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
„TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

SRC.00016.TE.11.2012

Bonn, den 28.11.2012

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 17. Dezember 2009 (BGBl. I S. 3932)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung des Produktes und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P der T-Systems International GmbH.

Das Produkt wird durch den Hersteller in der Produktvariante TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P vertrieben. Das Produkt ist eine Signaturkarte und wird im Folgenden kurz als „Sig Karte“ bezeichnet.

1.2 Auslieferung

Die „Sig Karte“ ist realisiert als sogenannte Dual Interface Karte, d.h. die Karte verfügt über eine kontakt-basierte und eine kontaktlose Schnittstelle. Je nach Konfiguration kann die Karte als ausschließlich kontakt-basierte, ausschließlich kontaktlose oder als Dual Interface Karte eingesetzt werden. Die Hardware der „Sig Karte“ besteht aus dem IFX Secure Smart Card Controller SLE78CLX1440P. Die Software besteht aus dem Betriebssystem TCOS 3.0 Signature Card Version 2.0 Release 1 (ROM, ggf. teilweise im EEPROM), sowie aus der Anwendung zur Erzeugung qualifizierter elektronischer Signaturen, die im Weiteren als „eSign-Anwendung“ bezeichnet wird.

Die Smartcard Embedded Software enthält das Betriebssystem TCOS 3.0 Signature Card Version 2.0 Release 1. 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 *eSign-Anwendung* und kann grundsätzlich mit weiteren Anwendungen (wie bspw. der bereits installierten Netkey-Applikation) versehen werden. Diese sind jedoch **nicht** Gegenstand der vorliegenden Bestätigung.

Das Produkt kann in den Varianten initialisiert, pre-personalisiert oder personalisiert ausgeliefert werden.

- Eine initialisierte „Sig Karte“ stellt zwar alle Funktionen bereit, es fehlen aber noch Signaturschlüssel und Zertifikat. Die Schlüsselerzeugung wird nach der Auslieferung durch den designierten Inhaber der sicheren Signaturerstellungseinheit initiiert. Ausgeführt wird die Schlüsselgenerierung, wie auch die Zertifikatseinbringung, von einem Zertifizierungsdiensteanbieter. Diese Aktivierungsprozedur ist vergleichbar mit der der eSign-Anwendung, die in einem elektronischen Personalausweis angewendet wird.
- Eine pre-personalisierte „Sig Karte“ enthält alle benötigten Schlüssel und kann anhand von Authentifizierungsdaten durch den Signierer vom Zustand „nicht-einsatzbereit“ in den Zustand „einsatzbereit“ gebracht werden. Hierzu ist noch das Zertifikat über den öffentlichen kryptografischen Signaturschlüssel durch einen autorisierten Zertifizierungsdiensteanbieter (ZDA) zu erstellen und in die „Sig Karte“ einzubringen.

- Eine personalisierte „Sig Karte“ enthält neben allen Karteninhaberdaten und des Signaturschlüsselpaares auch das Zertifikat über den öffentlichen kryptografischen Signaturschlüssel zur Signaturprüfung. Diese „Sig Karte“ ist somit bereits an den Endkunden gebunden.

Die Produktion und Auslieferung an den Endkunden, dem designierten Inhaber der sicheren Signaturerstellungseinheit „Sig Karte“ unterliegt über die Anforderungen des Signaturgesetzes hinaus spezifischen Gegebenheiten. Dies bezieht sich in erster Linie auf die Einbettung von ICs zur endgültigen Auslieferung an den im Rahmen der Evaluierung der „Sig Karte“ zertifizierten und auditierten Standorten der Einbetter.

Während der Initialisierung und Personalisierung der „Sig Karte“ werden durch den Kartenhersteller mindestens die folgenden Daten eingebracht:

- Master File (MF), u.a. mit folgenden Daten
  - einem signierten Chipauthentisierungsschlüssel
  - Authentisierungsdaten des Karteninhabers (Card Access Number (CAN); Karten-PINs)
- *eSign-Anwendung*

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

Für die bestätigte Version der TCOS 3.0 Signature Card Version 2.0 Release 1/ SLE78CLX1440P sind in [TCOSADM], Anhang E die herstellerspezifischen Werte zu den Parametern „Chip Manufacturer“, „Chip Type“, „Card Type (TCOS 3.0 Signature Card)“, „OS Version“, „OS Release Number“, „(Pre-)Completion Code Version“ und „File System Version“ in Abhängigkeit der zugrundeliegenden Hardware (Infineon SLE78CLX1440P) angegeben. Sie können während der Produktion bei dem Kommando „Format“ mit Verwendung der Option „Reading of Chip Information“ aus der Karte ausgelesen werden.

1.3 Lieferumfang

Der Lieferumfang des Produktes besteht aus den folgenden Komponenten:

Tabelle 1: Lieferumfang

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
1	Hardware	IFX Secure Smart Card Controller SLE78CLX1440P Package Type M8.4 (inkl. IC dedicated Test Software)			---
2	Software (Betriebs-system)	Smartcard Embedded Software (Betriebssystem) TCOS 3.0 Signature Card Version 2.0 Release 1 (implementiert im ROM/EEPROM des Halbleiters)			---
3	Software (Filesystem)	Smartcard Embedded Anwendung (*eSign-Anwendung* sowie die nicht in der Bestätigung betrachtete Netkey-Applikation), implementiert durch das File System '01'			---
4	Dokumenta-tion	TCOS 3.0 Signature Card Version 2.0 Re-lease 1/SLE78CLX1440P, Administrator's Guidance, T-Systems International GmbH, [TCOSADM]	0.1	02.07.2012	Dokument in elektronischer Form
5	Dokumenta-tion	TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P, Operational Guidance, T-Systems International GmbH, [TCOSOPG]	1.0	21.09.2012	Dokument in Papierform oder elektronisch

1.4 Hersteller

Hersteller des Produktes ist die T-Systems International GmbH, Untere Industriestraße 20, D-57250 Netphen.

