Bestätigung
von Produkten für qualifizierte elektronische Signaturen

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

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

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

Signaturerstellungseinheit
„STARCOS 3.5 ID GCC C1R“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

SRC.00014.TE.02.2012

Bonn, den 01.02.2012

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 15. November 2010 (BGBl. I S. 1542)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung des Produktes und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit STARCOS 3.5 ID GCC C1R der Giesecke & Devrient GmbH.

Das Produkt ist ein neuer (elektronischer) Personalausweis (nPA) und wird im Folgenden kurz als „nPA-Signaturkarte“ bezeichnet.

1.2 Auslieferung

Die „nPA-Signaturkarte“ ist realisiert als kontaktlose Chipkarte (Halbleiter) / Modul mit Smartcard Embedded Software (ROM Maske), bestehend aus dem STARCOS Betriebssystem in der Version 3.5 (STARCOS 3.5) 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 „nPA-Signaturkarte“ ausgelesen werden.

Die sichere Signaturerstellungseinheit „nPA-Signaturkarte“ ist ein hoheitliches Ausweisdokument, deren Produktion und Auslieferung bis an den Endkunden, dem designierten Ausweisinhaber, über die Anforderungen des Signaturgesetzes hinaus spezifischen Gegebenheiten unterliegt. Das Betriebssystem wird vom Kartenhersteller Giesecke & Devrient GmbH an den Hardware-Hersteller NXP geliefert. NXP übergibt die gefertigten Chips an verschiedene Inlay-Hersteller, die die produzierten Inlays an einen autorisierten Ausweishersteller (z.B. Bundesdruckerei) ausliefern. Alle Auslieferungsprozesse werden durch organisatorische Sicherheitsmaßnahmen geschützt.

Beim Ausweishersteller wird die „nPA-Signaturkarte“ initialisiert und personalisiert. Nach Fertigstellung des neuen Personalausweises liefert der Ausweishersteller die „nPA-Signaturkarte“ an die Ausweisbehörde, die die „nPA-Signaturkarte“ an den designierten Ausweisinhaber ausgibt. Die Ausstellung des Ausweises unterliegt den gesetzlichen Vorgaben des Personalausweisgesetzes [PAuswG].

Während der Initialisierung und Personalisierung der „nPA-Signaturkarte“ 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)
- *eSign-Anwendung* ohne Signaturschlüsselpaar und ohne Signatur-PIN

Nach Initialisierung und Personalisierung besitzt die „nPA-Signaturkarte“ weder einen Signaturschlüssel noch die zugehörige Signatur-PIN. Die Aktivierung der *eSign-Anwendung* erfolgt unter Kontrolle des zertifikatsausstellenden Zertifizierungsdiensteanbieter (ZDA) und des Ausweisinhabers. Erst in diesem Prozess wird in der „nPA-Signaturkarte“ 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 STARCOS 3.5 ID GCC C1R sind in [UG_Ini] die herstellerspezifischen Werte zu den Parametern „Chip Manufacturer Data“, „OS Manufacturer“, „OS Ver-sion number“ und „Version of ROM mask“ angegeben. Sie können während der Produktion mit dem Kommando „GET PROTOCOL DATA“ gemäß [UG_Ini], Kapitel 5.2.10 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	NXP Secure Smart Card Controllers P5CD128V0A Delivery Type A0 Module MOB6 (incl. IC dedicated Test Software) (Zertifizierung unter BSI-DSZ-CC-0645)			-
2	Software (Betriebs-system)	Smartcard Embedded Software (Betriebssystem) STARCOS 3.5 (implementiert im ROM/EEPROM des Halbleiters)			-
3	Software (Anwendungs software einschließlich Filesystem)	Smartcard Embedded Anwendungen (*ePassport*-, *eID*- und *eSign-Anwendung*), implementiert durch das Filesystem „CPFWxSCSI35-1A-0_V104"			-
4	Dokumen-tation	STARCOS 3.5 ID GCC C1 Guidance for Inlay Production [UG_Inlay]	1.0	16.08.2010	Dokument in elektronischer Form
5	Dokumen-tation	Guidance Documentation for the Initialisation phase STARCOS 3.5 ID GCC C1 [UG_Ini]	1.0	19.11.2010	Dokument in elektronischer Form
6	Dokumen-tation	Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID GCC C1R [UG_Pers]	1.3	23.01.2012	Dokument in elektronischer Form

