

Bestätigung

von Produkten für qualifizierte elektronische Signaturen

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

Bundesamt für Sicherheit in der Informationstechnik³

Godesberger Allee 185-189

53175 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 15 Abs. 2 und 4, § 11 Abs. 3 SigV,
dass die

**Signaturerstellungseinheit
ZKA SECCOS Sig v1.5.3**

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

BSI.02076.TE.12.2006



Bonn, den 04.12.2006

gez. Helmbrecht

Dr. Helmbrecht, Präsident

Das Bundesamt für Sicherheit in der Informationstechnik ist, auf Grundlage des BSI-Errichtungsgesetzes vom 17.12.1990, Bundesgesetzblatt I S. 2834 und gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

¹ Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

² Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) geändert durch 1. SigÄndG

³ Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Postfach 200363, 53133 Bonn, Tel: +49(0)3018 9582-0, Fax: +49(0)3018 9582-5455, E-Mail: bsi@bsi.bund.de, Web: www.bsi.bund.de

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3 der Sagem Orga GmbH⁴.

Auslieferung und Lieferumfang:

Die ZKA-Chipkarte wird als Geldkarte/Debit-Karte mit Signaturanwendung von Sagem Orga an die folgenden Verlage der Kreditwirtschaft ausgeliefert:

- Bank-Verlag GmbH
- Deutscher Genossenschafts-Verlag eG
- Deutscher Sparkassen Verlag GmbH
- Bundesverband Öffentlicher Banken-ZVD GmbH

Für die Auslieferung sind folgende Varianten vorgesehen:

- Auslieferung als nicht-initialisiertes Modul bzw. als nicht-initialisierte Smartcard:
Die Auslieferung als Modul bzw. Smartcard ist kombiniert mit der Auslieferung der von Sagem Orga erstellten kundenspezifischen Initialisierungstabelle (die insbesondere die evaluierte Signatur-Applikation beinhaltet) an den Kunden. Dort durchläuft die ausgelieferte Initialisierungstabelle das vorgesehene Post-Processing beim Empfänger für das Einfügen zusätzlicher Prüfdaten. Anschließend wird die finalisierte Initialisierungstabelle auf geeignet abgesichertem Transportweg zum Initialisierer gegeben zum Laden der Initialisierungstabelle. Für die Initialisierung sind die in der Benutzerdokumentation für den Initialisierer⁵ definierten Auflagen zu berücksichtigen, die von Sagem Orga erstellt und ausgeliefert wird. Die Initialisierungstabellen sind so abgesichert, dass auch beim Laden durch den Kunden gemäß den Anleitungen der entsprechenden User-Guidance keine unerlaubten Änderungen vorgenommen werden können. Solche Änderungen werden durch die Sicherheitsmechanismen der Chipkarten Hard- und Software erkannt und führen zum Fehlschlagen der Initialisierung.
- Auslieferung als initialisiertes Modul bzw. als initialisierte Karte:
Die Initialisierung der Module bzw. Karten wird durch Sagem Orga durchgeführt. Vor der Initialisierung wird die von Sagem Orga erstellte kundenspezifische Initialisierungstabelle (die insbesondere die evaluierte Signatur-Applikation beinhaltet) an den vorgesehenen Verlag der Kreditwirtschaft gesandt. Für die Finalisierung der Initialisierungstabelle sind die folgenden Prozesse auf Kundenseite auszuführen: Die ausgelieferte Initialisierungstabelle durchläuft das vorgesehene Post-Processing für das Einfügen zusätzlicher Prüfdaten. Anschließend wird die finalisierte Initialisierungstabelle vom Verlag der Kreditwirtschaft auf geeignet abgesichertem Transportweg an Sagem Orga als Initialisierer zum Laden der Initialisierungstabelle zurückgesandt.

⁴ Im Folgenden ZKA-Chipkarte genannt.

⁵ Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v1.5.3, Version 1.01, 07.07.2006

Im Fall der Auslieferung als Modul ist der letzte Schritt des Kartenproduktionsprozesses, d.h. das Embedding der ausgelieferten Module und finale Kartentests, Aufgabe des Kunden.