2. Funktionsbeschreibung

Funktionalität und Architektur

Das Chipkartenprodukt „TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P“ ist vorgesehen für den Einsatz als Signaturkarte. Aus technischer Sicht ist die „Sig Karte“ als Dual Interface Chipkarte mit einem proprietären Betriebssystem und einer Anwendungsebene, die direkt auf der Betriebssystemebene aufsetzt, realisiert.

Die „Sig Karte“ basiert auf dem Halbleiter „Infineon SLE78CLX1440P " mit proprietärer dedizierter Software der Infineon Technologies AG. Die Halbleiterfamilie SLE78CLX1440P inklusive der dedizierten Software wurde nach CC EAL 5+ evaluiert (CC Version 3.1) und wurde durch das BSI unter der Registrierungsnummer BSI-DSZ-CC-0640-2010 zertifiziert.

Die Software besteht aus dem Betriebssystem TCOS 3.0 Signature Card Version 2.0 Release 1 (ROM, ggf. teilweise im EEPROM) sowie aus der *eSign-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen.

Das Betriebssystem TCOS 3.0 Signature Card Version 2.0 Release 1 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 TCOS Betriebssystems unterstützt insbesondere die *eSign-Anwendung*. Neben der dedizierten *eSign-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen können sich grundsätzlich weitere Anwendungen (wie bspw. der bereits installierten Netkey-Applikation) auf der „Sig Karte“ 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 elektronischen Signaturen (Elliptische Kurven)

Zusammenfassend besteht die „Sig Karte“ insbesondere aus den folgenden Komponenten:

- Halbleiter (IC) von Infineon (SLE78CLX1440P) mit proprietärer dedizierter Software,
- TCOS Betriebssystem „TCOS 3.0 Signature Card Version 2.0 Release 1“ und
- der *eSign-Anwendung*.

Nach Ausgabe der „Sig Karte“ ist sie in einem der in Kapitel 1.2 erläuterten Zustände.

Im Zustand personalisiert sind sowohl der Signaturprüfschlüssel als auch das Zertifikat über den öffentlichen kryptografischen Signaturprüfschlüssel bereits in der Karte enthalten. Zur Aktivierung der „Sig Karte“ als sichere Signaturerstellungseinheit muss der Inhaber die voreingestellte Transport-PIN noch durch eine gültige Signatur-PIN ersetzen.

Befindet sich die Karte im Zustand pre-personalisiert, enthält die „Sig Karte“ alle benötigten Schlüssel und kann anhand von Authentifizierungsdaten durch den Signaturschlüsselinhaber vom Zustand „nicht-einsatzbereit“ in den Zustand „einsatzbereit“ gebracht werden. Zur Aktivierung der „Sig Karte“ als sichere Signaturerstellungseinheit muss der Inhaber die voreingestellte Transport-PIN zunächst durch eine gültige Signatur-PIN ersetzen. Anschließend ist noch das Zertifikat über den Signaturprüfschlüssel durch einen ZDA zu erstellen und in die „Sig Karte“ einzubringen (vgl. mit Zustand initialisiert).

Im Zustand initialisiert kann die „Sig Karte“ durch den Inhaber unter Kontrolle des zertifikatsausstellenden Zertifizierungsdiensteanbieters als sichere Signaturerstellungseinheit aktiviert werden. Hierzu ist an einem Signaturterminal durch den designierten Signaturschlüsselinhaber zunächst die Signatur-PIN in der Karte zu setzen. Erst danach kann die Generierung des Signaturschlüssels in der Karte durch einen autorisierten Zertifizierungsdiensteanbieter initiiert werden. Dieser muss sich hierzu gegenüber der Karte authentisieren. Nur ZDAs, die sich gegenüber der Karte erfolgreich authentisieren können, ist es möglich, die Schlüsselgenerierung auszulösen. Während der Aktivierung wird durch den ZDA in einem sicheren Kanal zwischen ZDA und „Sig Karte“ die Schlüsselgenerierung in der Karte initiiert und der öffentliche Signaturprüfschlüssel aus der Karte ausgelesen. Der ZDA darf das qualifizierte Zertifikat erst dann ausstellen, wenn er sich davon überzeugt hat, dass sich die „Sig Karte“ unter der Kontrolle des Signaturschlüsselinhabers befindet. Das durch den ZDA erzeugte qualifizierte Signaturschlüsselzertifikat kann anschließend mit Nutzung des sicheren Kanals integritätsgeschützt in die Karte eingebracht werden.

Der sichere Kanal sichert sowohl die Vertraulichkeit als auch die Authentizität der kommunizierten Daten (Secure Messaging).

Nach Aktivierung der *eSign-Anwendung* kann die „Sig Karte“ 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 „Sig Karte“ ist eine sogenannte Multisignatur-fähige sichere Signaturerstellungseinheit (Multisignatur-SSEE), mit der nach einer erfolgreichen Eingabe der Signatur-PIN entweder genau eine, eine begrenzte Anzahl (bis maximal 2^{16}-2) 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 „Sig Karte“ 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 „Sig Karte“ gelöscht. Anschließend muss die Signatur-PIN erneut eingegeben werden, um Signaturen erzeugen zu können. Die Verwendung einer Multisignatur-SSEE bedingt spezifische Einsatzbedingungen (s. Einsatzbedingungen an die Nutzung des Signaturzählers).

Die „Sig Karte“ verwendet ein PIN-Konzept (PIN-PIN-Verfahren), das die optionale Verwendung einer zweiten Signatur-PIN (Signatur-PIN2 oder PIN2.QES) durch den Signaturschlüsselinhaber ermöglicht. Die Signatur-PIN2 verfügt über eine Mindestlänge von

acht Stellen und ist somit von der eigentlichen Signatur-PIN unterscheidbar. Sie kann als Resetting-Code der Signatur-PIN sowie zum Erzeugen von qualifizierten Signaturen genutzt werden. Analog dazu, kann die Signatur-PIN auch als Resetting-Code von Signatur-PIN2 verwendet werden.

