

Bestätigung

von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 S. 1 Gesetz über Rahmenbedingungen für elektronische Signaturen¹ und § 11 Abs. 3 Signaturverordnung²

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 Residence Permit Card Version 1.1
Release 1/SLE78CLX1440P“**

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

SRC.00019.TE.11.2013

Bonn, den 22.11.2013

Detlef Kraus Thomas Hueske



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

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

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 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 Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P der T-Systems International GmbH.

Das Produkt wird durch den Hersteller in der Produktvariante TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P vertrieben. Das Produkt ist eine Signaturkarte und wird im Folgenden kurz als „eAT 1.1 Karte“ bezeichnet.

1.2 Auslieferung

Die „eAT 1.1 Karte“ ist realisiert als sogenannte Contactless Karte, d.h. die Karte verfügt nur über eine kontaktlose Schnittstelle. Die Hardware der „eAT 1.1 Karte“ besteht aus dem IFX Secure Smart Card Controller SLE78CLX1440P. Die Software besteht aus dem Betriebssystem TCOS Residence Permit Card Version 1.1 Release 1 (ROM, ggf. teilweise im EEPROM), sowie den dedizierten Anwendungen *ePassport-Anwendung*, *eID-Anwendung* und der *eSign-Anwendung* als Anwendung für die qualifizierte elektronische Signatur. Die *ePassport-Anwendung* und die *eID-Anwendung* sind **nicht** Gegenstand der vorliegenden Bestätigung.

Die Aktivierung der *eSign-Anwendung* (mit Schlüsselgenerierung und Einbringung des Signaturschlüsselzertifikats) durch den autorisierten Zertifizierungsdiensteanbieter (ZDA) setzt jedoch die Verwendung der *eID-Anwendung* voraus. Nach Authentisierung des ZDA hat dieser unter Einhaltung seiner Zugriffsrechte Zugriff auf Daten der *eID-Anwendung*. Diese können zur elektronischen Identifizierung des Antragstellers aus der „eAT 1.1 Karte“ ausgelesen werden.

Die sichere Signaturerstellungseinheit „eAT 1.1 Karte“ ist ein hoheitliches Ausweisdokument, deren Produktion und Auslieferung bis an den Endkunden, dem designierten Ausweisinhaber, über die Anforderungen des Signaturgesetzes hinaus spezifischen Gegebenheiten unterliegt. Die durch den Kartenhersteller produzierte kontaktlose Karte (Inlay) wird auf sicherem Wege vom Kartenhersteller an den autorisierten Ausweishersteller (Bundesdruckerei) ausgeliefert. Sie enthält insbesondere das Betriebssystem sowie die IC Identification Data.

Beim Ausweishersteller wird die „eAT 1.1 Karte“ initialisiert und personalisiert. Nach Fertigstellung des Aufenthaltstitels liefert der Ausweishersteller die „eAT 1.1 Karte“ an die Ausweisbehörde, die die „eAT 1.1 Karte“ an den designierten Ausweisinhaber ausgibt. Die Ausstellung des Ausweises unterliegt den gesetzlichen Vorgaben des Aufenthaltsgesetzes [AufenthG].

Während der Initialisierung und Personalisierung der „eAT 1.1 Karte“ werden durch den Ausweishersteller mindestens die folgenden Daten eingebracht:

- Master File (MF), u.a. mit folgenden Daten
 - einem signierten Chipauthentisierungsschlüssel

- Authentisierungsdaten des Ausweisinhabers (Card Access Number (CAN); Transport-eID-PIN, PUK)
- Vollständige *eID-Anwendung*
- Vollständige *ePassport-Anwendung*
- Vollständige *eSign-Anwendung* ohne Signaturschlüsselpaar und ohne Signatur-PIN

Nach Initialisierung und Personalisierung besitzt die „eAT 1.1 Karte“ weder einen Signaturschlüssel noch die zugehörige Signatur-PIN. Die Aktivierung der *eSign-Anwendung* erfolgt unter Kontrolle des zertifikatsausstellenden Zertifizierungsdiensteanbieters (ZDA). Erst in diesem Prozess wird in der „eAT 1.1 Karte“ das Signaturschlüsselpaar erzeugt. Voraussetzung hierzu ist, dass der designierte Signaturschlüsselinhaber die Signatur-PIN gesetzt hat. Erst dann kann die *eSign-Anwendung* zur Erzeugung von qualifizierten Signaturen genutzt werden.

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

Für die bestätigte Version der TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P sind in [TCOSADM], Anhang D die herstellereigenen Werte zu den Parametern „Chip Manufacturer (IFX)“, „Chip Type“, „Card Type (TCOS Residence Permit Card)“, „OS Version (ROM Mask Version)“, „(Pre-)Completion Code Version“, „File System Version“ und „Authentication Key Identifier“ 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 / Software	IFX Secure Smart Card Controller SLE78CLX1440P Package Type E-PIBD3-6-3 (inkl. IC dedicated Test Software)			--
2	Software (Betriebssystem)	IC Embedded Software (Betriebssystem) TCOS Residence Permit Card Version 1.1 Release 1 (implementiert im ROM/EEPROM des Halbleiters)			--
3	Software (Anwendungssoftware einschließlich Filesystem)	ePassport eID and (activated resp. not activated) eSign Applications implemented by File System Version '01' with the File System Version-ID '81'			--
4	Dokumentation	TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P, Administrator's Guidance, T-Systems International GmbH, [TCOSADM]	1.1	30.07.2013	Dokument in elektronischer Form
5	Dokumentation	TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P, Operational Guidance, T-Systems International GmbH, [TCOSOPG]	1.1	30.07.2013	Dokument in elektronischer Form

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 Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P“ ist vorgesehen für den Einsatz als elektronischer Aufenthaltstitel. Aus technischer Sicht ist die „eAT 1.1 Karte“ als kontaktlose Chipkarte mit einem proprietären Betriebssystem und einer Anwendungsebene, die direkt auf der Betriebssystemebene aufsetzt, realisiert.