Zur Nutzung der ZKA-Chipkarte als Signaturkarte arbeiten die Verlage jeweils mit ausgewählten Zertifizierungsdiensteanbietern zusammen. Die Initialisierungs- und Personalisierungsabläufe innerhalb eines Verlags müssen den Anforderungen des Signaturgesetzes genügen und sind ggf. durch ein separates Sicherheitskonzept nachzuweisen, das als Anlage zum Sicherheitskonzept des jeweiligen Zertifizierungsdiensteanbieters zur Akkreditierung bei der Bundesnetzagentur vorgelegt werden muss.

Antragsteller dieser Bestätigung sowie Hersteller und Vertreiber:

Sagem Orga GmbH

Heinz-Nixdorf-Ring 1

33106 Paderborn

Lieferumfang des Produktes:

Zum Lieferumfang des Produktes gehören zum einen die in Tabelle 1 dargestellten Anteile, die unabhängig vom Kunden immer ausgeliefert werden. Tabelle 2 führt paarweise zusammengehörige Initialisierungstabellen und Data Sheets auf, wobei genau ein Paar von Initialisierungstabelle und Data Sheet jeweils Bestandteil der Auslieferung des Produktes an einen speziellen Kunden ist.

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
1	Hardware	IC AE55C1 von Renesas Technology (Zertifizierung unter BSI-DSZ-CC-0379-2006)	02		Modul oder Smartcard
2	Software	Advanced Cryptographic Library, Version 1.43 with SHA-256 module (ACL). (Zertifizierung unter BSI-DSZ-CC-0379-2006)	ROM-Maske SECCOS_5.0_AE55C1_R1.2_SHA256		
3	Software	Smartcard Embedded Software (SECCOS Betriebssystem)			

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
4	Dokumentation	Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v1.5.3	1.01	07.07.2006	Gedrucktes oder elektronisches Dokument
5	Dokumentation	System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v1.5.3	1.01	07.07.2006	Gedrucktes oder elektronisches Dokument
6	Dokumentation	Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS	1.3	29.12.2004	Gedrucktes oder elektronisches Dokument
7	Dokumentation	Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Anhang - Debitkarte mit EMV- GA/Maestro- und Signatur-Anwendung	1.2	27.09.2005	Gedrucktes oder elektronisches Dokument

Tabelle 1: Kundenunabhängiger Lieferumfang

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
1	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SDR001G0.A_3		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.01	07.07.2006	Gedrucktes oder elektronisches Dokument
2	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SDR001G0.A_5		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.02	05.09.2006	Gedrucktes oder elektronisches Dokument
3	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SDR001G0.A_7		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.03	14.09.2006	Gedrucktes oder elektronisches Dokument
4	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SWR001H0.A_1		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.04	14.09.2006	Gedrucktes oder elektronisches Dokument
5	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SDR001G0.A_9		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.05	09.10.2006	Gedrucktes oder elektronisches Dokument
6	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SWR001H0.A_3		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.06	09.10.2006	Gedrucktes oder elektronisches Dokument

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
7	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SDR001G0.A_B		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.07	23.10.2006	Gedrucktes oder elektronisches Dokument
8	Software (Initialisierungstabelle)	Initialisierungstabelle mit Signaturapplikation	SWR001H0.A_5		Skripte in elektronischer Form
	Dokumentation	Data Sheet - ZKA-SECCOS Sig v1.5.3	Version 1.08	23.10.2006	Gedrucktes oder elektronisches Dokument

Tabelle 2: Kundenspezifische Initialisierungstabellen und Data Sheets

2 Funktionsbeschreibung

Kurzbeschreibung:

Das SECCOS Betriebssystem stellt eine interoperable, ISO 7816 konforme, multi-applikative Plattform zur Verfügung. Es ist in Form einer nativen Implementierung realisiert und setzt auf dem Halbleiter AE55C1 (HD65255C1), Version 02 und der zugehörigen Advanced Cryptographic Library, Version 1.43 mit SHA-256 Modul (ACL) von Renesas Technology Corp.⁶ auf. Die ACL stellt Kernroutinen für RSA und DES basierte kryptographische Operationen, Routinen für Hashwert-Berechnung (SHA-1, SHA-256, RIPEMD-160) und Routinen zur Zufallszahlengenerierung zur Verfügung.