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

- Wechsel einer Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der aktuell gültigen Signatur-PIN),
- Rücksetzen des Fehlbedienungszählers der Signatur-PIN mit oder ohne Setzen einer neuen Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der Signatur-PIN2 (PIN2.QES))
- Rücksetzen des Fehlbedienungszählers der Signatur-PIN2 mit oder ohne Setzen einer neuen Signatur-PIN2 (nach erfolgreicher Benutzerauthentisierung mit der Signatur-PIN (PIN1.QES))
- Außerbetriebnahme der Signaturfunktion mit Terminieren des Signaturschlüssels. In diesem Fall muss der Signaturschlüssel terminiert werden. Die Außerbetriebnahme setzt eine erfolgreiche Benutzerauthentisierung voraus.

Nach einer Außerbetriebnahme kann die *eSign-Anwendung* erneut aktiviert werden, d.h. es kann unter Kontrolle eines zertifikatsausstellenden ZDA ein neuer Signaturschlüssel in der Karte generiert, ein qualifiziertes Zertifikat erzeugt und dieses in die Karte eingebracht werden. Diese erneute Aktivierung der *eSign-Anwendung* erfolgt analog zur Aktivierung, die dem Auslieferungszustand initialisiert entspricht.

Alle für die Signaturanwendung relevanten Zugriffe über die kontaktlose Schnittstelle auf der „Sig Karte“ müssen an einem Signaturterminal unter Anwendung von Secure Messaging erfolgen. Zur gegenseitigen Authentisierung von Terminal und Karte sowie zum Aufbau eines sicheren Kommunikationskanals werden die Authentisierungsprotokolle PACE (kontaktlose Schnittstelle), Terminal- und Chipauthentisierung (kontaktlose und kontakt-basierte Schnittstelle) verwendet. Im Rahmen der Terminalauthentisierung werden die Zugriffsrechte des Terminals nachgewiesen. Hierzu gehören insbesondere auch die Rechte

- eines ZDA zur Aktivierung der *eSign-Anwendung*, die in einem für den ZDA spezifischen CV-Zertifikat kodiert sein müssen,
- eines Signaturterminals zur Erstellung von qualifizierten elektronischen Signaturen sowie zum Management der Signatur-PIN.

Zugriffe über die kontakt-basierte Schnittstelle zur Erzeugung von qualifizierten Signaturen und zur Administration der Signatur-PIN können auch ohne Secure Messaging erfolgen. Zugriffe eines ZDA (z.B. zur Schlüsselerzeugung) müssen jedoch immer mit Secure Messaging erfolgen.

Die Sicherheitseigenschaften der „Sig Karte“ werden mit der Beschreibung der Sicherheitsfunktionen weiter erläutert.

Die Installation des Filesystems (Filesystem '01’) 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 „Sig Karte“ nicht unterstützt.

Zur Erzeugung von Signaturschlüsselpaaren sowie von qualifizierten elektronischen Signaturen werden durch die „Sig Karte“ die folgenden kryptographischen Algorithmen unterstützt:

- DSA auf Basis elliptischer Kurven (ECDSA) basierend auf Gruppen E(Fp) (vgl. [TR-03111]) mit einer Schlüssellänge von 256, 320, 384 und 512 Bit sowie
- Zufallszahlenerzeugung auf Basis des Zufallszahlengenerators (RNG) der zugrundeliegenden Hardware. Dieser ist ein Zufallszahlengenerator mit einer P2 (SOF „hoch“) 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. [HW ST]).

Die „Sig Karte“ unterstützt die standardisierten Domain Parameter gemäß [RFC 5639] sowie die NIST P-256 Kurve, die in [TR-03110], Anhang A.2.1.1 angegeben ist.

Weiterhin werden die folgenden Algorithmen unterstützt. Diese kommen bei der Signaturerstellung in der Karte nicht zur Anwendung und sind daher nicht Gegenstand dieser Bestätigung.

- Hashfunktionen SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 gemäß [FIPS 180-2], wobei SHA-1 und SHA-256 zur Ableitung von symmetrischen Sessionkeys genutzt wird,
- Diffie-Hellman auf Basis elliptischer Kurven (ECDH) gemäß [TR-03111] mit einer Schlüssellänge von 192, 224, 256, 320, 384 oder 512 Bit 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. Zur Verschlüsselung der kommunizierten Daten wird der CBC Modus eingesetzt. Zur Sicherung der Datenintegrität wird der „CMAC Mode for Authentication“ verwendet, vgl. [SPUB 800-38B].

Die „Sig Karte“ wurde auf Basis der Common Criteria in der Version 3.1 sowie des Protection Profiles [BSI-CC-PP-0035] für Smartcard basierte Produkte erfolgreich evaluiert (vgl. [ETR]). Die Prüftiefe beträgt EAL 4+ mit der Augmentierung AVA_VAN.5.

Weiterhin berücksichtigt die „Sig Karte“ das „Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation“, prEN 14169-1:2009, [PP SSCD Part 2].

Sicherheitsfunktionen bzw. –eigenschaften der „Sig Karte“

Die „Sig Karte“ 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 „Sig Karte“ verwendet eine rollenbasierte Zugriffskontrolle. Diese unterscheidet u.a. zwischen den Rollen „Administrator“ (Administrator) und „Signierer“ (Signatory). Weiterhin werden die folgenden Sicherheitsattribute verwendet:

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

Der Zertifizierungsdiensteanbieter (ZDA), der den Prozess zur Aktivierung der *eSign-Anwendung* durchführt und hierzu über spezielle Zugriffsrechte verfügt, agiert in der Rolle des Administrators. Zur Nutzung dieser Rechte muss er sich gegenüber der Karte authentisieren (Terminalauthentisierung) und seine Zugriffsrechte gegenüber der Karte nachweisen.

Ein Anwender authentisiert sich gegenüber der „Sig Karte“ durch Eingabe der Signatur-PIN als Signierer.

Alle für die Signaturanwendung relevanten Zugriffe über die kontakt-basierte bzw. kontaktlose Schnittstelle der „Sig Karte“ müssen an einem Signaturterminal erfolgen. Zur gegenseitigen Authentisierung und zum Aufbau eines sicheren Kommunikationskanals zwischen Terminal und „Sig Karte“ werden die folgenden Authentisierungen verwendet:

- **PACE Protokoll** zur gegenseitigen Authentisierung und Aufbau eines sicheren Kanals 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 eines neuen qualifizierten Signaturschlüssels).
- **Chipauthentisierung** zur Authentisierung des Chips gegenüber dem Terminal sowie Aufbau eines sicheren Kanals zur verschlüsselten und integritätsgesicherten Kommunikation zwischen Karte und Terminal.