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
7	Dokumentation	Guidance Documentation for the Usage Phase STARCOS 3.5 ID GCC C1 [UG_Use]	1.4	19.11.2010	Dokument in elektronischer Form

1.4 Hersteller

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

2. Funktionsbeschreibung

Funktionalität und Architektur

Das Chipkartenprodukt STARCOS 3.5 ID GCC C1R ist vorgesehen für den Einsatz als neuer Personalausweis. Aus technischer Sicht ist die „nPA-Signaturkarte“ realisiert als kontaktlose Chipkarte mit einem zu ISO/IEC 7816-4 konformen Betriebssystem und einer Anwendungsebene, die direkt auf der Betriebssystemebene aufsetzt.

Die „nPA-Signaturkarte“ basiert auf dem Halbleiter "NXP P5CD128V0A" mit dedizierter Software der NXP Semiconductors GmbH. Der Halbleiter inklusive seiner dedizierten Software wurde nach CC EAL 5+ evaluiert (CC Version 3.1) und durch das BSI im Jahre 2010 unter der Registrierungsnummer BSI-DSZ-CC-0645 zertifiziert.

Die „nPA-Signaturkarte“ besteht u.a aus den folgenden Komponenten:

- Halbleiter (IC) von NXP mit dedizierter Software,
- Betriebssystem STARCOS 3.5 und
- der *eSign-Anwendung*.

Nach Ausgabe der „nPA-Signaturkarte“ besitzt die *eSign-Anwendung* weder ein Signaturschlüsselpaar noch eine Signatur-PIN. Die „nPA-Signaturkarte“ kann durch den Inhaber des Ausweises unter Kontrolle des zertifikatsausstellenden Zertifizierungsdiensteanbieter als sichere Signaturerstellungseinheit aktiviert werden. Hierzu ist an einem Signaturterminal[3] 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 „nPA-Signaturkarte“ die Schlüsselgenerierung initiiert und der öffentliche Signaturprüfschlüssel ausgelesen. Der ZDA darf das qualifizierte Zertifikat erst dann ausstellen, wenn er sich davon überzeugt hat, dass die „nPA-Signaturkarte“ 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.

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

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

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

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 Fehlbedienungszählers 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 initialen Aktivierung.

Alle für die Signaturanwendung relevanten Zugriffe auf die kontaktlose „nPA-Signaturkarte“ müssen an einem Signaturterminal unter Anwendung von Secure Messaging erfolgen. Zur gegenseitigen Authentisierung von Terminal und Karte sowie und 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,
- eines Signaturterminals zur Erstellung von qualifizierten elektronischen Signaturen sowie zum Management der Signatur-PIN.

Die Sicherheitseigenschaften der „nPA-Signaturkarte“ werden mit der Beschreibung der Sicherheitsfunktionen weiter erläutert.

Das STARCOS Betriebssystem erlaubt dem Kartenhersteller eine Reihe von Konfigurations-möglichkeiten. 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 „CPFWxSCSI35-1A-0_V104") 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 „nPA-Signaturkarte“ nicht unterstützt.

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

- DSA auf Basis elliptischer Kurven (ECDSA) basierend auf Gruppen $E(F_p)$ (vgl. [TR-03111]) sowie
- Zufallszahlenerzeugung auf Basis eines deterministischen Zufallszahlengenerators (DRNG), dessen Seed durch die zugrundeliegende Hardware generiert wird. Der DRNG wurde im Rahmen der Evaluierung als K4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet. Der Zufallszahlengenerator der zugrundeliegenden Hardware von NXP 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 NXP geprüft (vgl. [NXP ST Lite]).

Die „nPA-Signaturkarte“ verwendet die ECC Brainpool Kurve P256r1 gemäß [TR-03116-2], Kapitel 1.3.2.

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

- Hashfunktion SHA-256 gemäß [FIPS 180-2],
- Diffie-Hellman auf Basis elliptischer Kurven (ECDH) gemäß [TR-03111] 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 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 Änderungen der „nPA-Signaturkarte“ gegenüber dem Vorgängerprodukt STARCOS 3.5 GCC C1 bestehen aus Anpassungen des Betriebssystems sowie der Erweiterung der *eID-Anwendung* um ein zusätzliches Datenfeld. Die Kryptoalgorithmen sind durch die Anpassungen nicht betroffen.

