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
Emil-Nolde-Straße 7
53113 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 3.6 QES C1“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

SRC.00025.TE.06.2016

Bonn, den 08.06.2016

Gerd Cimiotti 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 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung des Produktes und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit STARCOS 3.6 QES C1 der Giesecke & Devrient GmbH.

Das Produkt ist ein Heilberufsausweis (HBA) der deutschen Gesundheitstelematik und wird im Folgenden kurz als „HBA-Signaturkarte“ bezeichnet.

1.2 Auslieferung

Die „HBA-Signaturkarte“ ist realisiert als Dual Interface Karte, d.h. die Karte verfügt über eine kontaktbehaftete und eine kontaktlose Schnittstelle. Die Hardware der „HBA-Signaturkarte“ besteht aus dem Chip M7893 B11 mit den zur Verfügung gestellten Crypto-Coprozessoren "Crypto@2304T" (Kryptographie mit RSA und elliptischen Kurven) und "Symmetric Crypto Processor" (Ver- und Entschlüsselungen mit dem AES), wobei die durch Infineon zur Verfügung gestellte Kryptobibliothek nicht verwendet wird..

Die Smartcard Embedded Software enthält das Betriebssystem STARCOS 3.6 COS C1. Diese Plattform stellt eine ISO-7816 kompatible, multifunktionale Plattform zur Verfügung, die den Anforderungen an das Kartenbetriebssystem der Generation 2 der deutschen Gesundheitstelematik gemäß [EGK-COS] genügt. Die Karte ist ein Heilberufsausweis und erfüllt die Anforderungen an das zugehörige Dateisystem gemäß [HBA-ObjSys]. Sie verfügt über die im Folgenden als *SSCD-Anwendung* bezeichnete Anwendung zur Erstellung von qualifizierten Signaturen und wird grundsätzlich mit weiteren Anwendungen, wie z.B. die *Heilberufsanwendung* und die *ESIGN-Anwendung*, versehen. Die weiteren Anwendungen sind jedoch **nicht** Gegenstand der vorliegenden Bestätigung.

Die „HBA-Signaturkarte“ wird als Karte mit SSCD-Anwendung vom Zertifizierungsdiensteanbieter (ZDA) an den Endkunden ausgeliefert. Hierzu bezieht der ZDA die Karten von Giesecke & Devrient GmbH. Der Hersteller lädt das Kartenbetriebssystem sowie ggf. die *SSCD-Anwendung* in die Karte.

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. Mit der Personalisierung erfolgen die karteninterne Generierung des Signaturschlüsselpaars sowie das Setzen einer spezifischen Transport-PIN als Transport-Schutz bei der Auslieferung zum Kunden. Mit Auslieferung an den Endkunden verfügt die Karte über alle weiteren Daten, d.h. der Signaturschlüssel sowie das zugehörige Signaturschlüsselzertifikat befinden sich bereits in der Karte.

Die Authentizität und Integrität einer Karte kann während der Personalisierung durch den korrekten Personalisierungsschlüssel authentisiert werden.

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

Für die bestätigte Version der STARCOS 3.6 QES C1 sind in [UG_Ini] die herstellerspezifischen Werte zu den Parametern „Chip Manufacturer Data“, „Version of the Operating System“, „Fabkey Key Material Identification“ und „OS Completion Level / Initialisation Table Identifier“ angegeben. Sie können während der Produktion mit dem Kommando „GET PROTOCOL DATA“ gemäß [UG_Ini], Kapitel 5.7.2 bzw. [UG_Pers], Kapitel 5.7.2 sowie während der Usage Phase aus der Karte ausgelesen werden. Während der Usage Phase können die Chip Manufacturer Data, der Komplettierungsstand und die Version des Betriebssystems gelesen werden.

1.3 Lieferumfang

Der Lieferumfang des Produktes besteht aus den folgenden Komponenten:

Tabelle 1: Lieferumfang

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
1	Hardware / Software	M7893 B11 von Infineon Technologies (inkl. IC dedizierter Software) Modultyp: T-M8.4-8-1 (Zertifizierung unter BSI-DSZ-CC-0879-V2-2015)	M7893 B11		Gesicherte Auslieferung an den ZDA bzw. einen beauftragten Dritten (Initialisierer, Personalisierer)
2	Software (Betriebssystem)	Smartcard Embedded Software (Betriebssystem) STARCOS 3.6 COS C1			Implementiert im Flash des Halbleiters
3	Anwendung	Smartcard Embedded Anwendung (Qualified Electronic Signature Application gemäß [HBA-ObjSys])			Implementiert im NVM des Halbleiters
4	Software	Mit dem Wrapper wird eine Schnittstelle zwischen dem Betriebssystem und einer externen Instanz (z.B. "Konsistenz-Prüftool") gemäß [EGK-Wrap] implementiert. Der Wrapper codiert die zu exportierenden Daten in einem standardisierten Format.	1.6.17		Auslieferung in digitaler Form