Bei kontaktloser Kommunikation muss die Terminal- und Chipauthentisierung unter dem sicheren Kanal, der mit dem erfolgreichen Durchlaufen des PACE Protokolls aufgebaut wird, durchgeführt werden. Der anschließend mit der erfolgreichen Chipauthentisierung aufgebaute sichere Kanal ersetzt dann den sicheren Kanal aus dem PACE Protokoll.

Bei einer kontakt-basierten Kommunikation kann ein sicherer Kanal mit Hilfe der Terminal- und Chipauthentisierung aufgebaut werden.

Diese Vorgehensweise ist insbesondere bei den Zugriffen eines ZDA zur Schlüsselerzeugung und Einbringung des qualifizierten Zertifikates erforderlich. Im Falle eines kontaktlosen Zugriffs wird durch das PACE Protokoll zunächst die lokale Luftschnittstelle zwischen Signaturterminal und „Sig Karte“ abgesichert. Nach Durchführung von Terminal- und Chipauthentisierung können die entfernten Zugriffe des ZDA auf die Karte unter dem sicheren Kanal, der durch die Chipauthentisierung aufgebaut wurde, geschützt erfolgen. Im Falle eines kontakt-basierten Zugriffs wird ein sicherer Kanal mit Hilfe der Terminal- und Chipauthentisierung realisiert. Hierdurch kann eine Ende-zu-Ende Sicherheit zwischen ZDA und Chip realisiert werden.

Weiterhin ist die Zugriffskontrolle realisiert unter Anwendung von Zugriffsbedingungen, die als Sicherheitsattribute in der „Sig Karte“ 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 u.a. die folgenden Regeln:

- Die Aktivierung der *eSign-Anwendung* (Erzeugung des Signaturschlüsselpaars, Auslesen des öffentlichen Schlüssels und Einbringung des qualifizierten Signaturschlüsselzertifikats) ist nur für einen autorisierten ZDA unter Aufbau und Nutzung eines sicheren Kanals möglich. Der Aufbau eines sicheren Kanals erfolgt mit einer gegenseitigen Authentisierung (PACE, Terminal- und Chipauthentisierung). Zur Durchführung einer Aktivierung muss der ZDA seine Zugriffsrechte nachweisen (in diesem Fall hat das Sicherheitsattribut „SCD / SVD Management“ für die zugreifende Rolle den Wert „authorised“). Im Falle einer bereits personalisierte „Sig Karte“ gilt dies nur im Zustand terminiert.
- Das Setzen der 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 es ist kein nutzbarer Signaturschlüssel auf der Karte vorhanden) der „Sig Karte“ nach einer erfolgreichen Benutzerauthentisierung erfolgen (Karten-PIN bzw. Transport-PIN nach Auslieferung der „Sig Karte“ im Zustand personalisiert oder pre-personalisiert).
- Das Setzen der Signatur-PIN2 durch den designierten Signaturschlüsselinhaber kann nur nach einer erfolgreichen Benutzerauthentisierung erfolgen (Signatur-PIN) und nachdem die Signatur-PIN bereits gesetzt wurde.
- 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 Außerbetriebnahme der Signaturfunktion setzt eine erfolgreiche Benutzer-authentisierung voraus (Karten-PIN). Nach einer erfolgreichen Außerbetriebnahme kann die *eSign-Anwendung* nicht zur Erzeugung qualifizierter Signaturen verwendet werden, d.h. die *eSign-Anwendung* hat nicht den Status „Einsatzbereit“.
- Signaturen können nur durch den Signaturschlüsselinhaber generiert werden. Hierzu ist eine vorherige erfolgreiche Benutzerauthentisierung mit einer Signatur-PIN erforderlich.
- Sensitive Daten wie Signaturschlüssel, Karten-PIN und Signatur-PIN können nicht über Kommandos des Betriebssystems ausgelesen werden.

„Password Authenticated Connection Establishment (PACE) Protokoll“

Die „Sig Karte“ 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 „Sig Karte“ 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 „Sig Karte“ und Terminal 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 „Sig Karte“ unterstützt die Kontrolle des Signaturschlüsselinhabers über die sichere Signaturerstellungseinheit bei Anwendung der Karte über die Luftschnittstelle.

In Abhängigkeit der durchzuführenden Funktion sind für das PACE Protokoll die folgenden Ausgangswerte zu unterscheiden. Dabei kann die CAN auf dem Kartenkörper aufgedruckt sein und ist damit kein Geheimnis für jeden, der physischen Zugriff auf die „Sig Karte“ hat. Durch Eingabe einer CAN wird vom Karteninhaber die Kommunikation mit einer kontaktlosen Karte begonnen und ist damit ein Äquivalent zum Einführen einer kontakt-basierten Karte in ein Lesegerät. Dadurch wird eine unbeaufsichtigte Kommunikation mit der „Sig Karte“ erschwert.

Die Durchführung der jeweiligen Funktion ist ggf. von zusätzlichen Sicherheitsfunktionen abhängig (z.B. erfolgreiche Eingabe der Signatur-PIN beim Wechsel der Signatur-PIN). Die Liste beschreibt lediglich welcher Parameter im Rahmen des PACE Protokolls zu verwenden ist.

- Card Access Number (CAN, sechsstellige dezimale zufällige Nummer)
    - PACE Protokoll
- Karten-PIN
    - Erzeugung des Signaturschlüsselpaares unter Kontrolle des zertifikatsausstellenden ZDA
    - Setzen einer neuen Signatur-PIN
    - Löschen des Signaturschlüssels

Die „Sig Karte“ unterstützt die Durchführung des PACE-Protokolls über die kontakt-basierte Schnittstelle.

„Terminalauthentisierung“

Die „Sig Karte“ unterstützt die Durchführung der Terminalauthentisierung. Dieses Protokoll wird zur Authentisierung des Terminals (Challenge-and-Response Protokoll) gegenüber der „Sig Karte“ genutzt. Weiterhin erfolgt mit dem Protokoll der Nachweis der Zugriffsrechte des Signaturterminals gegenüber der „Sig Karte“. Diese Rechte sind bei kontaktloser Kommunikation an den sicheren Kanal, der anschließend mit der Chipauthentisierung aufgebaut wird, gebunden.