Die „eAT 1.1 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-0813-2012 zertifiziert.

Die Software besteht aus dem Betriebssystem TCOS Residence Permit Card Version 1.1 Release 1 (ROM, ggf. teilweise im EEPROM) sowie aus der *eSign-Anwendung* zur Erzeugung qualifizierter elektronischer Signaturen.

Die „eAT 1.1 Karte“ besteht aus den folgenden Komponenten:

- Halbleiter (IC) von IFX (SLE78CLX1440P) mit proprietärer dedizierter Software,
- TCOS Betriebssystem „TCOS Residence Permit Card Version 1.1 Release 1“ und
- den Anwendungen
 - *ePassport-Anwendung*,
 - *eID-Anwendung* und
 - *eSign-Anwendung*.

Nach Ausgabe der „eAT 1.1 Karte“ besitzt die *eSign-Anwendung* weder ein Signaturschlüsselpaar noch eine Signatur-PIN. Die „eAT 1.1 Karte“ kann durch den Inhaber des Ausweises unter Kontrolle des zertifikatsausstellenden Zertifizierungsdiensteanbieters als sichere Signaturerstellungseinheit aktiviert werden. Hierzu ist an einem Signaturterminal³ 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 unter einem sicheren Kanal zwischen ZDA und „eAT 1.1 Karte“ die Schlüsselgenerierung in der Karte initiiert und der öffentliche Signaturprüfchlüssel aus der Karte ausgelesen. Der ZDA darf das qualifizierte Zertifikat erst dann ausstellen, wenn er sich davon überzeugt hat, dass sich die „eAT 1.1 Karte“ unter der Kontrolle des Signaturschlüsselinhabers steht. Das durch den ZDA erzeugte qualifizierte Signaturschlüsselzertifikat kann anschließend mit Nutzung des sicheren Kanals geschützt in die Karte eingebracht werden.

³ Dies kann entweder ein Standard-Chipkartenleser (Cat-S) oder ein Komfort-Chipkartenleser (Cat-K) sein. Gemäß [TR-03119] ist die Unterstützung der *eSign-Anwendung* durch einen Komfort-Chipkartenleser obligatorisch. Für einen Standard-Chipkartenleser sind diese Anforderungen optional.

Der sichere Kanal sichert sowohl die Vertraulichkeit als auch die Authentizität der kommunizierten Daten (Secure Messaging). Die „eAT 1.1 Karte“ unterstützt als Ausweisdokument auch das BAC Protokoll, auf welches in dieser Bestätigung jedoch nicht näher eingegangen wird, da es nicht im Rahmen der Signaturanwendung verwendet wird.

Nach Aktivierung der *eSign-Anwendung* kann die „eAT 1.1 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 *eSign-Anwendung* kann durch den Signaturschlüsselinhaber administriert werden. Hierzu gehören die folgenden Funktionen:

- Wechsel der Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der aktuell gültigen Signatur-PIN),
- Rücksetzen des Fehlbedienungs Zählers der Signatur-PIN ohne Setzen einer neuen Signatur-PIN (nach erfolgreicher Benutzerauthentisierung mit der PUK) und
- Außerbetriebnahme der Signaturfunktion mit Terminieren der Signatur-PIN und des Signaturschlüssels. In diesem Fall muss zuerst die Signatur-PIN und dann der Signaturschlüssel terminiert werden. Die Außerbetriebnahme setzt eine erfolgreiche Benutzauthentisierung mit der eID-PIN voraus.

Nach einer Außerbetriebnahme kann die *eSign-Anwendung* erneut aktiviert werden, d.h. es kann eine neue Signatur-PIN und 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 ersten Initialaktivierung.

Alle für die Signaturanwendung relevanten Zugriffe auf die kontaktlose „eAT 1.1 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, Terminal- und Chipauthentisierung 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. Der ZDA verwendet für seine Zugriffe ein Authentisierungsterminal (vgl. [TR-03117]),
- eines Signaturterminals zur Erstellung von qualifizierten elektronischen Signaturen sowie zum Management der Signatur-PIN.

Die Sicherheitseigenschaften der „eAT 1.1 Karte“ werden mit der Beschreibung der Sicherheitsfunktionen weiter erläutert.

Das TCOS 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 (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 „eAT 1.1 Karte“ nicht unterstützt.

Zur Erzeugung von Signaturschlüsselpaaren sowie von qualifizierten elektronischen Signaturen werden durch die „eAT 1.1 Karte“ die folgenden kryptographischen Algorithmen unterstützt:

- DSA auf Basis elliptischer Kurven (ECDSA) basierend auf Gruppen $E(F_p)$ (vgl. [TR-03111]) mit einer Schlüssellänge von 224, 256, 320, 384 und 512 Bit sowie
- Zufallszahlenerzeugung auf Basis des Zufallszahlengenerators (RNG) der zugrundeliegenden Hardware von Infineon. Dieser 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 geprüft (vgl. [HW ST]).

Die „eAT 1.1 Karte“ unterstützt die standardisierten Domain Parameter gemäß [TR-03116-2], Kapitel 1.3.2 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 nicht zur Anwendung und sind daher **nicht** Gegenstand dieser Bestätigung.