Die Signatur-Applikation ZKA-SigG-Q der Signaturkarte setzt direkt auf der SECCOS Betriebssystem-Plattform auf und umfaßt ein eigenes File- und Datensystem mit dedizierten Sicherheitsstrukturen. Darin sind applikationsspezifische Zugriffsregeln für den Zugriff auf Objekte, applikationsspezifische Sicherheitsmechanismen und ein eigenes PIN- und Key-Management enthalten. Das Design und die Implementierung der Signatur-Applikation und ihrer Sicherheitsstrukturen folgt der Schnittstellenspezifikation für die ZKA-Chipkarte⁷. Die Signatur-Applikation macht ausschließlich Gebrauch von den allgemeinen Datenstrukturen, der allgemeinen Sicherheitsarchitektur und den Standard- und Produktions-Kommandos, wie sie in der SECCOS Betriebssystem-Plattform⁸ implementiert sind.

Der große Umfang technischer, funktionaler und Sicherheits-Features der SECCOS Betriebssystem-Plattform, die im SECCOS Produkt von Sagem Orga implementiert wurde, unterstützt neben der dedizierten Signatur-Applikation weitere Anwendungen wie z. B. die GeldKarte-, EMV⁹- oder Electronic Cash-Applikation. Diese Applikationen nutzen dieselben Komponenten wie Halbleiter, ACL und SECCOS Betriebssystem-Plattform wie die Signatur-Applikation, jedoch ist eine komplette Trennung zwischen der Signatur-Applikation und diesen zusätzlichen Applikationen realisiert. Das Design der verschiedenen Applikationen ist derart aufgesetzt, daß die zusätzlichen Applikationen keinen Zugriff auf die Signatur-Applikation und ihre gespeicherten und verarbeiteten Daten haben. Das bedeutet insbesondere, dass nur die Signatur-Applikation auf den geheimen Signaturschlüssel und die Signatur-PIN zugreifen kann. Die zusätzlichen Applikationen verwalten und verarbeiten ausschließlich ihre eigenen File- und Datensysteme mit eigenen Sicherheitsstrukturen und eigenem PIN- und Key- Management. Für diese zusätzlichen Anwendungen sind spezifische Applikations-Kommandos in die SECCOS Betriebssystem-Plattform integriert. Diese zusätzlichen Kommandos und Applikationen sind **nicht** Bestandteil der Bestätigung. Diese Abgrenzung wird in Abbildung 1 noch einmal graphisch verdeutlicht.

⁶ Weitere Informationen sind im Bericht zum Zertifizierungsverfahren BSI-DSZ-CC-0379-2006 enthalten, siehe www.bsi.bund.de.

⁷ Interface Specification for the SECCOS ICC, Digital Signature Application, Version 5.3, 10.02.2006, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

⁸ Schnittstellenspezifikation für die ZKA-Chipkarte - Secure Chip Card Operating System (SECCOS) (mit Errata vom 13.06.2001 und Ergänzungen bezüglich SHA-256 vom 22.12.2005), Version 5.0, 05.06.2001, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