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

„Chipauthentisierung“

Die „Sig Karte“ 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 einem Hybridverfahren auf der Grundlage des Diffie-Hellman Protokolls zur Schlüsselvereinbarung. Dabei werden das ephemere DH Schlüsselpaar des Terminals (aus der Terminalauthentisierung) sowie das statische DH Schlüsselpaar der „Sig Karte“ 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 auf Basis elliptischer Kurven gemäß [TR-03111].

Die Chipauthentisierung verwendet den ephemeren öffentlichen Terminalschlüssel aus der vorangegangenen Terminalauthentisierung. Somit wird eine gegenseitige Authentisierung von Terminal und Karte erreicht.

Zur Chipauthentisierung besitzt die „Sig Karte“ einen Chipauthentisierungsschlüssel (statisches DH-Schlüsselpaar). Der öffentliche Schlüssel wird in der „Sig Karte“ in einer signierten Datenstruktur im EF.CardSecurity im MF der Karte gespeichert. Die Signatur wird durch den Hersteller mit seinem Schlüssel erzeugt.

Der Hersteller signiert nur öffentliche Schlüssel authentischer Signaturkarten. Hierüber kann die Echtheit der personalisierten Daten in EF.CardSecurity nachgewiesen werden (passive Authentisierung). Durch die erfolgreiche Chipauthentisierung und damit dem Nachweis, dass die Karte über den zugehörigen privaten Schlüssel verfügt, kann letztendlich die Echtheit des Chips nachgewiesen werden. D.h. es kann auch nachgewiesen werden, dass es sich bei der „Sig Karte“ um eine evaluierte und bestätigte Signaturkarte handelt.

„Prozesse der PIN-basierten Authentisierung zur Erzeugung qualifizierter Signaturen (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 einer vom Benutzer eingegebenen Signatur-PIN mit dem in der „Sig Karte“ (in der *eSign-Anwendung*) geheim gespeicherten Referenzwert (RAD).

Nach Auslieferung an den designierten Signaturschlüssel-Inhaber enthält die „Sig Karte“ keine echte Signatur-PIN. Es kann insbesondere keine gültige qualifizierte Signatur erzeugt werden.

Befindet sich die „Sig Karte“ im Zustand „initialisiert“, so ist die Signatur-PIN mit einer Mindestlänge von *m* Stellen (Defaultwert für die Mindestlänge ist sechs) vor der Aktivierung der *eSign-Anwendung* durch den designierten Signaturschlüsselinhaber zu setzen. Befindet sich die „Sig Karte“ im Zustand pre-personalisiert oder personalisiert muss der Signaturschlüsselinhaber die Transport-PIN durch eine echte Signatur-PIN ersetzen.

Zum Setzen der Signatur-PIN2 ist eine (implizite oder explizite) erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erforderlich. Weiterhin kann das Setzen der Signatur-PIN2 erst erfolgen, nachdem die Signatur-PIN gesetzt wurde.

Beide Signatur-PINs besitzen einen separaten Fehlbedienungszähler (FBZ) mit einem Initialwert (sig_{ad}), der nach Eingabe einer falschen PIN um eins erniedrigt wird. D.h. nach einer wiederholten Eingabe einer falschen PIN (mit sig_{ad} Wiederholungen) steht der FBZ auf Null und die betreffende Signatur-PIN ist blockiert. Sind beide Signatur-PINs blockiert, ist die „Sig Karte“ blockiert. In diesem Zustand kann weder eine weitere Prüfung einer Signatur-PIN erfolgen, noch eine qualifizierte elektronische Signatur erzeugt werden. Nach einer erfolgreichen Eingabe einer Signatur-PIN wird der zugehörige FBZ auf den Initialwert sig_{ad} gesetzt, jedoch nur dann, wenn die betroffene Signatur-PIN bzw. die „Sig Karte“ nicht blockiert ist. Der Initialwert sig_{ad} wird im Rahmen der Initialisierung der Karte gesetzt und hat für beide Signatur-PINs den Defaultwert drei.

Mit einem (Neu-)Setzen einer Signatur-PIN durch das Kommando CHANGE REFERENCE DATA ist keine Reinitialisierung des zugehörigen FBZ verbunden. Weiterhin kann ein (Neu-)Setzen einer Signatur-PIN durch das Kommando CHANGE REFERENCE DATA nur erfolgen, falls diese Signatur-PIN nicht blockiert ist.

Mit den Initialisierungsdaten, die durch den Kartenhersteller bereitgestellt werden, sind die Defaultwerte Mindestlänge der Signatur-PIN (sechs Byte), der Signatur-PIN2 (acht Byte) und FBZ (drei) gültig. Die Werte können im Rahmen der Personalisierung durch den Kartenhersteller geändert werden (vgl. Kapitel 3.2, Anforderungen an den Personalisierer).

Der FBZ der Signatur-PIN kann unter Anwendung der zweiten eingerichteten Signatur-PIN2 (PIN2.QES) zurückgesetzt werden. Die „Sig Karte“ unterstützt eine Signatur-PIN2 mit einer Länge von mindestens acht Stellen, die als Resetting-Code der Signatur-PIN verwendet werden kann. Analog dazu, kann der FBZ der Signatur-PIN2 unter Anwendung der Signatur-PIN zurückgesetzt werden.

Zum Zurücksetzen ist das Kommando RESET RETRY COUNTER zu verwenden. Dabei ist ein gleichzeitiger Wechsel einer Signatur-PIN möglich. Es erfolgt kein Setzen des Sicherheitszustandes einer Signatur-PIN, d.h. das Zurücksetzen einer blockierten Signatur-PIN ermöglicht ohne eine Prüfung der Signatur-PIN 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 „Sig Karte“ authentisieren, d.h. das Ändern einer Signatur-PIN in eine neue Signatur-PIN ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der jeweils aktuellen Signatur-PIN möglich (Kommando CHANGE REFERENCE DATA mit alter und neuer PIN).