- Hashfunktionen SHA-1, SHA-224 und SHA-256 gemäß [FIPS 180-2] zur Ableitung von symmetrischen Sessionkeys,
- Diffie-Hellman auf Basis elliptischer Kurven (ECDH) gemäß [TR-03111] mit einer Schlüssellänge von 112, 128, 192 oder 256 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. [SP800-38B].
- Symmetrischer TDEA Algorithmus gemäß [FIPS^o46-3] mit einer effektiven Schlüssellänge von 112 Bit. Zur Verschlüsselung der kommunizierten Daten wird der CBC Modus eingesetzt. Zur Sicherung der Datenintegrität wird der „Retail-MAC“ verwendet, vgl. [ISO^o9797].

Die „eAT 1.1 Karte“ wurde auf Basis der Common Criteria in der Version 3.1 sowie des Protection Profiles [BSI-CC-PP-0069] für den elektronisch Aufenthaltstitels erfolgreich evaluiert (vgl. [ETR]). Die Zertifizierung des Produktes erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem Sicherheitszertifikat BSI-DSZ-CC-0835. Die Prüftiefe beträgt EAL 4+ mit den Augmentierungen AVA_VAN.5, ATE_DPT.2 und ALC_DVS.2.

Weiterhin berücksichtigt die „eAT 1.1 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 „eAT 1.1 Karte“

Die „eAT 1.1 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 „eAT 1.1 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 authentifizierte 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 unter Anwendung eines Authentisierungsterminals gegenüber der Karte authentisieren (Terminalauthentisierung) und seine in einem CV-Zertifikat gekennzeichneten Zugriffsrechte gegenüber der Karte nachweisen.

Ein Anwender authentisiert sich gegenüber der „eAT 1.1 Karte“ durch Eingabe der Signatur-PIN als Signierer.

Alle für die Signaturanwendung relevanten Zugriffe auf die kontaktlose „eAT 1.1 Karte“ müssen an einem Signaturterminal erfolgen. Zur gegenseitigen Authentisierung und zum Aufbau eines sicheren Kommunikationskanals zwischen Terminal und „eAT 1.1 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 einer qualifizierten Signatur).
- **Chipauthentisierung** zur Authentisierung des Chips gegenüber dem Terminal sowie Aufbau eines sicheren Kanals zur verschlüsselten und integritätsgesicherten Kommunikation zwischen Karte und Terminal.

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

Diese Vorgehensweise ist insbesondere bei den Zugriffen eines ZDA zur Schlüsselerzeugung und Einbringung des qualifizierten Zertifikates erforderlich. In diesem Fall wird durch das PACE Protokoll zunächst die lokale Luftschnittstelle zwischen Signaturterminal und „eAT 1.1 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. Hierdurch kann eine Ende-zu-Ende Sicherheit zwischen ZDA und Chip realisiert werden. Der ZDA nutzt hierzu sein sogenanntes Authentisierungsterminal zur Kommunikation über das Signaturterminal zur „eAT 1.1 Karte“.

Die „eAT 1.1 Karte“ ermöglicht dem ZDA den Zugriff auf Daten der *eID-Anwendung*. Hierzu muss sich der ZDA authentisieren (Terminalauthentisierung) und nachweisen, dass er über die erforderlichen Zugriffsrechte verfügt. Diese sind in einem CV-Zertifikat zu seinem Authentifikationsschlüssel identifiziert. Die „eAT 1.1 Karte“ erlaubt den Zugriff auf Daten der *eID-Anwendung* gemäß diesen Zugriffsrechten, sofern eine erfolgreiche Authentisierung (PACE, Terminal- und Chipauthentisierung) stattgefunden hat. Der Zugriff muss unter dem mit der Chipauthentisierung aufgebauten sicheren Kanal erfolgen. Somit kann die Vertraulichkeit und Authentizität der ausgelesenen Ausweisinhaberdaten gewährleistet werden.

Weiterhin ist die Zugriffskontrolle realisiert unter Anwendung von Zugriffsbedingungen, die als Sicherheitsattribute in der „eAT 1.1 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:

- Zugriffe auf Funktionen und Daten der *eSign-Anwendung* können nur an einem Signaturterminal erfolgen, dass sich hierzu gegenüber der Karte authentisieren (PACE, Terminal- und Chipauthentisierung) und seine Zugriffsrechte nachweisen muss.
- 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“).
- Das Setzen der 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 es ist kein nutzbarer Signaturschlüssel auf der Karte vorhanden) der „eAT 1.1 Karte“ nach einer erfolgreichen Benutzerauthentisierung erfolgen (PACE mit eID-PIN und Authentisierung des Signaturterminals).
- Das Wechseln einer bestehenden Signatur-PIN in eine neue Signatur-PIN durch den Signaturschlüsselinhaber kann nur nach einer erfolgreichen Benutzerauthentisierung mit der alten Signatur-PIN erfolgen.
- Die PUK kann nur im Rahmen der Personalisierung gesetzt und nachträglich nicht mehr geändert werden.
- Die Außerbetriebnahme der Signaturfunktion setzt eine erfolgreiche Benutzerauthentisierung voraus (PACE mit eID-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 „operational“.

- Signaturen können nur durch den Signaturschlüsselinhaber generiert werden. Hierzu ist eine vorherige erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erforderlich.
- Sensitive Daten wie Signaturschlüssel, Signatur-PIN, PUK und eID-PIN können nicht über Kommandos des Betriebssystems ausgelesen werden.