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
5	Krypto-graphische Schlüssel	Kryptographische Schlüssel für die Initialisierung oder Personalisierung zum Schutz vor unberechtigter Modifikation			In elektroni-scher Form, zum Schutz vor Offenlegung bzw. Modifikation verschlüsselt und signiert
6	Dokumenta-tion	Guidance Documenta-tion STARCOS 3.6 – Main Document, [UG_Main]	1.7	29.07.2015	Dokument in elektronischer Form
7	Dokumenta-tion	Guidance Documenta-tion for the Initialisation Phase for STARCOS 3.6 QES C1, [UG_Ini]	1.2	10.05.2016	Dokument in elektronischer Form
8	Dokumenta-tion	Guidance Documenta-tion for the Personali-sation Phase for STARCOS 3.6 QES C1, [UG_Pers]	1.1	07.10.2015	Dokument in elektronischer Form
9	Dokumenta-tion	Guidance Documenta-tion for the Usage Phase for STARCOS 3.6 QES C1, [UG_Use]	1.1	10.05.2016	Dokument in elektronischer Form
10	Dokumenta-tion	Internal Design Specification for STARCOS 3.6 QES C1, [UG_internal]	1.3	31.07.2015	Dokument in elektronischer Form
11	Dokumenta-tion	STARCOS 3.6 Func-tional Specification – Part 1: Interface Specification, [FSP_IF_COS]	1.19	31.07.2015	Dokument in elektronischer Form
12	Dokumenta-tion	Guidance Documenta-tion for the Wrapper, [UG_Wrapper]	1.3	29.07.2015	Dokument in elektronischer Form

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
13	Dokumentation	Guidance Documentation for the Inlay Production, STARCOS 3.6 QES C1, [UG_Inlay]	1.1	13.07.2015	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 „HBA-Signaturkarte“ ist realisiert als Dual Interface Karte, d.h. die Karte verfügt über eine kontaktbehaftete und eine kontaktlose Schnittstelle. Die Hardware der „HBA-Signaturkarte“ besteht aus dem Chip M7893 B11 mit den zur Verfügung gestellten Crypto-Coprozessoren "Crypto@2304T" (Kryptographie mit elliptischen Kurven) und "Symmetric Crypto Processor" (Ver- und Entschlüsselungen mit dem AES), wobei die Kryptobibliothek von Infineon nicht verwendet wird. Der Chip M7893 B11 wurde nach CC 3.1 evaluiert und zertifiziert (BSI-DSZ-CC-0879-V2-2015).

Die Software besteht aus dem Betriebssystem STARCOS 3.6 COS C1 sowie aus der *SSCD-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen.

Das Betriebssystem STARCOS 3.6 COS C1 stellt eine interoperable, ISO 7816-konforme, multifunktionale 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 befinden sich gemäß den Vorgaben zum Filesystem des Heilberufsausweises [HBA-ObjSys] weitere Anwendungen auf der „HBA-Signaturkarte“. 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 RSA Schlüsseln
- Erzeugung von elektronischen Signaturen (RSA)

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

- Halbleiter (IC) M7893 B11 von Infineon mit dedizierter Software,
- Betriebssystem STARCOS 3.6 COS C1 und
- der *SSCD-Anwendung* mit den entsprechenden Datenstrukturen zur Speicherung und Verwaltung von Daten des Inhabers der Sicheren Signaturerstellungseinheit (Signatur-PIN, Signaturschlüssel).

Bevor die *SSCD-Anwendung* genutzt werden kann, ist diese zu vervollständigen. Dabei erfolgt die Generierung des Signaturschlüssels durch den Zertifizierungsdiensteanbieter (ZDA) (bzw. einen beauftragten Dritten) vor Auslieferung der Karte. Der Signaturschlüssel wird in der Karte

generiert. Im Rahmen dieser Komplettierung der *SSCD-Anwendung* wird auch das Signaturschlüsselzertifikat eingebracht und die Transport-PIN in der Karte gesetzt. Nach Abschluss der Personalisierung ist eine Änderung des Programmcodes nicht möglich.

Um mit der komplettierten *SSCD-Anwendung* eine Signatur erzeugen zu können, muss der designierte Signaturschlüsselinhaber die „HBA-Signaturkarte“ als sichere Signaturerstellungseinheit (SSEE) aktivieren. Dazu muss er die voreingestellte und maximal fünfstellige Transport-PIN durch eine gültige Signatur-PIN ersetzen.

Nach Aktivierung der *SSCD-Anwendung* kann die „HBA-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 „HBA-Signaturkarte“ ist eine sogenannte Multisignatur-fähige sichere Signaturerstellungseinheit (Multisignatur-SSEE) mit der nach einer erfolgreichen Eingabe der Signatur-PIN entweder genau eine oder mehrere, jedoch begrenzte Anzahl an qualifizierten Signaturen erzeugt werden können. Der Wert wird im Rahmen der Initialisierung festgelegt (Wert n des Signaturzählers mit n = 250) und kann anschließend nicht mehr verändert werden. Die „HBA-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 „HBA-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 Nutzung der Multisignatur-Fähigkeit bedingt, dass die „HBA-Signaturkarte“ in einem speziellen Sicherheitsmodus betrieben wird (Security Environment #2), der voraussetzt, dass die zu signierenden Daten über einen sicheren Kanal an die Karte übergeben werden. Der Aufbau des sicheren Kanals durch die Karte erfolgt nur, falls eine erfolgreiche gegenseitige Authentikation mit der externen Welt stattgefunden hat. Für die sichere Übertragung der zu signierenden Daten muss die externe Welt sich unter der Rolle "SAK für Stapel- oder Komfortsignatur" authentisieren. Dies ermöglicht die Anwendung der Stapel- bzw. Komfortsignatur gemäß [TR-03114] und [TR-03115].

Die Erzeugung von einzelnen Signaturen kann im Security Environment #1 ohne diese zusätzlichen Sicherheitsmechanismen erfolgen.