Die Anzahl der Signaturen, die nach einer erfolgreichen Eingabe der Signatur-PIN erzeugt werden können, ist konfigurierbar. Es sind die Werte von 1 bis 2^{16}-2 und unendlich konfigurierbar. Die „Sig Karte“ prüft intern, ob der Maximalwert erreicht bzw. überschritten wurde. Anschließend muss die Signatur-PIN erneut eingegeben werden, um Signaturen erzeugen zu können. Mit dem Filesystem, das der Kartenhersteller bereitstellt, wird der Signaturbegrenzungszähler auf den Wert „1“ gesetzt, d.h. nach jeder Signaturberechnung ist eine erneute Verifikation der Signatur-PIN erforderlich. Der Wert des Signaturzählers kann aber grundsätzlich durch den Personalisierer (Kartenhersteller) modifiziert werden (vgl. Kapitel 3.2, Anforderungen an den Personalisierer).

Mit Außerbetriebnahme der *eSign-Anwendung* kann der Signaturschlüssel „terminiert“ werden. Voraussetzung für die Terminierung hierzu ist eine erfolgreiche Benutzerauthentisierung mit der Karten-PIN. Nach dem Terminieren kann keine qualifizierte Signatur erzeugt werden.

Die Durchführung von Administrationsfunktionen für eine Signatur-PIN ist bei kontaktloser Kommunikation an die erfolgreiche Ausführung des PACE Protokolls gebunden. Der jeweilige Parameter, der durch den Karteninhaber für das PACE Protokoll einzugeben ist, ist abhängig von der durchzuführenden Administrationsfunktion (siehe Sicherheitsfunktion „Password Authenticated Connection Establishment (PACE) Protokoll“).

„Benutzerauthentisierung mit der Karten-PIN“

Die Sicherheitsfunktion beinhaltet die PIN-basierte Benutzerauthentifikation des Karteninhabers. Sie steht erst nach der erfolgreichen Initialisierung und Personalisierung zur Verfügung. Die Authentisierung des Karteninhabers mit der Karten-PIN erfolgt durch die Eingabe der korrekten Karten-PIN durch den Karteninhaber. Zur Durchführung der Operationen in der Karte ist die Karten-PIN im MF der Karte nicht auslesbar gespeichert.

Die Karten-PIN dient zur Aktivierung der Authentisierungsfunktion der „Sig Karte“. Sie dient insbesondere auch als Sicherheitsmerkmal für Administrationsfunktionen der *eSign-Anwendung* (z.B. Außerbetriebnahme der *eSign-Anwendung*).

Nach erfolgreicher Personalisierung enthält die „Sig Karte“ – abhängig vom Personalisierungsmodell - für die Karten-PIN entweder eine fünfstellige Transport-PIN oder keinen Referenzwert. Die Transport-PIN berechtigt den Karteninhaber ausschließlich zum Setzen seiner durch ihn gewählten mindestens sechsstelligen Karten-PIN. D.h. vor der erstmaligen Administration der *eSign-Anwendung* muss die Transport-PIN in eine Karten-PIN geändert werden. Hierzu muss sich der Karteninhaber durch eine erfolgreiche Eingabe der Transport-PIN gegenüber der „Sig Karte“ authentisieren. Nach Setzen der Karten-PIN kann die Transport-PIN nicht mehr verwendet werden. Die Benutzerauthentisierung mit der Transport-PIN ermöglicht keine Terminalauthentisierung.

Die Karten-PIN besitzt einen Fehlbedienungszähler (FBZ). Nach einer Anzahl von aufeinanderfolgenden Fehlversuchen wird die Karten-PIN blockiert. In diesem Zustand kann eine erneute Eingabe der Karten-PIN nur erfolgen, falls vorher eine erfolgreiche Eingabe der Karten-PIN2 erfolgt ist (Zustand „unblock – reset retry counter“).

Der Fehlbedienungszähler wird bei der Initialisierung auf 3 gesetzt. Hierdurch wird sichergestellt, dass maximal 3 aufeinanderfolgende Versuche zum Erraten der Karten-PIN durchgeführt werden können.

Die Karten-PIN (Karten-PIN2) kann durch den Karteninhaber geändert werden. Hierzu muss er sich durch die erfolgreiche Eingabe der aktuellen Karten-PIN (Karten-PIN2) gegenüber der „Sig Karte“ authentisieren, d.h. das Ändern der Karten-PIN (Karten-PIN2) in eine neue Karten-PIN (Karten-PIN2) ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der aktuellen Karten-PIN (Karten-PIN2) möglich.

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

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

„Speicheraufbereitung“

Die „Sig Karte“ 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 „Sig Karte“ 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 „Sig Karte“ die Session. In Abhängigkeit des Fehlers ist die „Sig Karte“ entweder blockiert oder kann nach Ausführung eines Resets in weiteren Sessions genutzt werden.

„Resistenz gegen Seitenkanalangriffe“

Die „Sig Karte“ 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 „Sig Karte“, 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 „Sig Karte“ aktiv.

„Selbsttest“

Die „Sig Karte“ 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 „Sig Karte“ stellt die kryptographischen Funktionen zur Verfügung. Sie stützt sich auf die kryptographischen Funktionen des evaluierten und zertifizierten Halbleiters und seiner dedizierten Software ab.

Die „Sig Karte“ unterstützt die in Kapitel 3.3 gelisteten Algorithmen.

„Erzeugung von ECDSA-Schlüsselpaaren“

Die „Sig Karte“ unterstützt eine karteninterne Erzeugung von ECDSA-Schlüsselpaaren zur Erzeugung von qualifizierten Signaturen mit einer Länge von 256, 320, 384 und 512 Bit.

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

- Es werden Schlüssel für das ECDSA Verfahren auf Basis von E(Fp) mit einer Schlüssellänge von 256, 320, 384 und 512 Bit generiert.