⁹ EMV=Europay, MasterCard, Visa

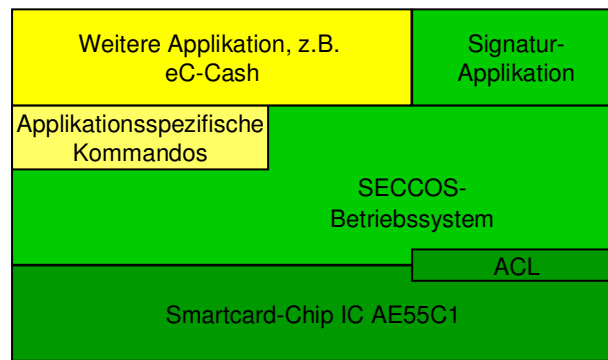


Abbildung 1: Abgrenzung der bestätigten Anteile der ZKA-Chipkarte

Die in Abbildung 1 in Grüntönen markierten Anteile stellen schematisch die Bestandteile dieser Bestätigung dar. Sie wurden im Rahmen einer kompositiven Evaluierung¹⁰ unter Einbeziehung der Ergebnisse des Zertifizierungsverfahrens BSI-DSZ-CC-0379-2006⁶ eingehend geprüft. Dabei umfasst die Evaluierung zum Zertifizierungsverfahren BSI-DSZ-CC-0379-2006 den Smartcard-Chip und die ACL. In Gelbtönen schematisch dargestellt sind Anteile der ZKA-Chipkarte, die nicht Bestandteil dieser Bestätigung sind.

Das SECCOS-Betriebssystem bietet dem Hersteller der ZKA-Chipkarte eine Reihe von Konfigurationsmöglichkeiten. Vor der Produktion hat der Hersteller über eine Initialisierungstabelle die Konfiguration gemäß den Kundenwünschen festgelegt, die im Rahmen der Evaluierung geprüft und mit einem dazugehörigen Data Sheet dokumentiert wird. Die in Tabelle 2 aufgeführten Initialisierungstabellen mit zugehörigen Data Sheets sind Bestandteil dieser Bestätigung und stellen somit verschiedene, bestätigte Konfigurationen der ZKA-Chipkarte dar. Die ZKA-Chipkarte sichert kryptographisch ab, dass genau die festgelegte Initialisierungstabelle aufgespielt werden kann. Ein Aufspielen von nachträglich unberechtigt geänderten Initialisierungstabellen ist nicht möglich. Die ZKA-Chipkarte erlaubt auch nicht, weitere Software nachträglich auf die Karte aufzubringen.

Funktionsbeschreibung des Produkts

Die umfangreichen Sicherheitsfunktionen der ZKA-Chipkarte sind nicht in allen Phasen ihres Lebenszyklus aktiv. Funktionalität, die lediglich in der Initialisierungs- und Personalisierungsphase vor der Auslieferung an den Endkunden relevant ist, ist in den nachfolgenden Beschreibungen entsprechend gekennzeichnet.

PIN-basierte Authentifizierung des Signierers

Die Möglichkeit, sich über eine Signatur-PIN als Signierer zu authentifizieren, ist erst nach der Initialisierungs- und Personalisierungsphase möglich. Die Authentifizierung geschieht über den Vergleich der von außen zur Verfügung gestellten Signatur-PIN mit den geheimen Vergleichsdaten, die nicht auslesbar auf der Karte gespeichert sind.

Direkt nach dem Ende der Initialisierungs- und Personalisierungsphase ist gemäß der Schnittstellenspezifikation der ZKA-Chipkarte⁷ eine 5-stellige Transport-PIN vorgegeben. Die ZKA-Chipkarte erzwingt, dass der Signierer vor der Erstellung der ersten qualifizierten elektronischen Signatur eine neue, mindestens 6-stellige

¹⁰ siehe auch den Bericht zum Zertifizierungsverfahren BSI-DSZ-CC-0386-2006, erhältlich in elektronischer Form auf www.bsi.bund.de

Signatur-PIN setzt. Dafür muss er sich durch Eingabe der Transport-PIN gegenüber der ZKA-Chipkarte authentifizieren. Die Transport-PIN dient ausschliesslich zu dieser Authentifizierung, so dass insbesondere mit der Transport-PIN keine qualifizierte elektronische Signatur erstellt werden kann.