Die „nPA-Signaturkarte“ wurde auf Basis der Common Criteria in der Version 3.1 sowie des Protection Profiles [BSI-CC-PP-0061] für den neuen Personalausweis erfolgreich evaluiert [ETR]. Die Zertifizierung des Produktes erfolgt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem Sicherheitszertifikat BSI-DSZ-CC-0800. Die Prüftiefe beträgt EAL 4+ mit den Augmentierungen AVA_VAN.5, ATE_DPT.2 und ALC_DVS.2.

Weiterhin berücksichtigt die „nPA-Signaturkarte“ das Protection Profile „Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation“, prEN 14169-1:2009, BSI-CC-PP-0059 [BSI-CC-PP-0059].

Sicherheitsfunktionen bzw. –eigenschaften der „nPA-Signaturkarte“

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

„Zugriffskontrolle“

Die „nPA-Signaturkarte“ 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: „yes“, „no“)
- Für das Datenobjekt Secure 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 „nPA-Signaturkarte“ durch Eingabe der Signatur-PIN als Signierer.

Alle für die Signaturanwendung relevanten Zugriffe auf die kontaktlose „nPA-Signaturkarte“ müssen an einem bestätigten Signaturterminal erfolgen. Zur gegenseitigen Authentisierung und zum Aufbau eines sicheren Kommunikationskanals zwischen Terminal und „nPA-Signaturkarte“ werden die Authentisierungen PACE Protokoll, Terminal- und Chipauthentisierung verwendet.

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

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

In Abhängigkeit der durchzuführenden Funktion sind für das PACE Protokoll die Ausgangswerte (Card Access Number (CAN), eID-PIN, PUK) zu unterscheiden. Dabei ist die CAN auf der Vorderseite des Kartenkörpers aufgedruckt und damit kein Geheimnis für jeden, der physischen Zugriff auf die „nPA-Signaturkarte“ hat. Durch Eingabe einer CAN wird vom Karteninhaber die Kommunikation mit einer kontaktlosen Karte begonnen und ist damit ein Äquivalent zum Einführen einer kontaktbehafteten Karte in ein Lesegerät. Dadurch wird eine unbeaufsichtigte Kommunikation mit der „nPA-Signaturkarte“ erschwert.

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

„Terminalauthentisierung“

Die „nPA-Signaturkarte“ unterstützt die Durchführung der Terminalauthentisierung. Dieses Protokoll wird zur Authentisierung des Terminals (Challenge-and-Response Protokoll) gegenüber der „nPA-Signaturkarte“ genutzt. Weiterhin erfolgt mit dem Protokoll der Nachweis der Zugriffsrechte des bestätigten Signaturterminals gegenüber der „nPA-Signaturkarte“. Diese Rechte werden an den sicheren Kanal, der anschließend mit der Chipauthentisierung aufgebaut wird, gebunden. 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 „nPA-Signaturkarte“ sind die beiden EAC-PKI'n 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 bestätigtes Signaturterminal erfolgen, werden über die EAC-PKI der *eSign-Anwendung* authentisiert.

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

Die Zugriffsrechte eines bestätigten 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 „nPA-Signaturkarte“.

„Chipauthentisierung“

Die „nPA-Signaturkarte“ unterstützt die Durchführung der Chipauthentisierung. Dieses Protokoll wird zur Authentisierung des Chips gegenüber dem Terminal sowie zum Aufbau eines sicheren Kanals für die verschlüsselte und integritätsgesicherte Kommunikation zwischen Terminal und Karte genutzt. Das Protokoll basiert auf einem Hybridverfahren auf der Grundlage des Diffie-Hellman Protokolls zur Schlüsselvereinbarung. 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 „nPA-Signaturkarte“ einen Chipauthentisierungsschlüssel (statisches DH Schlüsselpaar). Der öffentliche Schlüssel wird in der „nPA-Signaturkarte“ in einer signierten Datenstruktur im MF (im EF.CardSecurity) der Karte gespeichert. Die Signatur wird durch den Ausweishersteller mit einem Schlüssel erzeugt, dessen Authentizität mit einer spezifischen PKI, der Dokumenten-PKI, nachgewiesen wird.