„Password Authenticated Connection Establishment (PACE) Protokoll“

Die „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 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 ist die CAN auf der Vorderseite des Kartenkörpers aufgedruckt und damit kein Geheimnis für jeden, der physischen Zugriff auf die „eAT 1.1 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 „eAT 1.1 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)
 - Erzeugung von qualifizierten elektronischen Signaturen
 - Wechsel der Signatur-PIN
- eID-PIN
 - Erzeugung des Signaturschlüsselpaars unter Kontrolle des zertifikatsausstellenden ZDA
 - Setzen einer neuen Signatur-PIN
 - Löschen der Signatur-PIN
 - Löschen des Signaturschlüsselpaars
- PUK
 - Rücksetzen des Fehlbedienungszählers (FBZ) der Signatur-PIN ohne Setzen einer neuen Signatur-PIN

„Terminalauthentisierung“

Die „eAT 1.1 Karte“ unterstützt die Durchführung der Terminalauthentisierung. Dieses Protokoll wird zur Authentisierung des Terminals (Challenge-and-Response Protokoll) gegenüber der „eAT 1.1 Karte“ genutzt. Weiterhin erfolgt mit dem Protokoll der Nachweis der Zugriffsrechte des Signaturterminals gegenüber der „eAT 1.1 Karte“. Diese Rechte werden an den sicheren Kanal, der anschließend mit der Chipauthentisierung aufgebaut wird, gebunden.

Zur Authentisierung erzeugt das Terminal mit seinem privaten Schlüssel ein Authentisierungstoken über eine Zufallszahl der „eAT 1.1 Karte“ sowie über weitere Daten (z.B. Identität der „eAT 1.1 Karte“, ephemeralen öffentlichen Terminalschlüssel). Das Authentisierungstoken wird durch die „eAT 1.1 Karte“ mit dem öffentlichen Schlüssel des Terminals geprüft. Kryptographische Grundlage bildet das Verfahren ECDSA.

Die Authentizität der öffentlichen Terminalschlüssel wird durch CV-Zertifikate sichergestellt, die aus speziellen PKIs, den Extended Access Control (EAC) PKIs für elektronische Personalausweise, stammen. Diese CV-Zertifikate enthalten auch die Zugriffsrechte des Terminals, das sich mit diesem Zertifikat authentisiert. Für die Nutzung der „eAT 1.1 Karte“ sind die beiden EAC-PKIs für die *eID-Anwendung* und die *eSign-Anwendung* zu berücksichtigen. Die Authentisierung des ZDA zur Aktivierung der *eSign-Anwendung* erfolgt unter der EAC-PKI für *eID-Anwendung* (Authentisierungsterminal des ZDA). Alle anderen Zugriffe, die über ein Signaturterminal erfolgen, werden über die EAC-PKI der *eSign-Anwendung* authentisiert.

Die EAC-PKI der *eID-Anwendung* (für Zugriffe des ZDA) ist dreistufig und unterscheidet die folgenden Rollen

- Country Verifying CA (CVCA; Wurzelinstanz)
- Document Verifier (DV, CA der zweiten Ebene)
 - Official Domestic Document Verifier
 - Non-Official or foreign Document Verifier
- Authentisierungsterminal des ZDA

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

Die EAC-PKI der *eSign-Anwendung* (für alle anderen Zugriffe auf die *eSign-Anwendung*) ist ebenfalls dreistufig und unterscheidet insbesondere die folgenden Rollen

- Country Verifying CA (CVCA; Wurzelinstanz)
- Document Verifier (DV, CA der zweiten Ebene) für Terminals zur Erstellung qualifizierter elektronischer Signaturen
- Signaturterminal

Die Zugriffsrechte eines Signaturterminals zur Erstellung qualifizierter Signaturen beinhaltet das Recht zum Erstellen qualifizierter Signaturen sowie zur Verwaltung der Signatur-PIN. Dieses Recht autorisiert Zugriffe auf die *eSign-Anwendung* der „eAT 1.1 Karte“.

Die Gültigkeit der CV-Zertifikate ist durch die Angabe der Daten „Gültig-ab-Datum“ und „Gültig-bis-Datum“ begrenzt. Die „eAT 1.1 Karte“ speichert den öffentlichen Schlüssel der Wurzelinstanz (das CV-Zertifikat der CVCA) sowie das jüngste bekannte Gültig-ab-Datum eines gültigen Zertifikats zur Prüfung der CV-Zertifikate. Mit jeder Prüfung einer Zertifikatskette eines

Terminals wird ggf. das jüngste Gültig-ab-Datum aktualisiert. Hierdurch kann ein Fortschreiten der Zeit in der Karte nachgehalten und ein Zertifikat, dessen Gültigkeit bereits abgelaufen ist, durch die Karte identifiziert werden.

„Chipauthentisierung“

Die „eAT 1.1 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 ephemeral DH Schlüsselpaar des Terminals (aus der Terminalauthentisierung) sowie das statische DH Schlüsselpaar der „eAT 1.1 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 ephemeralen öffentlichen Terminalschlüssel aus der vorangegangenen Terminalauthentisierung. Somit wird eine gegenseitige Authentisierung von Terminal und Karte erreicht.

Zur Chipauthentisierung besitzt die „eAT 1.1 Karte“ einen Chipauthentisierungsschlüssel (statisches DH Schlüsselpaar). Der öffentliche Schlüssel wird in der „eAT 1.1 Karte“ in einer signierten Datenstruktur im EF.CardSecurity im MF der Karte gespeichert. Die Signatur wird durch den Ausweishersteller mit einem Schlüssel erzeugt, dessen Authentizität mit der spezifischen Dokumenten-PKI nachgewiesen wird.