Die Transport- und die Signatur-PIN besitzen einen Fehlbedienungsähler von 3, was zur Folge hat, dass nach dreimaliger Eingabe einer falschen PIN in Folge die ZKA-Chipkarte blockiert ist. Da kein PUK¹¹ für die Transport- oder Signatur-PIN existiert, kann der Fehlbedienungsähler einer einmal blockierten PIN nicht zurückgesetzt werden. Ist die ZKA-Chipkarte einmal blockiert, können keine Signaturen mehr erstellt werden. Die erfolgreiche Eingabe der Signatur-PIN setzt den Fehlbedienungsähler wieder auf 3 zurück, falls die Karte noch nicht blockiert ist. Zur Behandlung von Transport- und Signatur-PIN sind insbesondere die Auflagen an den Signierer zu beachten, die in Kapitel 3.2 sowie in der Benutzerdokumentation für den Personalisierer¹² dargestellt sind.

Der Signierer kann die Signatur-PIN ändern. Dazu muss er im Rahmen der Änderung die alte Signatur-PIN unmittelbar vor der Eingabe der neuen Signatur-PIN eingeben. Sofern die Karte noch nicht blockiert ist, kann er eine andere, mindestens 6-stellige Signatur-PIN vorgeben.

Nach einmaliger Eingabe der Signatur-PIN kann nur eine qualifizierte elektronische Signatur erstellt werden. Für jede weitere Signatur oder die Änderung der Signatur-PIN ist die Signatur-PIN erneut einzugeben.

Die ZKA-Chipkarte unterstützt Secure Messaging gemäß dem Standard ISO/IEC 7816-4 (s.u.). Secure Messaging wird für die Übertragung der vom Benutzer eingegebenen PIN zur ZKA-Chipkarte angeboten aber nicht erzwungen.

Sicherung der Integrität von gespeicherten Daten

Die ZKA-Chipkarte überwacht die Integrität von bestimmten Datenobjekten, zu denen insbesondere das Signaturschlüssel-Paar sowie die Signatur-PIN gehören. Vor dem Zugriff auf ein entsprechend gesichertes Datenobjekt wird ein 16-Bit CRC¹³ gebildet und dieser mit einem bei Erstellung des Datenobjektes erzeugten Referenzwert abgeglichen.

Ergeben sich Unterschiede, so kann auf das entsprechende Datenobjekt nicht zugegriffen werden. Ein Kommando, das für seine Abarbeitung den Zugriff auf die fehlerhaften Daten veranlasst hat, wird abgebrochen und ein sicherer Betriebszustand eingenommen.

Sicherer Datenaustausch

Die ZKA-Chipkarte stellt die Möglichkeit zur Verfügung, Daten zwischen der Chipkarte und der externen Welt vertraulich und integer auszutauschen. Dazu stellt die ZKA-Chipkarte das Leistungsmerkmal „Secure Messaging“ gemäß dem Standard ISO/IEC 7816-4 bereit.

¹¹ PUK=Personal Unblocking Key

¹² System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v1.5.3, Version V1.01, 07.07.2006

¹³ CRC=Cyclic redundancy check

Die symmetrischen, kryptographischen Schlüssel, die zur Sicherung des Datenaustauschs benötigt werden, handelt die ZKA-Chipkarte basierend auf einem Challenge- and Response-Verfahren mit der externen Welt zu Beginn einer Kommunikation aus.

Wiederaufbereitung von Speicher

Die ZKA-Chipkarte stellt sicher, dass nach der Deallokation von Ressourcen alle sicherheitskritischen Informationen gelöscht werden. Dabei werden alle flüchtigen und permanenten Speicherbereiche, in denen im Rahmen der ausgeführten Kommandos sicherheitsrelevante Daten zwischengepuffert wurden, physikalisch überschrieben.

Hierbei greift die ZKA-Chipkarte auf evaluierte und zertifizierte Funktionalität der Advanced Cryptographic Library zurück (siehe Tabelle 1) und nutzt weitere im SECCOS-Betriebssystem für die Speicheraufbereitung implementierte Routinen.