Der Ausweishersteller signiert nur öffentliche Schlüssel authentischer nPAs. 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 „nPA-Signaturkarte“ 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 „nPA-Signaturkarte“ (in der *eSign-Anwendung*) geheim gespeicherten Referenzwert (RAD).

Die Signatur-PIN mit einer Mindestlänge von sechs Stellen ist vor der Aktivierung der *eSign-Anwendung* durch den designierten Signaturschlüsselinhaber zu setzen. Dies muss an einem bestätigten Signaturterminal, das über eine entsprechende Berechtigung verfügt, erfolgen. Weiterhin kann die Signatur-PIN nur gesetzt werden, falls kein nutzbarer Signaturschlüssel auf der Karte vorhanden ist.

Die Signatur-PIN besitzt einen Fehlbedienungszähler (FBZ) mit dem Initialwert drei, der nach Eingabe einer falschen PIN um eins erniedrigt wird. D.h. nach einer dreimaligen Eingabe einer falschen PIN steht der FBZ auf Null und die „nPA-Signaturkarte“ ist blockiert. In diesem Zustand kann weder eine weitere Prüfung der Signatur-PIN erfolgen, noch eine qualifizierte elektronische Signatur erzeugt werden.

Der FBZ der Signatur-PIN einer blockierten „nPA-Signaturkarte“ kann unter Anwendung eines globalen Resetting Codes (PUK) zurückgesetzt werden. Die „nPA-Signaturkarte“ unterstützt Resetting Codes mit einer Länge von mindestens zehn Stellen, wobei ein Resetting Code maximal zehnmal genutzt werden kann. D.h. der Nutzungszähler (Use counter) eines Resetting Codes ist maximal zehn. Nach maximal zehnmaliger Eingabe des Resetting Codes (falsch oder korrekt) kann dieser nicht mehr verwendet werden und das Zurücksetzen einer blockierten „nPA-Signaturkarte“ ist nicht mehr möglich.

Die Signatur-PIN kann durch den Signaturschlüsselinhaber geändert werden. Das Ändern der Signatur-PIN in eine neue Signatur-PIN ist nur nach einer erfolgreichen Benutzerauthentisierung unter Anwendung der aktuellen Signatur-PIN möglich.

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 „nPA-Signaturkarte“ sichergestellt.

Mit Außerbetriebnahme der *eSign-Anwendung* kann die Signatur-PIN und das Signaturschlüsselpaar „terminiert“ werden. Voraussetzung für die Terminierung 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.

„Benutzerauthentisierung mit der eID-PIN“

Die Sicherheitsfunktion beinhaltet die PIN basierte Benutzerauthentisierung 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 nPA. Sie dient insbesondere auch als Sicherheitsmerkmal für Administrationsfunktionen der *eSign-Anwendung* (z.B. Setzen der Signatur-PIN, Außerbetriebnahme der *eSign-Anwendung*).

Nach erfolgreicher Personalisierung enthält die „nPA-Signaturkarte“ 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 „nPA-Signaturkarte“ 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 Fehlbedienungszähler (FBZ) mit dem Initialwert drei, der nach Eingabe einer falschen eID-PIN um eins erniedrigt wird. D.h. nach einer dreimaligen Eingabe einer falschen eID-PIN steht der FBZ auf Null und die Nutzung der eID-PIN ist blockiert. Nach einer erfolgreichen Eingabe der eID-PIN wird der FBZ auf den Initialwert von drei gesetzt, jedoch nur dann wenn die eID-PIN nicht blockiert ist.

Nach zwei falschen Eingaben der eID-PIN kann eine erneute Eingabe der eID-PIN nur erfolgen, falls vorher eine erfolgreiche Eingabe der CAN erfolgt ist (Absicherung gegen DoS-Angriffe).

Der FBZ der eID-PIN einer blockierten eID-PIN kann unter Anwendung eines globalen Resetting Codes (PUK) zurückgesetzt werden. Die „nPA-Signaturkarte“ unterstützt einen Resetting Code mit einer Länge von mindestens zehn Stellen, wobei der Resetting Code maximal zehnmal genutzt werden kann. D.h. der Nutzungszähler (Use counter) des Resetting Codes ist maximal zehn. Nach maximal zehnmaliger Eingabe des Resetting Codes (falsch oder korrekt) kann dieser nicht mehr verwendet werden und das Zurücksetzen einer blockierten eID-PIN ist nicht mehr möglich.