Die Dokumenten-PKI verwendet X.509-Zertifikate und besteht aus den folgenden Zertifikaten bzw. Schlüssel:

- dem Country Signing Certification Authority Certificate (X.509-Zertifikat der Wurzelinstanz),
- dem Document Signer Certificate, das X.509-Zertifikat der Instanz, die den öffentlichen Schlüssel der „eAT 1.1 Karte“ signiert und
- dem öffentlichen Schlüssel der „eAT 1.1 Karte“, der im MF gespeichert und vom Document Signer signiert ist.

Der Ausweishersteller signiert nur öffentliche Schlüssel authentischer Aufenthaltstitel. 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 „eAT 1.1 Karte“ um eine evaluierte und bestätigte Signaturkarte handelt.

„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 „eAT 1.1 Karte“ (in der *eSign-Anwendung*) geheim gespeicherten Referenzwert (RAD).

Nach erfolgreicher Personalisierung enthält die „eAT 1.1 Karte“ keinen Referenzwert für die Signatur-PIN. Es ist kein Signaturschlüssel auf der Karte vorhanden und es kann insbesondere keine gültige qualifizierte Signatur erzeugt werden.

Die Signatur-PIN mit einer Mindestlänge von m Stellen (Defaultwert für die Mindestlänge ist sechs in Kapitel 9.2.11 von [TCOSADM]) ist vor der Aktivierung der *eSign-Anwendung* durch den designierten Signaturschlüsselhaber zu setzen (Kommando CHANGE REFERENCE DATA mit einer PIN). Dies muss an einem Signaturterminal, das über eine entsprechende Berechtigung verfügt, erfolgen. Voraussetzung für das Setzen der Signatur-PIN ist die erfolgreiche Benutzerauthentisierung mit eID-PIN (PACE Protokoll). Weiterhin kann die Signatur-PIN nur gesetzt werden, falls für das Datenobjekt SCD das Sicherheitsattribut „SCD operational“ den Wert „no“ hat, d.h. insbesondere, dass kein nutzbarer Signaturschlüssel auf der Karte vorhanden ist.

Die Signatur-PIN besitzt einen 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 „eAT 1.1 Karte“ 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 auf den Initialwert Sig_{ad} gesetzt, jedoch nur dann wenn die „eAT 1.1 Karte“ nicht blockiert ist. Der Initialwert Sig_{ad} wird im Rahmen der Initialisierung der Karte gesetzt und hat den Defaultwert drei siehe Kapitel 5.4.4 in [TCOSADM].

Mit einem (Neu-)Setzen der Signatur-PIN ist eine Reinitialisierung des FBZ verbunden. Weiterhin kann ein (Neu-)Setzen der Signatur-PIN nur erfolgen, falls die Signatur-PIN nicht blockiert ist.

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

Der FBZ der Signatur-PIN einer blockierten „eAT 1.1 Karte“ kann unter Anwendung eines globalen Resetting Codes (PUK) zurückgesetzt werden. Die „eAT 1.1 Karte“ unterstützt einen Resetting Code mit einer Länge von mindestens zehn Stellen (siehe Kapitel 5.1.3.3 in [TCOSADM]). Nach einer falschen Eingabe des Resetting Codes blockiert die „eAT 1.1 Karte“ die gesamte PACE-Authentisierungsprozedur und das gesamte Kommunikations-Protokoll muss nach einer Zeitspanne wiederholt werden.

Zum Zurücksetzen ist das Kommando RESET RETRY COUNTER zu verwenden (Kapitel 7.3.14 in [TCOSOPG]). Es erfolgt kein Setzen des Sicherheitszustandes der Signatur-PIN, d.h. das Zurücksetzen einer blockierten Karte ermöglicht nicht die Erzeugung einer qualifizierten Signatur.

Die Signatur-PIN kann durch den Signaturschlüsselinhaber geändert werden. Hierzu muss er sich durch die erfolgreiche Eingabe der aktuellen Signatur-PIN gegenüber der „eAT 1.1 Karte“ authentisieren, d.h. das Ändern der Signatur-PIN in eine neue Signatur-PIN ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der aktuellen Signatur-PIN möglich (Kommando CHANGE REFERENCE DATA mit alter und neuer PIN).

Nach einer erfolgreichen Eingabe der Signatur-PIN kann maximal eine Signatur erzeugt werden, d.h. vor jeder Erzeugung einer qualifizierten elektronischen Signatur ist die Signatur-PIN erfolgreich einzugeben. Dies wird durch die „eAT 1.1 Karte“ sichergestellt. Das Betriebssystem unterstützt einen Signaturbegrenzungszähler. Mit dem Filesystem, das der Kartenhersteller bereit stellt, 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 (Ausweishersteller) modifiziert werden (vgl. Kapitel 3.2, Anforderungen an den Personalisierer).

Mit Außerbetriebnahme der *eSign-Anwendung* kann die Signatur-PIN und das Signaturschlüsselpaar „terminiert“ werden. Voraussetzung für die Terminierung hierzu ist eine erfolgreiche Benutzerauthentisierung mit der eID-PIN (PACE Protokoll). Nach dem Terminieren der Signatur-PIN kann weder eine erfolgreiche Benutzerauthentisierung mit der Signatur-PIN erfolgen, noch kann eine qualifizierte Signatur erzeugt werden.

Die Eingabe der Signatur-PIN (zum Setzen bzw. Ändern der Signatur-PIN sowie zum Erzeugen von qualifizierten Signaturen) darf nur an einem Standard- oder Komfort-Chipkartenleser erfolgen.