Schutz bei Funktionsfehlern von Hard- oder Software

Bei den folgenden Fehlfunktionen von Hard- oder Software geht die ZKA-Chipkarte in einen sicheren Betriebszustand über:

- Durch Hard- oder Software ausgelöstes Reset der ZKA-Chipkarte,
- Abbruch der Spannungsversorgung,
- Unerwarteter Abbruch der Ausführung einer der hier aufgeführten Sicherheitsfunktionen,
- genereller Ausfall des Betriebssystems,
- Interne Hard- oder Software-Fehler,
- Manipulation von Programmcode,
- Verfälschung von sicherheitsrelevanten Statusinformationen,
- physikalische Überbelastung,
- Eingabe von falschen oder inkonsistenten Daten,
- Manipulation bzw. ungenügende Qualität des Hardware-basierten Zufallszahlengenerators,
- Inkonsistenzen bei der Erzeugung von Signaturen und
- Fault injection attacks.

Wird eine entsprechende Situation erkannt, geht die ZKA-Chipkarte in einen sicheren Betriebszustand über. Auf jeden Fall werden dabei alle in Verbindung mit der Fehlfunktion stehenden Prozesse abgebrochen. Je nach Schwere der Fehlfunktion schliesst die ZKA-Chipkarte die aktuelle Betriebssession und kann entweder durch ein Reset neu angesprochen werden oder ist irreversibel blockiert. Unabhängig davon, ob die Karte nach einem Reset neu angesprochen werden kann oder blockiert ist, wird nach detektierten Fehlfunktionen immer ein sicherer Betriebszustand eingenommen.

Zur Überwachung des eigenen Betriebszustands bzw. Aufdeckung entsprechender Situationen greift die ZKA-Chipkarte auf die Sicherheitsfunktionalität der zugrundeliegenden Hardware und des SECCOS-Betriebssystems zurück.

Kryptographische Funktionen

Die ZKA-Chipkarte unterstützt die folgenden kryptographischen Funktionen:

- Hashwert-Berechnung mittels SHA-1, SHA-256 und RIPEMD-160.
- DES/3DES-Verschlüsselung gemäß dem ANSI X9.52-Standard mit einer Schlüssellänge von 56 bzw. 112 Bit¹⁴.
- RSA-Berechnung mit einer Schlüssellänge von 1024-1984 Bit (s.u.)
- Hardware-basierte Erzeugung von Zufallszahlen

Für diese Funktionalität greift die ZKA-Chipkarte maßgeblich auf die zugrundeliegende Hardware und die Advanced Cryptographic Library des Hardware-Herstellers zurück (siehe Tabelle 1).

Erzeugung eines RSA-Schlüsselpaares

Die ZKA-Chipkarte kann RSA-Schlüsselpaare mit einer Bitlänge von 1024-1984 Bits erzeugen.

Die Zufallszahlen, die im Rahmen der Schlüsselerzeugung benötigt werden, werden durch einen Hardware-Zufallszahlengenerator des zugrundeliegenden Chips erzeugt. Die hohe Qualität der Zufallszahlen stellt sicher, dass der geheime und öffentliche Schlüssel nicht vorhersagbar und mit hoher Wahrscheinlichkeit einzigartig sind.

Die Generierung eines Schlüsselpaares erfolgt unter Einbeziehung der zertifizierten ACL nach einem erprobten und genügend starken Algorithmus, bei dem die Anforderungen an RSA-Schlüssel aus dem Algorithmenkatalog der Bundesnetzagentur¹⁵ beachtet werden. Die ZKA-Chipkarte erzeugt nur RSA-Schlüsselpaare, bei denen der private Schlüssel nicht aus dem öffentlichen Schlüssel ableitbar ist. Nach der Erzeugung der Schlüssel überprüft die ZKA-Chipkarte, ob der öffentliche und der geheime Schlüssel zusammenpassen. Lediglich gültige Schlüsselpaare werden herausgegeben.

Für die Signatur-Applikation kann nur einmalig im Rahmen der Initialisierungs- und Personalisierungsphase ein gültiges Schlüsselpaar erzeugt werden, wobei ein Import von RSA-Schlüsseln für die Signatur-Applikation nicht möglich ist.