Im Security Environment #2 unterstützt die „HBA-Signaturkarte“ auch die Übergabe der Signatur-PIN über einen sicheren Kanal der mittels einer gegenseitigen Authentisierung aufgebaut wurde und die externe Welt sich unter der Rolle "Remote-PIN-Sender" authentisiert hat. Damit wird das Konzept einer "entfernten PIN-Eingabe" unterstützt (vgl. [TR-03114], [TR-03115]), wobei das eHealth-Kartenterminal, das der Signaturschlüsselinhaber zur PIN-Eingabe nutzt, und das eHealth-Kartenterminal in dem die „HBA-Signaturkarte“ steckt, verschieden sind. Dabei erfolgt die sichere Ende-zu-Ende Kommunikation zwischen der „HBA-Signaturkarte“ und einem Sicherheitsmodul des zur PIN-Eingabe verwendeten Kartenterminals. Für die Nutzung dieses Szenarios gelten besondere Einsatzbedingungen.

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) und
- Rücksetzen des Fehlbedienungszählers der Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der PUK).

In der *SSCD-Anwendung* können bis zu drei Attributzertifikate gespeichert werden. Diese können nachträglich, nach Ausgabe der Karte, gelöscht oder überschrieben werden sofern der Signaturschlüsselinhaber diesen Vorgang mittels einer spezifischen Benutzer-PIN (PIN.CH) autorisiert.

Für die Signaturanwendung relevanten Zugriffe unterstützt die „HBA-Signaturkarte“ die Anwendung von Secure Messaging. Zur (gegenseitigen) Authentisierung von externer Welt und Karte sowie zum Aufbau eines sicheren Kommunikationskanals werden die Authentisierungsprotokolle Password Authentication Connection Establishment (PACE), Asymmetrische Rollenauthentisierung bzw. Berechtigungsnachweis, Interne Authentisierung und gegenseitige Authentisierung mit/ohne Aushandlung von Sessionkeys gemäß [EGK-COS] unterstützt. Im Rahmen der Authentisierungen werden Zugriffsrechte der externen Welt nachgewiesen. Hierzu gehört insbesondere auch das Recht einer Signaturanwendungskomponente zur Erzeugung von Multisignaturen bzw. als "Remote-PIN-Sender".

Die Sicherheitseigenschaften der „HBA-Signaturkarte“ werden mit der Beschreibung der Sicherheitsfunktionen weiter erläutert (s. Abschnitt „Sicherheitsfunktionen bzw. –eigenschaften der HBA-Signaturkarte“).

Das STARCOS Betriebssystem erlaubt dem Kartenhersteller eine Reihe von Konfigurationsmöglichkeiten. Vor der Initialisierung hat der Kartenhersteller die Konfiguration durch die Erstellung des Filesystems sowie der Festlegung weiterer Daten 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 Betriebssystemcodes und Laden des Filesystems) durch den Initialisierer. Die Installation des File-systems 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 Sinne kann man von einer Ende-zu-Ende-Sicherung zwischen Kartenhersteller und Chip sprechen. Das Laden von unautorisiert geänderten Initialisierungsdaten wird hierdurch verhindert. Ein nachträgliches Einbringen weiterer Software wird durch die „HBA-Signaturkarte“ nicht unterstützt. Zugelassene Initialisierungstabellen, die auch über eine erfolgreiche Zertifizierung gemäß [TR-03144] verfügen, sowie zugehörige Identifikationsdaten sind auf den Web-Seiten von Giesecke & Devrient GmbH angegeben. Der Initialisierer muss die in den Guidancedokumenten beschriebenen Anforderungen an die Initialisierung berücksichtigen.

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

- Asymmetrischer RSA Algorithmus gemäß [PKCS#1] mit einer Schlüssellänge von 2048 Bit.
- Hashfunktion SHA-256 gemäß [FIPS 180-4].
- Zufallszahlenerzeugung auf Basis eines deterministischen Zufallszahlengenerators (DRNG), dessen Seed durch den True Random Number Generator (TRNG) der zugrundeliegenden Hardware generiert wird. Der DRNG wurde im Rahmen der Evaluierung als DRG.4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet. Der TRNG ist ein 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], [IFX_Cert]).

Die Erzeugung von Hashwerten kann entweder innerhalb der „HBA-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.

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

- DSA auf Basis elliptischer Kurven (ECDSA) basierend auf Gruppen E(Fp) (vgl. [TR-03111]),
- Asymmetrische Operationen mit dem RSA (Schlüssellängen 2048 und 3072 Bit; vgl. [PKCS#1]) und auf Basis elliptischer Kurven (vgl. [TR-03111]) zur Authentisierung und Ver- und Entschlüsselung,
- Hashfunktionen SHA-1, SHA-384 und SHA-512 gemäß [FIPS 180-4],
- Elliptic Curve Diffie-Hellman (ECDH) gemäß [TR-03110], [TR-03111] zur Authentisierung (PACE) und Schlüsselvereinbarung für den Secure Messaging Kanal,
- Symmetrischer AES Algorithmus gemäß [FIPS 197] mit einer effektiven Schlüssellänge von 128, 192 oder 256 Bit (CBC-Modus, CMAC gemäß [TR-03110], [SP800-38B]).

Die „HBA-Signaturkarte“ unterstützt die ECC Brainpool Kurven P256r1, P384r1 und P512r1 gemäß [RFC 5639] sowie die ANSI Kurven ansix9p256r1 und ansix9p384r1, die identisch sind zu P-256 und P-384 gemäß [FIPS 186-4].

Die „HBA-Signaturkarte“ wurde auf Basis der Common Criteria in der Version 3.1 erfolgreich evaluiert [ETR]. Die Prüftiefe beträgt EAL 4+ mit der Augmentierung AVA_VAN.5.