Die PUK wird in die Karte personalisiert und kann nachträglich nicht mehr geändert werden. Die Übergabe der PUK an den designierten Signaturschlüsselinhaber erfolgt durch die Ausweisbehörde mittels eines hierzu geeigneten Mediums (z.B. PIN-Brief).

Die Durchführung von Administrationsfunktionen für die Signatur-PIN ist auch 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 eID-PIN“

Die Sicherheitsfunktion beinhaltet die PIN basierte Benutzerauthentifikation des Ausweisinhabers. Sie steht erst nach der erfolgreichen Initialisierung und Personalisierung zur Verfügung. Die Authentisierung des Ausweisinhabers mit der eID-PIN erfolgt durch die erfolgreiche Durchführung des PACE Protokolls mit Verwendung der eID-PIN. Hierzu ist die eID-PIN durch den Ausweisinhaber korrekt am Terminal einzugeben. Zur Durchführung der Operationen in der Karte ist die eID-PIN im MF der Karte nicht auslesbar gespeichert.

Die eID-PIN dient zur Aktivierung der Authentisierungsfunktion des Aufenthaltstitels. Sie dient insbesondere auch als Sicherheitsmerkmal für Administrationsfunktionen der *eSign-Anwendung* (z.B. Außerbetriebnahme der *eSign-Anwendung*).

Nach erfolgreicher Personalisierung enthält die „eAT 1.1 Karte“ eine fünfstellige Transport-eID-PIN. Diese berechtigt den Ausweisinhaber ausschließlich zum Setzen seiner durch ihn

gewählten sechsstelligen eID-PIN. D.h. vor der erstmaligen Administration der *eSign-Anwendung* muss die Transport-eID-PIN in eine echte eID-PIN geändert werden. Hierzu muss sich der Ausweisinhaber durch eine erfolgreiche Eingabe der Transport-eID-PIN gegenüber der „eAT 1.1 Karte“ authentisieren. Nach Setzen der eID-PIN kann die Transport-eID-PIN nicht mehr verwendet werden. Die Benutzerauthentisierung mit der Transport-eID-PIN ermöglicht keine Terminalauthentisierung und damit auch keinen Zugang zur *eSign-Anwendung*.

Die eID-PIN besitzt einen Fehlbedienungsähler (FBZ). Nach einer Anzahl von Suspend_{ad} aufeinanderfolgenden Fehlversuchen wird die eID-PIN suspendiert. In diesem Zustand kann eine erneute Eingabe der eID-PIN nur erfolgen, falls vorher eine erfolgreiche Eingabe der CAN erfolgt ist (Zustand „resume“ Absicherung gegen DoS-Angriffe). Nach einer weiteren Anzahl von Block_{ad} nacheinander erfolglosen Eingabeversuchen wird die Nutzung der eID-PIN blockiert und die Sperrung kann nur unter Anwendung einer globalen PUK wieder aufgehoben werden.

Die Parameter Suspend_{ad} und Block_{ad} werden im Rahmen der Initialisierung gesetzt und können mit Werten aus dem Bereich eins bis maximal sechs für Suspend_{ad} und eins bis maximal drei für Block_{ad} belegt werden. Hierdurch wird sichergestellt, dass maximal neun aufeinanderfolgende Versuche zum Erraten der eID-PIN durchgeführt werden können.

Eine blockierte eID-PIN kann nur unter Anwendung eines globalen Resetting Codes (PUK) zurückgesetzt werden.

Die eID-PIN kann durch den Ausweisinhaber geändert werden. Hierzu muss er sich durch die erfolgreiche Eingabe der aktuellen eID-PIN gegenüber der „eAT 1.1 Karte“ authentisieren, d.h. das Ändern der eID-PIN in eine neue eID-PIN ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der aktuellen eID-PIN möglich.

Das Setzen und Ändern der eID-PIN darf nur an einem Standard- oder Komfort-Chipkartenleser vorgenommen werden.

Die Transport-eID-PIN und die PUK werden in die Karte personalisiert. Die PUK kann anschließend nicht mehr geändert werden. Die Übergabe der Transport-eID-PIN sowie der PUK an den designierten Signaturschlüsselinhaber erfolgt durch die Ausweisbehörde mittels eines hierzu geeigneten Mediums (z.B. PIN-Brief).

Die „eAT 1.1 Karte“ unterstützt die Möglichkeit in einer Ausweisbehörde eine neue eID-PIN ohne Kenntnis der alten eID-PIN zu setzen (z.B. der Ausweisinhaber hat seine aktuelle eID-PIN vergessen). Das Recht, eine neue eID-PIN zu setzen, muss die Ausweisbehörde über die Terminalauthentisierung mit einem speziellen Zugriffsrecht nachweisen.

„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 Signaturprüf Schlüssel 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 „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 Karte“ die Session. In Abhängigkeit des Fehlers ist die „eAT 1.1 Karte“ entweder blockiert oder kann nach Ausführung eines Resets in weiteren Sessions genutzt werden.

„Resistenz gegen Seitenkanalangriffe“

Die „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 Karte“ aktiv.

„Selbsttest“

Die „eAT 1.1 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 „eAT 1.1 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 „eAT 1.1 Karte“ unterstützt die in Kapitel 3.3 gelisteten Algorithmen.