- Die Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2012], Kapitel 3.2.a) DSA-Varianten basierend auf Gruppen E(Fp).
- Zur Schlüsselerzeugung wird der Zufallszahlengenerator der zugrundeliegenden Hardware von Infineon verwendet.
- Die Schlüsselerzeugung stellt sicher, dass der Signaturschlüssel nicht aus dem Signaturprüfschlüssel ableitbar ist.
- Nach der Schlüsselgenerierung verifiziert die „Sig Karte“, ob der Signaturschlüssel und der Signaturprüfschlüssel zusammenpassen. Es werden nur gültige Schlüsselpaare zugelassen.
- Ein Import von ECDSA-Schlüsselpaaren 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 ist nur möglich, sofern sich der ZDA gegenüber der „Sig Karte“ authentisiert hat und seine zur Schlüsselerzeugung erforderlichen Zugriffsrechte nachgewiesen hat. In diesem Fall hat das Sicherheitsattribut SCD / SVD Management den Wert „authorised“. Das Kartenkommando zur Schlüsselgenerierung (GENERATE ASYMMETRIC KEY PAIR) wird nur unter einem sicheren Kanal (Aufbau nach Terminal- und Chipauthentisierung) ausgeführt, an den die Zugriffsrechte, die in der Terminalauthentisierung nachgewiesen wurden, gebunden werden.

Die Erzeugung des Signaturschlüssels erfolgt ausschließlich kartenintern während der Aktivierung der *eSign-Anwendung*. Dabei werden durch die „Sig Karte“ die genannten Sicherheitsanforderungen zur Erzeugung von ECDSA-Schlüsselpaaren eingehalten.

Bei einer nicht personalisierten „Sig Karte“ kann das Kommando GENERATE ASYMMETRIC KEY PAIR zur Erzeugung des Schlüsselpaars nur durch einen autorisierten ZDA über den mittels einer Authentisierung (Terminal- und Chipauthentisierung) aufgebauten sicheren Kanal zwischen ZDA und „Sig Karte“ aufgerufen werden.

Im Rahmen der Initialisierung der „Sig Karte“ werden Parameter elliptischer Kurven in die Karte geladen. Die Guidance Dokumente [TCOSADM] und [TCOSOPG] listen die zugelassenen Kurven auf. Mit dem Kommando zur Schlüsselgenerierung wird die Schlüssellänge nicht direkt durch den ZDA vorgegeben, sondern es wird eine elliptische Kurve ausgewählt, auf deren Basis die Schlüsselgenerierung erfolgt. Damit ist implizit auch die Länge des Schlüssels definiert, da die Kurvenparameter in der Karte hinterlegt sind. Somit können ausschließlich solche Kurven bzw. Schlüssellängen zum Einsatz kommen, deren Parameter entweder bereits in der Karte gespeichert sind oder mit dem Kommando GENERATE ASYMMETRIC KEY PAIR an die Karte übergeben werden.

Bei der Schlüsselgenerierung muss der ZDA sicherstellen, dass eine Kurve bzw. eine Schlüssellänge gewählt wird, deren Eignung zum Zeitpunkt der Schlüsselerzeugung bis Ende der Laufzeit des qualifizierten Signaturschlüsselzertifikats gegeben ist. Hierzu ist jeweils der aktuelle Algorithmenkatalog (Algorithmenkatalog 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) heranzuziehen.

Der Signaturschlüsselinhaber muss den Prozess zur Schlüsselgenerierung durch eine erfolgreiche Benutzerauthentisierung mit der Karten-PIN autorisieren.

„Erzeugung von qualifizierten Signaturen“

Die „Sig Karte“ unterstützt die Erzeugung von qualifizierten elektronischen Signaturen mit dem ECDSA Signaturschlüssel mit einer Schlüssellänge von 256, 320, 384 und 512 Bit. Die Sicherheitsfunktion hat die folgenden Eigenschaften:

- Empfang von (bereits gehashten) Daten (Data to be signed, DTBS) zur Erzeugung von qualifizierten elektronischen Signaturen.
- Berechnungen von ECDSA Signaturen gemäß [TR-03111] mit einer Schlüssellänge von 256, 320, 384 und 512 Bit.
- Zur Erzeugung von Zufallszahlen für die Generierung von ECDSA Signaturen wird der Zufallszahlengenerator der zugrundeliegenden Hardware von Infineon 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 einer Signatur-PIN (Kommando VERIFY) stattgefunden und das Sicherheitsattribut „SCD operational“ des Datenobjekts SCD den Wert „yes“ hat.
- Bei Anwendung über die kontaktlose Schnittstelle muss das Kartenkommando zur Erzeugung einer qualifizierten Signatur (PSO : Compute Digital Signature) unter einem sicheren Kanal (Aufbau nach PACE, optional Terminal- und Chipauthentisierung) an die Karte gesendet 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** 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 T-Systems International 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 [TCOSADM] und [TCOSOPG] 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 sollte.

Anforderungen an den Personalisierer

- Der Kartenhersteller muss sicherstellen, dass die Personalisierungsdaten (insbesondere der *eSign-Anwendung*) in einer sicheren Art und Weise behandelt werden. Die Personalisierungsdaten müssen hinsichtlich Integrität, Authentizität und Vertraulichkeit geschützt werden.
- Der Kartenhersteller muss sicherstellen, dass kryptographische Schlüssel, die zur Sicherung der Personalisierungsdaten eingesetzt werden, sicher behandelt werden.
- Die Vorgaben des Kartenherstellers an die Personalisierung gemäß [TCOSADM] und [TCOSOPG] sind zu berücksichtigen.
- Für die Personalisierung von Parametern für die Datenobjekte Signatur-PIN und Signatur-PIN2 sind die Angaben gemäß [TCOSADM] und [TCOSOPG] zu berücksichtigen. Insbesondere darf die Mindestlänge *m* der Signatur-PIN den Wert sechs nicht unterschreiten. Weiterhin darf der FBZ der Signatur-PIN maximal mit dem Wert m/2 (abgerundet) personalisiert werden und den Wert 20 nicht überschreiten. Die Mindestlänge der Signatur-PIN2 muss größer oder gleich 8 sein. Die vom Kartenhersteller eingestellten Defaultwerte erfüllen bereits diese Anforderungen.
- Der vom Kartenhersteller mit dem Wert eins eingestellte Signaturbegrenzungszähler darf während der Personalisierung nur unter Beachtung der Einsatzbedingungen an die Nutzung des Signaturzählers verändert werden.