Weiterhin berücksichtigt die „HBA-Signaturkarte“ die Protection Profiles „Protection profiles for Secure signature creation device", Part 2: "Device with key generation", BSI-CC-PP-0059-2009-MA-01 [BSI-CC-PP-0059] und Part 4: "Extension for device with key generation and trusted communication with certificate generation application", BSI-CC-PP-0071-2012 [BSI-CC-PP-0071] sowie "Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2)", BSI-CC-PP-0082-V2-2014, Version 1.9 [BSI-CC-PP-0082].

Sicherheitsfunktionen bzw. –eigenschaften der „HBA-Signaturkarte“

Die „HBA-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 „HBA-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 „HBA-Signaturkarte“ durch die Kenntnis eines geheimen Schlüssels als Administrator (wie bspw. Initialisierer, Personalisierer oder Karten-managementsystem) bzw. durch Eingabe der Signatur-PIN als Signierer.

In der Nutzungsphase wird die Anwendung eines sicheren Kanals sowohl bei Verwendung der kontaktbehafteten als auch der kontaktlosen Schnittstelle durch die „HBA-Signaturkarte“ unterstützt. Bei der Nutzung der kontaktbehafteten Schnittstelle kann die Verbindung zwischen der „HBA-Signaturkarte“ und der Signaturanwendung optional kryptographisch abgesichert werden, jedoch nur falls einzelne Signaturen erzeugt werden. Die Erstellung von Signaturen unter Anwendung der Multisignatur-Fähigkeit setzt immer die Kommunikation über einen sicheren Kanal voraus. Eine Nutzung der kontaktlosen Schnittstelle kann ausschließlich unter Anwendung eines sicheren Kanals erfolgen.

Dabei können die Sitzungsschlüssel durch verschiedene Verfahren ausgehandelt werden. Die „HBA-Signaturkarte“ stellt sowohl symmetrische als auch asymmetrische Authentisierungs-protokolle gemäß [EGK-COS] zur Verfügung. 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.
- **Rollenauthentisierung** bzw. **Berechtigungsnachweis** mit asymmetrischen Schlüsseln zur (gegenseitigen) Authentisierung ohne Aufbau eines sicheren Kanals.

- **Device-Authentisierung** mit asymmetrischen Schlüsseln zur gegenseitigen Authentisierung und Aufbau eines sicheren Kanals zur Übertragung der zu signierenden Daten bei Anwendung der Multisignatur-Fähigkeit bzw. bei einer gesicherten Übertragung der Signatur-PIN.
- **CMS-Authentisierung** mit symmetrischen oder asymmetrischen Schlüsseln zur gegenseitigen Authentisierung und Aufbau eines sicheren Kanals zum Kartenmanagementsystem.

Bei Zugriffen über die Luftschnittstelle, die bereits über einen sicheren Kanal nach einer Device-Authentisierung oder CMS-Authentisierung erfolgen, kann auf eine zusätzliche Sicherung der Schnittstelle über einen sicheren Kanal auf Basis des PACE-Protokolls verzichtet werden.

Weiterhin ist die Zugriffskontrolle realisiert unter Anwendung von Zugriffsbedingungen, die als Sicherheitsattribute in der „HBA-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 karteninterne Schlüsselgenerierung kann nur im Rahmen der Personalisierung und nur dann erfolgen, 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. private Signaturschlüssel, Transport-PIN, Signatur-PIN) über die Betriebssystem-Kommandos ist aufgrund der gesetzten Zugriffsregeln nicht möglich.
- Das Ersetzen der Transport-PIN durch eine Signatur-PIN durch den designierten Signaturschlüsselinhaber kann nur im initialen 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 „HBA-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.
- Signaturen können nur durch den Signaturschlüsselinhaber generiert werden. Hierzu ist eine vorherige erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erforderlich.
- Die Nutzung der Multisignatur-Fähigkeit ist nur im Security Environment #2 möglich. In diesem Fall können Signaturen nur dann erzeugt werden, falls eine erfolgreiche Benutzerauthentisierung erfolgt ist, eine gegenseitige Authentisierung mit Aufbau eines sicheren Kanals stattgefunden hat und die weiteren Zugriffe zur Signaturerzeugung unter Anwendung von Secure Messaging erfolgen. Dabei muss sich die externe Welt unter der Rolle "SAK für Stapel- oder Komfortsignatur" authentisiert haben.

„Password Authenticated Connection Establishment (PACE) Protokoll“

Die „HBA-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 „HBA-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 „HBA-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 „HBA-Signaturkarte“ unterstützt die Kontrolle des Signaturschlüsselinhabers über die sichere Signaturerstellungseinheit bei Anwendung der Karte über die Luftschnittstelle.

Dabei ist die CAN auf der Vorderseite des Kartenkörpers aufgedruckt und damit kein Geheimnis für jeden, der physischen Zugriff auf die „HBA-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 „HBA-Signaturkarte“ erschwert.

„Rollenauthentisierung und Berechtigungsnachweis“

Die „HBA-Signaturkarte“ unterstützt die Durchführung einer Rollenauthentisierung bzw. eines Berechtigungsnachweises mittels einer (gegenseitigen) asymmetrischen Authentikation auf der Grundlage des RSA bzw. elliptischer Kurven gemäß [EGK-COS].

Die Protokolle zur externen und internen Authentikation verwenden Challenge-and-Response-Protokolle auf der Grundlage geeigneter Zufallszahlen. Die Verfahren basieren auf der Verwendung von CV-Zertifikaten, um die Authentizität der öffentlichen Schlüssel nachzuweisen. Diese enthalten Rollen- bzw. Berechtigungsangaben und somit können hiermit verbundene Zugriffsrechte nachgewiesen werden. Zur internen Authentisierung verfügt die „HBA-Signaturkarte“ über private Schlüssel zur Rollenauthentisierung bzw. zum Berechtigungsnachweis. Weiterhin enthält die Karte die erforderlichen Root-Schlüssel, um die Prüfung von CV-Zertifikaten zu ermöglichen.

