt, die die Evaluierungsergebnisse der CC Evaluierung des M7820 A11 des Herstellers Infineon Technologies berücksichtigt. Diese Evaluierung erfolgte mit der Prüfstufe **EAL5+** (EAL5 mit

den Augmentierungen ALC_DVS.2 und AVA_VAN.5). Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential.

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0813 vom 6. Juni 2012 vor.

Die für die SSEE nach SigV maßgebende Evaluierungsstufe **EAL4+** (mit Augmentierung AVA_VAN.5) und die Prüfung gegen ein **hohes** Angriffspotential sind damit erreicht und in Teilen übertroffen.

## Referenzen


[SigG] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091).

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542).

[Alg_Kat 2013] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001, 27. März 2013

[AIS 20] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1, 2.12.1999.

[AIS 31] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.9.2001, samt mathematisch-technischem Anhang, (Version 3.1, 25.09.2001)

[BSI-CC-PP-0059] Protection profiles for Secure signature creation device – Part 2: Device with key generation; prEN 14169-2:2012; Version 2.0.1; 2012-01, BSI-CC-PP-0059-2009-MA-01

[EN 14890-1] European Standard, EN 14890-1:2008, Application Interface for Smart Cards used as secure signature creation devices – Part 1: Basic services

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.5 ID ECC C1R, Version 1.2, 27.03.2013, BSI-DSZ-CC-0880

[FIPS 180-2] NIST: FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 und Change Notice 1, Februar 2004.

[FIPS 197] NIST: FIPS Publication 197: Specification for the Advanced Encryption Standard (AES), 26. November 2001

[IFX_Cert] Certification Report, BSI-DSZ-CC-0813-2012, Infineon smart card IC (Security Controller) M7820A11 with optional RSA2048/4096 v1.02.008, ECv1.02.008, SHA-2 v1.01 and Toolbox v1.02.008libraries and with specific IC dedicated software, 6. June 2012

[ISO 7816-4] ISO/IEC 7816-4: Integrated circuit(s) cards with contacts. Part 4: Inter-industry commands for interchange, ISO/IEC 7816-4, First edition, September 1.1995

[PKCS#1] PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002

[SEC 2] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 2000, Version 1

[ST] Giesecke & Devrient GmbH, STARCOS 3.5 ID ECC C1R, Security Target, Version 2.2, 21.03.2013

[STHW] Infineon Technologies AG, Chipcard and Security, Security Target, M7820 A11 including optional Software Libraries RSA – EC – SHA-2, Version 1.5, 2012-05-07

[TR-03110] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.05, Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-03110, 14. Oktober 2010

Die aktuelle Version ist 2.10 (in Bezug auf den Inhalt identisch zu Version 2.05)

Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-03110, 20. März 2012

[TR-03111] BSI. Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 1.11, 17. April 2009

[UG_Main] Guidance Documentation STARCOS 3.5 ID Main Document, Version 0.6, 19.10.2011

[UG_Ini] Guidance Documentation for the Initialization Phase STARCOS 3.5 ID EAC+AA C1, STARCOS 3.5 ID SAC+EAC+AA C1 and STARCOS 3.5 ID ECC C1, Version 1.5, 15.06.2012

[UG_Pers] Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID ECC C1, Version 0.8, 15.06.2012

[UG_Use] Guidance Documentation for the Usage Phase STARCOS 3.5 ID ECC C1, Version 1.2, 27.06.2012

[UG_GenApp] Generic Application of STARCOS 3.5 ID ECC C1R, Januar 2013

## Ende der Bestätigung