Erzeugung von qualifizierten elektronischen Signaturen

Basierend auf einem zuvor erzeugten RSA-Schlüssel mit einer Schlüssellänge von 1024-1984 Bit, stellt die ZKA-Chipkarte die folgende Funktionalität zur Erzeugung von qualifizierten elektronischen Signaturen bereit:

- Empfang von Hashwerten oder Zwischenwerten einer Hashwertberechnung mit Berechnung des abschließenden Hashwertes für die Erzeugung von qualifizierten elektronischen Signaturen gemäß den Algorithmen SHA-1, SHA-256 und RIPEMD-160,
- Erzeugen von Hashwerten aus übergebenen Daten gemäß den Algorithmen SHA-1, SHA-256 und RIPEMD-160,

¹⁴ Die Algorithmen DES/3DES kommen bei der Signaturerstellung nicht zur Anwendung und sind daher nicht Gegenstand dieser Bestätigung.

¹⁵ Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 23. März 2006, Bundesanzeiger Nr. 58, S. 1913-1915

- Erzeugung von digitalen Signaturen gemäß dem Standard DIN 66291-4, Anhang A, Kap. 2.1.1 „DSI according to ISO/IEC 9796-2 with Random Number“ (unter Gebrauch des Hashalgorithmus RIPEMD-160) und
- Erzeugung von digitalen Signaturen gemäß dem Standard DIN 66291-4, Anhang A, Kap. 2.1.2 „DSI according to #PKCS1“ (unter Gebrauch der Hashalgorithmen SHA-1 und SHA-256).

Eine Signatur wird so erstellt, dass der geheime Schlüssel nicht aus den Signaturen ermittelt werden kann. Während der Erzeugung von Signaturen können keine Informationen über den geheimen Schlüssel ermittelt werden.

Zur Generierung von Zufallszahlen zum Auffüllen von Datensätzen im Rahmen der Signaturerstellung sowie zur Hashwertberechnung und Signaturerstellung nutzt die ZKA-Chipkarte die oben aufgeführten kryptographischen Funktionen.

Widerstandsfähigkeit gegen Seitenkanal-Angriffe

Die ZKA-Chipkarte widersteht den folgenden Seitenkanal-Angriffen zum Auslesen sicherheitsrelevanter Daten wie z.B. dem geheimen Signaturschlüssel:

- Simple Power Analysis
- Differential Power Analysis
- Differential Fault Analysis
- Timing Analysis

Dies bedeutet, dass insbesondere Informationen über Leistungsaufnahme und Ausführungszeiten von Kommandos keine Rückschlüsse auf die verarbeiteten sicherheitsrelevanten Daten wie kryptographische Schlüssel oder PINs erlauben. Ein Angreifer kann diese Daten auch nicht über außenliegende Kontakte oder über die Hardware-Oberfläche auslesen.

Vor jeder kryptographischen Operation wird über das Betriebssystem eine sichere Session eingerichtet, in der auch eine Reihe von Leistungsmerkmalen der Hardware aktiviert werden.

Diese Schutzmechanismen sind mit einer Ausnahme in allen operativen Phasen des Lebenszyklus der ZKA-Chipkarte (Initialisierung, Personalisierung und Endbenutzung) aktiv. Der Schutzmechanismus ist nur dann nicht aktiv, wenn die „unsichere“ Variante der Schlüsselerzeugung zur Beschleunigung der Produktionsprozesse im Rahmen der Initialisierungs- und Personalisierungsphase gewählt wurde. Bei Wahl dieser „unsicheren“ Variante der Schlüsselgenerierung gelten besondere Bedingungen an die Einsatzumgebung für die Initialisierungs- bzw. Personalisierungsinstanz, die in Kapitel 3.2 beschrieben sind.

Selbsttests

Die ZKA-Chipkarte verfügt über verschiedene Möglichkeiten einen Selbsttest durchzuführen.

Nach dem Anlegen der Betriebsspannung und in fest vorgegebenen periodischen Abständen während des Betriebs wird automatisch die Integrität von Software-Patches zum Betriebssystem überprüft. Weiterhin verfügt die ZKA-Chipkarte über einen umfangreichen Selbsttest, bei dem zusätzlich noch die Integrität der bei der Herstellung des Chips unveränderbar eingebrachten Software (wie z.B. das Karten-Betriebssystem) überprüft wird. Dieser umfangreiche Selbsttest steht nur im Rahmen

der Initialisierungsphase der ZKA-Chipkarte zur Verfügung und muss über ein besonderes Kommando explizit veranlasst werden.