„Device-Authentisierung“

Die „HBA-Signaturkarte“ unterstützt die Durchführung einer gegenseitigen Device-Authentisierung mit Aufbau eines sicheren Kanals mittels asymmetrischer Verfahren auf der Grundlage von elliptischen Kurven gemäß [EGK-COS].

Die Protokolle zur externen und internen Authentikation verwenden Challenge-and-Response-Protokolle auf der Grundlage geeigneter Zufallszahlen. Die Verfahren basieren auf der Verwendung von CV-Zertifikaten um die Authentizität der öffentlichen Schlüssel nachzuweisen. Diese enthalten Berechtigungsangaben und somit können hiermit verbundene Zugriffsrechte nachgewiesen werden. Device-Authentisierungen dienen insbesondere zur Kommunikation mit

einer Signaturanwendungskomponente, die über die Berechtigung einer "SAK für Stapel- oder Komfortsignatur" und/oder "Remote-PIN-Sender" verfügt. Hiermit können die Signatur-PIN sowie im Falle der Nutzung der Multisignatur-Fähigkeit zu signierende Daten gesichert an die Karte übertragen werden.

Zur internen Authentisierung verfügt die „HBA-Signaturkarte“ über einen spezifischen privaten Schlüssel zur Device-Authentisierung. Weiterhin enthält die Karte den erforderlichen Root-Schlüssel um die Prüfung von CV-Zertifikaten zu ermöglichen.

„CMS-Authentisierung“

Die „HBA-Signaturkarte“ unterstützt die Durchführung einer gegenseitigen Authentisierung mit Aufbau eines sicheren Kanals mittels asymmetrischer Verfahren auf der Grundlage von elliptischen Kurven oder mittels symmetrischer Verfahren auf der Grundlage des AES mit einem Kartenmanagementsystem gemäß [EGK-COS].

Die Protokolle zur externen und internen Authentikation verwenden Challenge-and-Response-Protokolle auf der Grundlage geeigneter Zufallszahlen.

Das asymmetrische Verfahren basiert auf der Verwendung von CV-Zertifikaten, um die Authentizität der öffentlichen Schlüssel des Kartenmanagementsystems nachzuweisen. Diese enthalten Berechtigungsangaben und somit können hiermit verbundene Zugriffsrechte nachgewiesen werden. Zur internen Authentisierung verfügt die „HBA-Signaturkarte“ über einen privaten Schlüssel. Weiterhin enthält die Karte einen spezifischen Root-Schlüssel zur Administration, um die Prüfung dieser CV-Zertifikate zu ermöglichen.

Für das Protokoll auf Basis symmetrischer Algorithmen kann die „HBA-Signaturkarte“ grundsätzlich über AES-Schlüsselpaare, einen Schlüssel für Ver- und Entschlüsselungsoperationen und einen Schlüssel zur MAC-Bildung, der Länge 128 Bit und 256 Bit, verfügen. Aufgrund der gewählten Einsatzbedingungen werden diese Schlüssel jedoch nicht personalisiert und die Anwendung einer symmetrischen CMS-Authentisierung ist somit nicht möglich.

„Administration der „HBA-Signaturkarte“ bzw. der Signaturanwendung“

Diese Sicherheitsfunktion findet Anwendung innerhalb der Prozesse zur Initialisierung und Personalisierung der „HBA-Signaturkarte“. Für die Initialisierung und Personalisierung der „HBA-Signaturkarte“ sind die zugehörigen Anforderungen des Herstellers zu berücksichtigen (s. Kapitel 4.2).

Weiterhin können die in der *SSCD-Anwendung* gespeicherte Daten Signaturschlüsselzertifikat und Attributzertifikate nach Ausgabe der Karte an den designierten Schlüsselinhaber durch ein Kartenmanagementsystem administriert werden.

Die Sicherheitsfunktion erzwingt insbesondere die folgenden Regeln:

- Initialisierung und Personalisierung der „HBA-Signaturkarte“ können nur erfolgen, nachdem eine erfolgreiche Authentikation gegenüber der „HBA-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 den Guidance-Dokumentationen [UG_Ini] und [UG_Pers]. Das Laden des Initialisierungsskripts ist durch Sicherheitsmaßnahmen zur Wahrung von Sicherheit und Vertraulichkeit geschützt.
- Zugriffe des Kartenmanagementsystems auf die „HBA-Signaturkarte“ können nur erfolgen, nachdem eine erfolgreiche gegenseitige Authentikation gegenüber der „HBA-Signaturkarte“ mit einem geheimen Schlüssel stattgefunden hat und ein sicherer Kanal aufgebaut wurde. Alle weiteren Zugriffe müssen dann unter Anwendung von Secure Messaging erfolgen.

„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 „HBA-Signaturkarte“ (in der *SSCD-Anwendung*) geheim gespeicherten Referenzwert (RAD).

Nach erfolgreich abgeschlossener Personalisierung ist die „HBA-Signaturkarte“ mit einer Transport-PIN (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 „HBA-Signaturkarte“ authentisieren. Die Erzeugung einer Signatur nach Eingabe der Transport-PIN ist nicht möglich, dies wird durch die „HBA-Signaturkarte“ verhindert.