„Erzeugung von ECDSA-Schlüsselpaaren“

Die „eAT 1.1 Karte“ unterstützt eine karteninterne Erzeugung von ECDSA-Schlüsselpaaren zur Erzeugung von qualifizierten Signaturen mit einer Länge von 224, 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 $E(F_p)$ mit einer Schlüssellänge von 224, 256, 320, 384 und 512 Bit generiert.
- Die Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2013], Kapitel 3.2.a) DSA-Varianten basierend auf Gruppen $E(F_p)$.
- Zur Schlüsselerzeugung wird der Zufallszahlengenerator der zugrundeliegenden Hardware von Infineon verwendet.
- Die Schlüsselerzeugung stellt sicher, dass der Signaturschlüssel nicht aus dem Signaturprüf Schlüssel ableitbar ist.
- Nach der Schlüsselgenerierung verifiziert die „eAT 1.1 Karte“, ob der Signaturschlüssel und der Signaturprüf Schlüssel 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 „eAT 1.1 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 „eAT 1.1 Karte“ die genannten Sicherheitsanforderungen zur Erzeugung von ECDSA-Schlüsselpaaren eingehalten.

Das Kommando GENERATE ASYMMETRIC KEY PAIR zur Erzeugung des Schlüsselpaars kann nur durch einen authentisierten ZDA über den mittels einer Authentisierung (Terminal- und Chipauthentisierung) aufgebauten sicheren Kanal zwischen ZDA und „eAT 1.1 Karte“ aufgerufen werden.

Im Rahmen der Initialisierung der „eAT 1.1 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 bereits in der Karte gespeichert sind.

Der ZDA muss jedoch 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 ist an dem Prozess der Schlüsselgenerierung nicht beteiligt.

„Erzeugung von qualifizierten Signaturen“

Die „eAT 1.1 Karte“ unterstützt die Erzeugung von qualifizierten elektronischen Signaturen mit dem ECDSA Signaturschlüssel mit einer Schlüssellänge von 224, 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 224, 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 der Signatur-PIN (Kommando VERIFY) stattgefunden und das Sicherheitsattribut „SCD operational“ des Datenobjekts SCD den Wert „yes“ hat.
- Die Erzeugung qualifizierter Signaturen ist nur an einem Signaturterminal möglich, das sich gegenüber der „eAT 1.1 Karte“ als Signaturterminal authentisiert hat und sein zur Erzeugung qualifizierter Signaturen erforderliches Zugriffsrecht nachgewiesen hat. Das Kartenkommando zur Erzeugung einer qualifizierten Signatur (PSO : Compute Digital Signature) wird nur unter einem sicheren Kanal (Aufbau nach Terminal- und Chipauthentisierung) ausgeführt, an den die Zugriffsrechte, die in der Terminalauthentisierung nachgewiesen wurden, gebunden 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)	<p>Anforderung</p> <p>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.</p>
Abs. (3)	<p>Anforderung</p> <p>Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um</p>
Nr. 1	<p>bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ...</p>

Tabelle 3: Erfüllung der Anforderungen der Signaturverordnung

Referenz	Anforderung / Erläuterung / Ergebnis
§ 15	Anforderungen an Produkte für qualifizierte elektronische Signaturen
Abs. (1)	<p>Anforderung</p> <p>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</p>

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 Signaturprüf Schlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.
Abs. (4)	<p>Anforderung</p> <p>Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.</p>
<p>Anl. 1, I, 1.1</p> <p>b)</p>	<p>Anforderung</p> <p>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 - GMBI vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen.</p> <p>Die Prüfung muss</p> <p>bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen.</p>
<p>Anl. 1, I, 1.2</p>	<p>Anforderung</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Anl. 1, I, 1.3</p>	<p>Anforderung</p> <p>Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein.</p>

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.

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 PUK 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 PUK muss größer oder gleich 10 sein. Die vom Kartenhersteller eingestellten Defaultwerte erfüllen bereits diese Anforderungen.
- Der vom Kartenhersteller mit dem Wert eins eingestellte Signaturbegrenzungszähler darf während der Personalisierung nicht verändert werden.

Anforderungen an den Zertifizierungsdiensteanbieter

- Die eingesetzte Zertifizierungskomponente (Anwendung) zur Erzeugung von qualifizierten Zertifikaten (Signature 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 „eAT 1.1 Karte“ – besitzt und diese vollständig unter seiner alleinigen Kontrolle steht.
- Weiterhin ist im Sicherheitskonzept des ZDA zu beschreiben, wie die Identifizierung des Antragstellers mithilfe des elektronischen Identitätsnachweises gemäß § 78 des

Aufenthaltsgesetzes [AufenthG] durch den ZDA vorgenommen wird. Es sind zusätzliche (organisatorische) Sicherheitsmaßnahmen beim ZDA vorzusehen, die sicherstellen, dass der autorisierte Ausweisinhaber (dessen personenbezogene Daten in der *eID-Anwendung* der Karte personalisiert sind) auch im Besitz des Ausweises ist.

Die sichere Identifizierung muss beinhalten, dass der Antragsteller im Besitz **seiner** „eAT 1.1 Karte“ ist, d.h. dass die Zuordnung zwischen Karte und Person korrekt ist. Hierzu darf die Identifizierung nicht alleine auf der *eID-Anwendung* des Ausweises beruhen, vielmehr sind zusätzliche Sicherheitsmaßnahmen zu ergreifen, die eine korrekte Zuordnung zwischen Karte und Antragsteller sicherstellen.

- 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.