Die eID-PIN kann durch den Ausweisinhaber geändert werden. Hierzu muss er sich durch die erfolgreiche Eingabe der aktuellen eID-PIN gegenüber der „nPA-Signaturkarte“ 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.

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

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

„Speicheraufbereitung“

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

„Schutz bei Fehlersituationen der Hard- oder Software“

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

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

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

„Resistenz gegen Seitenkanalangriffe“

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

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

zur Verfügung. Alle sicherheitskritischen Operationen der „nPA-Signaturkarte“, insbesondere die kryptographischen Funktionen, sind durch diese Hard- und Softwaremechanismen

geschützt. Informationen über Leistungsaufnahme sowie Ausführungszeiten von Kommandos lassen keine Rückschlüsse auf sicherheitsrelevante Daten wie Signaturschlüssel oder Signatur-PIN zu.

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

„Selbsttest“

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

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

„Kryptographische Algorithmen“

Diese Sicherheitsfunktion der „nPA-Signaturkarte“ stellt die kryptographischen Funktionen zur Verfügung. Sie stützt sich auf die kryptographischen Funktionen des evaluierten und zertifizierten Halbleiters und seiner dedizierten Software ab.

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

„Erzeugung von ECDSA-Schlüsselpaaren“

Die „nPA-Signaturkarte“ unterstützt eine karteninterne Erzeugung von ECDSA-Schlüsselpaaren zur Erzeugung von qualifizierten Signaturen mit einer Länge von 256 Bit.

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

- Es werden Schlüssel für das ECDSA Verfahren auf Basis von $E(F_p)$ generiert. Die Länge der Parameter p und q beträgt 256 Bit.
- Die Schlüsselgenerierung erfüllt die Anforderungen gemäß [Alg_Kat 2012], Kapitel 3.2.a) DSA-Varianten basierend auf Gruppen $E(F_p)$.
- Zur Schlüsselerzeugung wird der deterministische Zufallszahlengenerator der „nPA-Signaturkarte“ verwendet.
- Die Schlüsselerzeugung stellt sicher, dass der Signaturschlüssel nicht aus dem Signaturprüfschlüssel ableitbar ist.
- Nach der Schlüsselgenerierung verifiziert die „nPA-Signaturkarte“, 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 „nPA-Signaturkarte“ authentisiert hat und seine zur Schlüsselerzeugung erforderlichen Zugriffsrechte nachgewiesen hat. In diesem Fall hat das Sicherheitsattribut SCD / SVD Management den Wert „yes“. 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 „nPA-Signaturkarte“ 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 „nPA-Signaturkarte“ aufgerufen werden. Die für die Schlüsselgenerierung zu verwendende Schlüssellänge wird durch den Kartenhersteller in die Initialisierungsdaten eingetragen und mit der Initialisierung der „nPA-Signaturkarte“ in der Karte unveränderbar gespeichert. Das Kommando GENERATE ASYMMETRIC KEY PAIR wertet zur Erzeugung des Signaturschlüssels die in der Karte gespeicherte Schlüssellänge aus.

Die Initialisierungsdaten (Filesystem und weitere Parameter) werden durch Giesecke & Devrient GmbH erzeugt. Sie unterliegen einer Ende-zu-Ende Sicherung zwischen Kartenhersteller und Karte. Nachträgliche Änderungen an den Initialisierungsdaten können somit durch die Karte erkannt werden. Somit kann die in der Karte gespeicherte Schlüssellänge weder vom Ausweishersteller noch vom ZDA verändert werden.

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

„Erzeugung von qualifizierten Signaturen“

Die „nPA-Signaturkarte“ unterstützt die Erzeugung von qualifizierten elektronischen Signaturen mit dem ECDSA Signaturschlüssel mit einer Schlüssellänge von 256 Bit. Die Sicherheits-funktion hat die folgenden Eigenschaften:

- Empfang von Daten (Data to be signed, DTBS) zur Erzeugung von qualifizierten elektronischen Signaturen.
- Berechnungen von ECDSA Signaturen gemäß EN 14890 [EN 14890-1] mit einer Schlüssellänge von 256 Bit.
- Zur Erzeugung von Zufallszahlen für die Generierung von ECDSA Signaturen wird der deterministische Zufallszahlengenerator der „nPA-Signaturkarte“ verwendet.
- Die Signaturerzeugung ist resistent gegen Seitenkanalangriffe.