Die Signatur-PIN besitzt einen Fehlbedienungszähler (FBZ), welcher während der Initialisierung auf drei gesetzt wird und der nach Eingabe einer falschen PIN um eins erniedrigt wird. D.h. nach 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 erzeugt werden. 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 „HBA-Signaturkarte“ unterstützt einen Resetting Code mit einer Länge von mindestens vier bis maximal 12 Stellen, wobei der Resetting Code maximal zehnmal genutzt werden kann. D.h. der Nutzungszähler (Use counter) des Resetting Codes ist 10. Nach maximal zehnmaliger Eingabe des Resetting Codes (falsch oder korrekt) kann dieser nicht mehr verwendet werden und das Zurücksetzen einer blockierten Signatur-PIN ist nicht mehr möglich. Aufgrund der Einsatzbedingungen an den Personalisierer (s. Kapitel 3.2) beträgt die Mindestlänge des Resetting Codes acht Stellen.

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 „HBA-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 abhängig von der in der Karte gesetzten Sicherheitsumgebung (Security Environment). Nach einer erfolgreichen Benutzauthentisierung können im Security Environment #1 genau eine Signatur und im Security Environment #2 bis zu 250 Signaturen erzeugt werden. Die „HBA-Signaturkarte“ prüft intern, ob der Maximalwert erreicht bzw. überschritten wurde. Anschließend muss die Signatur-PIN erneut eingegeben werden, um Signaturen erzeugen zu können.

„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 abgebrochen.

„Sicherer Datenaustausch“

Die „HBA-Signaturkarte“ unterstützt den verschlüsselten und integritätsgesicherten Datenaustausch mit der externen Welt auf Basis des Secure Messaging gemäß dem ISO Standard [ISO 7816-4] bzw. den Vorgaben an das Kartenbetriebssystem gemäß [EGK-COS].

Hierzu werden durch eine gegenseitige Authentisierung mit der externen Welt vereinbarte symmetrische Schlüssel (Sessionkeys) eingesetzt.

„Speicheraufbereitung“

Die „HBA-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 „HBA-Signaturkarte“ eine Fehlersituation fest, geht sie in einen sicheren Betriebszustand über. In schwerwiegenden Fehlersituationen schließt die „HBA-Signaturkarte“ die Session. In Abhängigkeit des Fehlers ist die „HBA-Signaturkarte“ entweder blockiert oder kann nach Ausführung eines Resets in weiteren Sessions genutzt werden.

„Resistenz gegen Seitenkanalangriffe“

Die „HBA-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 „HBA-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 „HBA-Signaturkarte“ aktiv.

„Selbsttest“

Die „HBA-Signaturkarte“ stellt verschiedene Arten von Selbsttests zur Verfügung. Nach jedem Reset sowie in periodischen Abständen während der Laufzeit werden automatisch Selbsttests 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 „HBA-Signaturkarte“ stellt die kryptographischen Funktionen zur Verfügung. Sie stützt sich auf die kryptographischen Funktionen des evaluierten und zertifizierten Halbleiters und seiner dedizierten Software ab.

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

„Erzeugung von Schlüsselpaaren“

Die „HBA-Signaturkarte“ unterstützt die karteninterne Erzeugung von RSA-Schlüsselpaaren zur Erzeugung von qualifizierten Signaturen mit einer Länge von 2048 Bit.

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

- Es können RSA-Schlüsselpaare mit einer Länge von 2048 Bit generiert werden.
- Die Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2016], Kapitel 3.1 RSA-Verfahren.
- 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 2016], Kapitel 3.1 und 4.
- Die karteninterne Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2016], Kapitel 3.1 hinsichtlich der Wahl des öffentlichen Exponent e mit $2^{16} + 1 \leq e < 2^{256}$.
- Zur Schlüsselerzeugung wird der deterministische Zufallszahlengenerator (DRNG) der „HBA-Signaturkarte“ verwendet.
- Die Schlüsselerzeugung stellt sicher, dass der Signaturschlüssel nicht aus dem Signaturprüfschlüssel ableitbar ist.
- Durch den Prozess der Schlüsselgenerierung wird sichergestellt, dass der Signaturschlüssel und der Signaturprüfschlüssel zusammenpassen.
- Die Schlüsselerzeugung ist resistent gegen Seitenkanalangriffe.
- Die Schlüsselerzeugung ist nur möglich, sofern das Sicherheitsattribut „SCD operational“ des Datenobjekts SCD den Wert „no“ hat.

Bei der karteninternen Erzeugung des Signaturschlüssels werden durch die „HBA-Signaturkarte“ die genannten Sicherheitsanforderungen zur Erzeugung von RSA-Schlüsselpaaren eingehalten. In der Nutzungsphase kann das Kommando GENERATE ASYMMETRIC KEY PAIR nur zum Auslesen des öffentlichen Schlüssels genutzt werden. Eine erneute Generierung des Signaturschlüssels ist nicht möglich.

Der designierte Signaturschlüsselinhaber ist an dem Prozess der Schlüsselgenerierung nicht beteiligt.