- Sofern es sich um einen akkreditierten ZDA handelt, unterliegt das Sicherheitskonzept einschließlich der zusätzlichen Bestandteile für den Prozess zur Aktivierung der *eSign-Anwendung* sowie zur Identifizierung mit dem elektronischen Identitätsnachweis gemäß § 78 des Aufenthaltsgesetzes ebenfalls einem Bestätigungsprozess.
- 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 „eAT 1.1 Karte“ zur Verfügung stellt (d.h. mit denen der Signaturschlüsselinhaber seine eID-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 Ausweisinhaber muss zum Ersetzen der Transport-eID-PIN in eine echte eID-PIN sowie zum Ändern der eID-PIN einen Chipkartenleser mit sicherer PIN-Eingabe (d.h. Cat-K oder mindestens Cat-S gemäß [TR-03119]) verwenden.
- Der Signaturschlüsselinhaber muss verifizieren, dass die fünfstellige Transport-PIN noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte PIN setzt, die über eine Länge von sechs Stellen verfügt. Ist die Transport-PIN nicht gültig oder hat diese nicht genau fünf Stellen, so muss sich der Karteninhaber mit der ausgebenden Kartenbehörde in Verbindung setzen.

- Der Ausweisinhaber muss zum Setzen und Ändern der Signatur-PIN ein Signaturterminal mit sicherer PIN-Eingabe (d.h. Cat-K oder mindestens Cat-S gemäß [TR-03119]) und einer sicheren Signaturanwendungskomponente verwenden.
- Der Signaturschlüsselinhaber muss die Transport-eID-PIN sowie die von ihm selbst gewählten PINs eID-PIN und Signatur-PIN vertraulich behandeln. Der Signaturschlüsselinhaber darf diese PINs niemanden anvertrauen und muss sie sicher verwahren.
- Der Signaturschlüsselinhaber muss seine eID-PIN und Signatur-PIN in regelmäßigen Abständen ändern.
- Der Signaturschlüsselinhaber muss die „eAT 1.1 Karte“ so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Zur Erzeugung von qualifizierten Signaturen verwendet der Signaturschlüsselinhaber die „eAT 1.1 Karte“ nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.
- Wenn möglich, sollte der Einsatz des elektronischen Ausweistitels grundsätzlich an einem Standard- oder Komfort-Chipkartenleser erfolgen, **jedenfalls** nur an vertrauenswürdigen Computersystemen.

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 „eAT 1.1 Karte“ stellt das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ zur Erstellung von elektronischen Signaturen gemäß [TR-03111] bereit. Es werden Schlüssellängen von 224, 256, 320, 384 und 512 Bit unterstützt. Dabei erfolgt die Signaturerzeugung mit einer ausschließlich externen Hashwertberechnung.

Zur Erzeugung von Zufallszahlen wird in der „eAT 1.1 Karte“ der durch die Hardware von Infineon zur Verfügung gestellte Zufallszahlengenerator verwendet. Der Zufallszahlengenerator der zugrundeliegenden Hardware ist ein PTG.2 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 2013] als geeignet eingestuft.

Für das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ 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 2019
p	Keine Einschränkung	Keine Einschränkung
q	224 Bit	250 Bit

Diese Bestätigung der „eAT 1.1 Karte“ ist somit maximal gültig bis **31.12.2019**. 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 Residence Permit Card Version 1.1 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, ATE_DPT.2 und ALC_DVS.2) evaluiert.

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

Hierfür liegt das deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0835 vom 31. Oktober 2013 vor.

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-0813-2012 vom Juni 2012 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).

[AufenthG]	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz – AufenthG) vom 19. August 2013 (BGBl. I S. 3484)
[EU-RPSpec]	EU – Residence Permit Specification, Annex II.a to Commission Decision C(2008), Version 1.0, 20.08.2008
[Alg_Kat 2013]	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001, veröffentlicht am 18. Februar 2013
[AIS 31]	AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013
[BSI-CC-PP-0069]	Protection Profile - CC Protection Profile: Electronic Residence Permit Card (RP_Card PP), Compliant to EU-Residence Permit Specification V 1.0, BSI-CC-PP-0069, Version 1.00, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2010-08-13
[ETR]	SRC, Evaluation Report, Evaluation Technical Report (ETR), TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P Version 1.2, 25.10.2013, BSI-DSZ-CC-0835
[FIPS 180-2]	NIST: FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 und Change Notice 1, Februar 2004.
[FIPS°46-3]	Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. DoC/NIST
[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]	Infineon Technologies AG, Chipcard and Security, M7820 A11 including optional Software Libraries RSA – EC – SHA-2 - Toolbox, Version 1.5, 07.05.2012
[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
[SP800-38B]	NIST: Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005
[ISO°9797]	ISO 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, ISO, 2005-01-04
[ST]	Specification of the Security Target TCOS Residence Permit Card Version 1.1 Release 1/SLE78CLX1440P, T-Systems International GmbH, Version 1.1.1/20130913, 13.09.2013

- [TCOSADM] TCOS Residence Permit Card 1.1 Release 1, Administrator's Guidance, Guidance Documentation of TCOS Residence Permit Card Version 1.1 with ePassport, eID and eSign Application, Version 1.1, 30.07.2013
- [TCOSOPG] TCOS Residence Permit Card 1.1 Release 1, Operational Guidance, Guidance Documentation of TCOS Residence Permit Card Version 1.1 with ePassport, eID and eSign Application, Version 1.1, 30.07.2013
- [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 2.10, 2012-03
- [TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 2.0, 2012-06
- [TR-03116-2] BSI: Technische Richtlinie TR-03116-2, eCard Projekte der Bundesregierung, Teil 2 - Hoheitliche Kartendokumente, Stand 2013
- [TR-03117] BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, Version 1.0, 2009
- [TR-03119] BSI: Technische Richtlinie TR-03119, Anforderungen an Chipkartenleser mit ePA Unterstützung, Version 1.3, 22.03.2013

Ende der Bestätigung