- Die Signaturerzeugung erfolgt in der Art und Weise, dass der Signaturschlüssel nicht aus der erzeugten Signatur abgeleitet werden kann und während der Signaturerzeugung keine Informationen über den Signaturschlüssel ermittelt werden können.
- Eine Signaturerzeugung kann nur durchgeführt werden, wenn eine erfolgreiche Benutzerauthentisierung mit der 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 bestätigten Signaturterminal möglich, das sich gegenüber der „nPA-Signaturkarte“ 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)	**Anforderung** Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.
Abs. (3) Nr. 1	**Anforderung** Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ...

Tabelle 3: Erfüllung der Anforderungen der Signaturverordnung

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

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

3.2 Einsatzbedingungen

Anforderungen an den Initialisierer

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

Anforderungen an den Personalisierer

- Der Ausweishersteller 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 Ausweishersteller muss sicherstellen, dass kryptographische Schlüssel, die zur Sicherung der Personalisierungsdaten eingesetzt werden, sicher behandelt werden.
- Die Vorgaben des Kartenherstellers an die Personalisierung gemäß [UG_Pers] sind zu berücksichtigen.

Anforderungen an den Zertifizierungsdiensteanbieter

- Die eingesetzte Zertifizierungskomponente (Anwendung) zur Erzeugung von qualifizierten Zertifikaten (Signature generation Application, CGA) sollte die Sicherheitsanforderungen von [UG_Use], Kapitel 5.5.3 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 nPA – 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 § 18 des Personalausweisgesetzes [PAuswG] 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* des nPA personalisiert sind) auch im Besitz des nPA ist.

  Die sichere Identifizierung muss beinhalten, dass der Antragsteller im Besitz **seiner** „nPA-Signaturkarte“ ist, d.h. dass die Zuordnung zwischen Karte und Person korrekt ist. Hierzu darf die Identifizierung nicht alleine auf der *eID-Anwendung* des nPA 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.

- Programme, die ein ZDA seinen Kunden i.S.v. § 5 Abs. 1 Satz 2 SigV zur Übertragung von Referenzdaten auf die „nPA-Signaturkarte“ 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 bestätigten Chipkartenleser mit sicherer PIN-Eingabe (d.h. Cat-K oder mindestens Cat-S gemäß [TR-03119]) verwenden.
- Der Ausweisinhaber muss verifizieren, dass die fünfstellige Transport-eID-PIN noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte eID-PIN setzt, die über eine Länge von sechs Stellen verfügt. Ist die Transport-eID-PIN nicht gültig oder hat diese nicht genau fünf Stellen, so muss sich der Ausweisinhaber mit der ausgebenden Ausweisbehörde in Verbindung setzen.
- Der Ausweisinhaber muss zum Setzen und Ändern der Signatur-PIN ein bestätigtes 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 „nPA-Signaturkarte“ so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Zur Erzeugung von qualifizierten Signaturen verwendet der Signaturschlüsselinhaber die „nPA-Signaturkarte“ nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.
- Wenn möglich, sollte der Einsatz des neuen Personalausweises 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 STARCOS 3.5 sowie der *eSign-Anwendung* geeignet berücksichtigen.
- Bei der Erzeugung einer qualifizierten Signatur mit Übergabe eines extern berechneten Hashwerts ist die Auswahl einer geeigneten Hashfunktion durch die Signaturanwendungskomponente sicherzustellen.
- Der Hersteller einer Signaturanwendungskomponente zur Erzeugung von qualifizierten elektronischen Signaturen (Signature Creation Application, SCA) sollte die Sicherheitsanforderungen von [UG_Use], Kapitel 5.5.4 berücksichtigen.

3.3 Algorithmen und zugehörige Parameter

Die „nPA-Signaturkarte“ stellt das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ mit einer Länge von 256 Bit für die Parameter p und q zur Erstellung von elektronischen Signaturen bereit. Auf der Grundlage dieser Berechnungen können mit der „nPA-Signaturkarte“ ECDSA Signaturen gemäß EN 14890 erzeugt werden [EN 14890-1]. Dabei erfolgt die Signaturerzeugung mit einer ausschließlich externen Hashwertberechnung. Eine karteninterne Hashwertberechnung mit dem SHA-256 gemäß [FIPS 180-2] stellt die „nPA-Signaturkarte“ zwar zur Verfügung, zur Erzeugung qualifizierter Signaturen wird sie jedoch nicht genutzt.