„Erzeugung von qualifizierten Signaturen“

Die „HBA-Signaturkarte“ unterstützt die Erzeugung von qualifizierten elektronischen Signaturen mit dem RSA Signaturschlüssel mit einer Schlüssellänge von 2048 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 „HBA-Signaturkarte“ übergebene Hashwert mit einem MAC gesichert werden.
- Erzeugung von digitalen Signaturen mit dem RSA gemäß dem Standard PKCS #1 in der Version 2.1 [PKCS#1] mit dem Formatierungsverfahren RSASSA-PSS sowie dem ISO-Standard 9796-2 [ISO 9796-2] mit dem Formatierungsverfahren ISO9796-2 DS2.
- 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.
- Die Nutzung der Multisignatur-Fähigkeit ist nur im Security Environment #2 möglich. In diesem Fall können Signaturen nur dann erzeugt werden, falls eine erfolgreiche Benutzerauthentisierung erfolgt ist, eine gegenseitige Authentisierung mit Aufbau eines sicheren Kanals stattgefunden hat und die weiteren Zugriffe zur Signaturerzeugung unter Anwendung von Secure Messaging erfolgen. Dabei muss sich die externe Welt unter der Rolle "SAK für Stapel- oder Komfortsignatur" authentisiert haben.

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** 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) Nr. 1	**Anforderung** Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um 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** 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** Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.
Anl. 1, I, 1.1 b)	**Anforderung** 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. Die Prüfung muss bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen.
Anl. 1, I, 1.2	**Anforderung** 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. 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. 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** 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.
- Es sind die Auflagen resultierend aus der TR-Zertifizierung gemäß [TR_PB] und [TR_PB_Anh] zu berücksichtigen.

Einsatzbedingungen an die Nutzung des Signaturzählers

Im Rahmen der Initialisierung wird festgelegt, wie viele Signaturen n (Wert des Signaturzählers, Security Environment #1: n = 1, Security Environment #2: n = 250) 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 Signaturschlüsselinhaber 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 Signaturschlüsselinhabers 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 Signaturschlüsselinhaber 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.
- Die PUK zur Signatur-PIN muss mit einer Mindestlänge von acht Stellen gewählt werden.
- Es sind die Auflagen resultierend aus der TR-Zertifizierung gemäß [TR_PB] und [TR_PB_Anh] zu berücksichtigen.

Anforderungen an den Zertifizierungsdiensteanbieter

- Die eingesetzte Zertifizierungskomponente (Anwendung) zur Erzeugung von qualifizierten Zertifikaten (Certificate Generation Application, CGA) sollte die Sicherheitsanforderungen von [UG_Use], Kapitel 5.5.2 erfüllen.
- 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 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 „HBA-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.

  Stellt ein akkreditierter ZDA seinen Kunden solche Programme zur Verfügung, muss die Erfüllung der genannten Anforderungen im Rahmen der Bestätigung seines Sicherheitskonzeptes durch eine Stelle nach § 18 SigG mitgeprüft und nachgewiesen werden.

Anforderungen an den Signaturschlüssel- bzw. Karteninhaber

- Der Signaturschlüsselinhaber soll zum Ersetzen der Transport-PIN und Setzen der Signatur-PIN 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 noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte Signatur-PIN 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 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 „HBA-Signaturkarte“ so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Zur Erzeugung von qualifizierten Signaturen verwendet der Signaturschlüsselinhaber die „HBA-Signaturkarte“ nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.
- Bei Nutzung der "entfernten PIN-Eingabe" muss sich die „HBA-Signaturkarte“ in einem eHealth-Kartenterminal in einem gesicherten Bereich befinden und für die PIN-Eingabe muss der Signaturschlüsselinhaber ein eHealth-Kartenterminal nutzen, das er unter seiner Kontrolle hat. Der gesicherte Bereich muss über hinreichend Schutz verfügen, um die alleinige physische Kontrolle des Signaturschlüsselinhabers über die „HBA-Signaturkarte“ zu gewährleisten. Insbesondere darf die „HBA-Signaturkarte“ nicht entwendet werden können.

Anforderungen an Hersteller von Signaturanwendungskomponenten

- Der Hersteller einer Signaturanwendungskomponente muss die Schnittstellen des Betriebssystems STARCOS 3.6 COS C1 sowie der *SSCD-Anwendung* geeignet berücksichtigen.
- Bei der Erzeugung einer qualifizierten Signatur mit Übergabe eines extern berechneten Hashwerts 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.

3.3 Algorithmen und zugehörige Parameter

Die „HBA-Signaturkarte“ stellt zur Erstellung von elektronischen Signaturen das RSA-Verfahren bereit. Das RSA-Verfahren basiert auf dem RSA-Algorithmus mit einer Schlüssellänge von 2048 Bit. Die Schlüssellänge wird durch die berücksichtigten Initialisierungsskripte während der Initialisierung gesetzt und kann nachträglich nicht mehr geändert werden. Als Formatierungsverfahren werden RSASSA-PSS gemäß [PKCS#1] und ISO9796-2 DS2 gemäß [ISO 9796-2] unterstützt.

Zur Erzeugung von elektronischen Signaturen kann eine karteninterne bzw. eine teilweise karteninterne Hashwertberechnung mit der Hashfunktion SHA-256 gemäß [FIPS 180-4] 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 Zufallszahlengenerators (DRNG) unterstützt, dessen Seed durch den Zufallszahlengenerator (TRNG) der zugrundeliegenden Hardware erzeugt wird. Der DRNG wurde im Rahmen der Evaluierung als DRG.4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet. Die Anforderungen gemäß [Alg_Kat 2016] an die erforderliche Entropie der Seed werden erfüllt.

Der TRNG der zugrundeliegenden Hardware von Infineon Technologies ist ein Zufallszahlengenerator 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 2016] als geeignet eingestuft.

Für die Hashfunktionen gemäß [FIPS 180-4] 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 2022
SHA-256, SHA-512/256, SHA-384, SHA-512

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

Tabelle 5: Mindest-Schlüssellängen für den RSA Algorithmus

Parameter	Bis Ende 2022
Schlüssellänge	1976 Bit

Die Formatierungsverfahren RSASSA-PSS und ISO9796-2 DS2 sind gemäß [Alg_Kat 2016] bis 2022 geeignet.