Anforderungen an den Zertifizierungsdiensteanbieter

- Die eingesetzte Zertifizierungskomponente (Anwendung) zur Erzeugung von qualifizierten Zertifikaten (Certificate Generation Application, CGA) sollte die Sicherheitsanforderungen des Protection Profiles Secure Signature-Creation Device, [PP SSCD Part 2], Kapitel 5.3.1 erfüllen.
- Der ZDA muss den Prozess zur Aktivierung der *eSign-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 – hier „Sig Karte“ – 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.

- Der ZDA muss sicherstellen, dass die Eignung der durch ihn implizit ausgewählten Schlüssellänge zum Zeitpunkt der Schlüsselerzeugung bis Ende der Laufzeit des qualifizierten Signaturschlüsselzertifikats gegeben ist. Hierzu ist jeweils der aktuelle Algorithmenkatalog (Algorithmenkatalog 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) heranzuziehen.
- Programme, die ein ZDA seinen Kunden i.S.v. § 5 Abs. 1 Satz 2 [SigV] zur Übertragung von Referenzdaten auf die „Sig Karte“ zur Verfügung stellt (d.h. mit denen der Signaturschlüsselinhaber seine Karten-PIN bzw. 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 einer Signatur-PIN einen Kartenleser mit sicherer PIN-Eingabe (d.h. mind. Klasse 2) und einer sicheren Signaturanwendungskomponente verwenden.
- Der Signaturschlüsselinhaber muss – abhängig vom Personalisierungsmodell - verifizieren, dass die fünfstellige Transport-PIN noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte Signatur-PIN setzt, die über eine Länge von mindestens 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 gewählten Signatur-PINs vertraulich behandeln. Der Signaturschlüsselinhaber darf eine Signatur-PIN niemandem anvertrauen und muss sie sicher verwahren.
- Der Signaturschlüsselinhaber muss seine Signatur-PIN in regelmäßigen Abständen ändern.

- Der Signaturschlüsselinhaber muss bei Nutzung der Signatur-PIN2 beide Signatur-PINs verschieden wählen.
- Der Signaturschlüsselinhaber muss die „Sig Karte“ so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Zur Erzeugung von qualifizierten Signaturen verwendet der Signaturschlüsselinhaber die „Sig Karte“ nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

Anforderungen an Hersteller von Signaturanwendungskomponenten

- Der Hersteller einer Signaturanwendungskomponente muss die Schnittstellen des Betriebssystems TCOS sowie der *eSign-Anwendung* (vgl. [TCOSADM] und [TCOSOPG]) 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 des Protection Profiles Secure Signature-Creation Device [PP SSCD Part 2], Kapitel 5.3.2 berücksichtigen.

3.3 Algorithmen und zugehörige Parameter

Die „Sig Karte“ stellt das ECDSA-Verfahren basierend auf Gruppen E(F_p) zur Erstellung von elektronischen Signaturen gemäß [TR-03111] bereit. Es werden Schlüssellängen von 256, 320, 384 und 512 Bit unterstützt. Dabei erfolgt die Signaturerzeugung mit einer ausschließlich externen Hashwertberechnung.

Zur Erzeugung von Zufallszahlen wird in der „Sig Karte“ der durch die Hardware von Infineon zur Verfügung gestellte Zufallszahlengenerator verwendet. Der Zufallszahlengenerator der zugrundeliegenden Hardware ist ein P2-Generator mit SOF „hoch“ im Sinne der [AIS 31]. Die Zufallszahlen werden im laufenden Betrieb statistischen Tests unterzogen („Onlinetests“).

Die verwendeten kryptographischen Algorithmen sind gemäß dem Algorithmenkatalog der Bundesnetzagentur [Alg_Kat 2012] als geeignet eingestuft.

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

Tabelle 4: Mindest-Schlüssellängen für das ECDSA-Verfahren basierend auf Gruppen E(F_p)

Parameter \ Zeitraum	Bis Ende 2015	Bis Ende 2018
p	Keine Einschränkung	Keine Einschränkung
q	224 Bit	250 Bit

Diese Bestätigung der „Sig Karte“ ist somit maximal gültig bis **31.12.2018**. 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 TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P wurde erfolgreich nach den Common Criteria (CC) Version 3.1 mit der Prüfstufe **EAL 4+** (EAL 4 mit den Augmentierungen AVA_VAN.5) evaluiert.

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

Die Evaluierung wurde in Form einer sogenannten „Composition Evaluation“ durchgeführt, die die Evaluierungsergebnisse der CC Evaluierung des Halbleiters SLE78CLX1440P des Herstellers Infineon Technologies AG berücksichtigt. Diese Evaluierung erfolgte mit der Prüfstufe **EAL 5+** (EAL 5 mit den Augmentierungen ALC_DVS.2, AVA_VAN.5). Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential.

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0640-2010 vom 28. Juli 2010 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 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 17. Dezember 2009 (BGBl. I S. 3932).

[Alg_Kat 2012] 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, 30. Dezember 2011, veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243

[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-0035] Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0035-2007

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P Version 1.0, 13.09.2012, SRC.00016.TE.11.2012

[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

[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

[HW ST] Security Target of the underlying hardware platform Security Target M7820 A11, Version 0.7, Infineon Technologies AG, Chipcard and Security, Evaluation Documentation, 2010-08-11

[PP SSCD Part 2] CEN/TC 224 prEN 14169-1:2009: Protection profiles for Secure signature generation devices, Version 1.03, December 11th 2009, Zertifiziert durch das Bundesamt für Sicherheit in der Informationstechnik unter BSI-CC-PP-0059

[RFC 5639] M. Lochter, Johannes Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, Internet Engineering Task Force (IETF), 2010-03

[SPUB 800-38B] NIST: Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[ST] Specification of the Security Target TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P, T-Systems International GmbH, Version 2.0.1, 14.09.2012

[TCOSADM] TCOS 3.0 Signature Card Version 2.0 Release 1, Administrator's Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0, Version 0.1, 02.07.2012

[TCOSOPG] Operational Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0 Release 1 with the application Netkey, 1.0, 21.09.2012

[TR-03110] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, 24. März 2010

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

Ende der Bestätigung