Zur Erzeugung von Zufallszahlen wird in der „nPA-Signaturkarte“ ein deterministischer Zufallszahlengenerator verwendet. Der Zufallszahlengenerator ist ein K4-Generator mit Resistenz gegen Angriffe mit hohem Angriffspotenzial im Sinne der [AIS 20]. Der Parameter „Seed“ wird durch die zugrundeliegende Hardware mit einer Entropie von mindestens 100 Bit erzeugt. 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 $E(F_p)$ 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 2018
p	Keine Einschränkung	Keine Einschränkung
q	224 Bit	250 Bit

Diese Bestätigung der „nPA-Signaturkarte“ 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 STARCOS 3.5 ID GCC C1R wurde erfolgreich nach den Common Criteria (CC) Version 3.1 mit der Prüfstufe **EAL4+** (EAL4 mit den Augmentierungen AVA_VAN.5, ATE_DPT.2, ALC_DVS.2) evaluiert.

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

Hierfür liegt das deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0800 vom 31. Januar 2012 vor.

Die Evaluierung wurde in Form einer sogenannten „Composition Evaluation“ durchgeführt, die die Evaluierungsergebnisse der CC Evaluierung des NXP P5CD128V0A des Herstellers NXP Semiconductors GmbH berücksichtigt. Diese Evaluierung erfolgte mit der Prüfstufe **EAL5+** (EAL5 mit den Augmentierungen ALC_DVS.2, AVA_VAN.5 und ASE_TSS.2). Die Evaluierung erfolgte gegen ein **hohes** Angriffspotential.

Hierfür liegt das deutsche Sicherheitszertifikat BSI-DSZ-CC-0645 vom 23. Juli 2010 vor.

Hierzu wurde im April 2011 ein Maintenance Verfahren (BSI-DSZ-CC-0645-2010-MA-01) sowie im Oktober 2011 eine erneute Bewertung (Re-Asssessment) des Halbleiters erfolgreich abgeschlossen.

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

Referenzen

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

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

[PAuswG] Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PauswG) vom 18. Juni 2009 (BGBl. I S. 1346)

[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 im Bundesanzeiger Nr. 10 vom 18. Januar 2012, S. 243

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

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

[BSI-CC-PP-0059] Protection profiles for Secure signature creation device — Part 2: Device with key generation, BSI-CC-PP-0059 prEN 14169-1:2009, Version 1.03, 2009-12

[BSI-CC-PP-0061] Common Criteria Protection Profile – Electronic Identity Card (ID_Card PP), BSI-CC-PP-0061, Version 1.03, December 15th 2009, Bundesamt für Sicherheit in der Informationstechnik

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

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.5 ID GCC C1R, Version 1.1, 27.01.2012, BSI-DSZ-CC-0800

[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: Interindustry commands for interchange, ISO/IEC 7816-4, First edition, September 1.1995

[ISO 10118-3] ISO/IEC 10118-3: Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions, 2nd ed., 2004

[NXP ST Lite] NXP, NXP Secure Smart Card Controllers P5Cx128V0A/P5Cx145V0A, MSO, Security Target Lite, Rev. 1.7, 16 December 2010

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

[ST] Giesecke & Devrient GmbH, STARCOS 3.5 ID GCC C1R, Security Target, Version 1.2, 09.12.2011

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

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

[TR-03116-2] BSI. Technische Richtlinie TR-03116-2, eCard Projekte der Bundesregierung, Teil 2 - Hoheitliche Ausweisdokumente, Stand 2010

[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 1.2, 27. Mai 2011

[UG_Inlay] STARCOS 3.5 ID GCC C1 Guidance for Inlay Production, Version 1.0, 16.08.2010

[UG_Ini] Guidance Documentation for the Initialisation phase STARCOS 3.5 ID GCC C1, Version 1.0, 19.11.2010

[UG_Pers] Guidance Documentation for the Personalisation Phase STARCOS 3.5 ID GCC C1R, Version 1.3, 23.01.2012

[UG_Use] Guidance Documentation for the Usage Phase STARCOS 3.5 ID GCC C1, Version 1.4, 19.11.2010

Ende der Bestätigung