Diese Bestätigung der „HBA-Signaturkarte“ ist somit **maximal** gültig bis **31.12.2022**.

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 3.6 QES C1 wurde erfolgreich nach den Common Criteria (CC) Version 3.1 mit der Prüfstufe **EAL 4+** (EAL 4 mit der Augmentierung AVA_VAN.5) evaluiert.

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

Das zugrundeliegende Kartenbetriebssystem STARCOS 3.6 COS C1 wurde erfolgreich nach den Common Criteria (CC) Version 3.1 mit der Prüfstufe **EAL 4+** (EAL 4 mit den Augmentierungen ALC_DVS.2, ATE_DPT.2 und AVA_VAN.5) evaluiert. Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential.

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0916-2015 vom 7. August 2015 vor.

Die Evaluierung des Produkts STARCOS 3.6 QES C1 wurde in Form einer sogenannten „Composition Evaluation“ durchgeführt, die die Evaluierungsergebnisse der CC Evaluierung des M7893 B11 des Herstellers Infineon Technologies berücksichtigt. Diese Evaluierung erfolgte mit der Prüfstufe **EAL 6+** (EAL 6 mit der Augmentierung ALC_FLR.1). Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential.

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0879-V2-2015 vom 13. November 2015 vor.

Die für die SSEE nach SigV maßgebende Evaluierungsstufe **EAL 4+** (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 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154).

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154).

[Alg_Kat 2016] 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, 9. Dezember 2015, Veröffentlicht auf den Internetseiten des Bundesanzeigers (www.bundesanzeiger.de) unter "BAnz AT 01.02.2016 B5".

[AIS 20] Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013

[AIS 31] Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema, AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013

[BSI-CC-PP-0059] CC Protection profile: Protection profiles for secure signature creation device, Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01, Information Society Standardization System (CEN/ISSS), 2012-01-23

[BSI-CC-PP-0071] CC Protection profile: Protection profiles for secure signature creation device, Part 2: Extension for device with key generation and trusted communication with certificate generation application, Version 1.0.1, BSI-CC-PP-0071-2012, Information Society Standardization System (CEN/ISSS), 2012-11-14

[BSI-CC-PP-0082] CC Protection Profile: Card Operating System Generation 2 (PP COS G2), Version 1.9, BSI-CC-PP-0082-V2, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014-11-18

[EGK-COS] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH, inklusive der normativen Errata

[EGK-Wrap] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.6.0, 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.6 QES C1, Version 1.1, 13.05.2016

[FIPS 180-4] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012

[FIPS 186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[FIPS 197] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[FSP_IF_COS] STARCOS 3.6 Functional Specification – Part 1: Interface Specification, Version 1.19, 31.07.2015

[HBA-ObjSys] Spezifikation des elektronischen Heilberufsausweis HBA-Objektsystem, Version 3.8.1, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 30.09.2015

[IFX_Cert] Certification Report of the underlying hardware platform, BSI-DSZ-CC-0879-V2-2015 for Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006,SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-11-13

[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

[ISO 9796-2] ISO/IEC 9796-2:2010 Information technology -- Security techniques -- Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO, 2010-12

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, October 27, 2012

[RFC 5639] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[SP800-38B] ISO 15946, Information technology – Security techniques – Cryptographic techniques Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

[ST] Security Target STARCOS 3.6 QES C1, Giesecke & Devrient GmbH, Version 1.1/10.05.16

[STHW] Security Target Lite M7893 B11 Including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Version 0.2, Infineon Technologies AG, Chipcard and Security, 2015-08-31

[TR-03106] Technische Richtlinie BSI TR-03106, eHealth – Zertifizierungskonzept für Karten der Generation G2, Bundesamt für Sicherheit in der Informations-technik (BSI), Version 1.1, 22.05.2015

[TR-03110] Technische Richtlinie BSI TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.10, Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-03110, 20.03.2012

[TR-03111] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 2.0, 28. Juni 2012

[TR-03114] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03114, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007

[TR-03115] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007

[TR-03143] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03143, eHealth G2-COS Konsistenz-Prüftool, Version 1.0, 08.05.2015

[TR-03144] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03144, eHealth – Konformitätsnachweis für Karten-Produkte der Karten-generation G2, Version 1.1, 22.05.2015

[UG_Main] Guidance Documentation STARCOS 3.6 – Main Document, Version 1.7/ 29.07.2015

[UG_Ini] Guidance Documentation for the Initialization Phase STARCOS 3.6 QES, Version 1.2/ Status 10.05.2016

[UG_Inlay] STARCOS 3.6 COS C1/2 Guidance Documentation for Inlay Production, Version 1.1/ Status 13.07.2015

[UG_internal] STARCOS 3.6 Internal Design Specification, Version 1.3, Status 31.07.2015

[UG_Pers] Guidance Documentation for the Personalization Phase STARCOS 3.6 QES, Version 1.1/ Status 07.10.2015

[UG_Use] Guidance Documentation for the Usage Phase STARCOS 3.6 QES, Version 1.1/ Status 10.05.2016

[UG_Wrapper] STARCOS 3.6 COS C1/2 Guidance Documentation for the Wrapper, Version 1.3/ Status 29.07.2015

[TR_PB] SRC, TR-Prüfbericht STARCOS 3.6 Health HBA R1, Version 1.4, 01.06.2016

[TR_PB_Anh] SRC, Anhang zum TR-Prüfbericht STARCOS 3.6 Health HBA R1, Version 1.3, 30.05.2016

Ende der Bestätigung