Im laufenden Betrieb wird beim Zugriff auf entsprechend geschützte Daten automatisch eine Integritätsprüfung durchgeführt, wie sie in der Funktion „Sicherung der Integrität von gespeicherten Daten“ beschrieben ist.

Administration der Signatur-Applikation

Die ZKA-Chipkarte erzwingt ein rollenbasiertes Zugriffskonzept. Dieses Konzept unterscheidet zwischen einem „Initialisierer/Personalisierer“ und einem „Signierer“. Ein Nutzer kann sich durch Kenntnis eines bestimmten Passworts als Initialisierer/Personalisierer oder durch Eingabe der Signatur-PIN als Signierer gegenüber der ZKA-Chipkarte identifizieren.

Während der Initialisierungs- und Personalisierungsphase hat lediglich der Initialisierer/Personalisierer Zugriff auf die entsprechenden Daten der Signatur-Applikation. Nach dem Ende der Personalisierungsphase sperrt die ZKA-Chipkarte die Zugriffsmöglichkeit für den Initialisierer/Personalisierer.

Für einen Initialisierer/Personalisierer bietet die ZKA-Chipkarte die folgende Funktionalität:

- Die ZKA-Chipkarte erzwingt eine Authentifizierung über ein Passwort (Chippasswort). Das Passwort wird anfangs vom Chipkartenhersteller festgelegt, kann aber vom Verlag entsprechend dem Personalisierungskonzept¹⁶ geändert werden.
- Nur ein Initialisierer/Personalisierer kann den Signaturschlüssel erzeugen. Die ZKA-Chipkarte speichert nur ein Signaturschlüssel-Paar, das auch nur einmalig erzeugt werden kann. Ein Wechsel des Signaturschlüssels ist nicht möglich.

Das Konzept zur Personalisierung von ZKA-Chipkarten des deutschen Kreditwesens¹⁶ wird von der ZKA-Chipkarte unterstützt. Dafür sind insbesondere die folgenden Funktionalitäten vorgesehen:

- Das Lebenszyklus-Modell der ZKA-Chipkarte für die Initialisierungs- und Personalisierungsphase wird maßgeblich durch einen „Chipzustand“ bestimmt. Je nach Chipzustand sind unterschiedliche Kommandos verfügbar. Nur ein Initialisierer/Personalisierer kann den Chipzustand gemäß den vorgegebenen Regeln verändern.
- Nur ein Initialisierer/Personalisierer kann die Initialisierungstabelle laden und die nachfolgende Verifikationsprüfung über entsprechende Betriebssystem-Kommandos starten.
- Nur ein Initialisierer/Personalisierer kann das Laden der Personalisierungsdaten veranlassen.

Diese Sicherheitsfunktion ist ausschliesslich im Rahmen der Initialisierungs- und Personalisierungsphase relevant.

¹⁶ Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Version 1.3, 29.12.2004, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH und Bundesverband Öffentlicher Banken-ZVD GmbH

Kontrolle des Zugriffs auf die Signatur-Applikation

Beim Zugriff auf Daten der Signatur-Applikation setzt die ZKA-Chipkarte unter Hinzunahme des Rollenkonzeptes die folgenden Regeln durch:

- Nur ein Initialisierer/Personalisierer kann den öffentlichen Signaturschlüssel exportieren. Die ZKA-Chipkarte sorgt dabei für die Verwendung eines sicheren Verfahrens.
- Nur der Initialisierer/Personalisierer darf die Transport-PIN während der Personalisierungsphase importieren.
- Secure Messaging wird im Rahmen der Personalisierung für die Wahrung der Vertraulichkeit der Personalisierungsdaten von der ZKA-Chipkarte erzwungen.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Produkt erfüllt die Anforderungen nach:

SigG

§17 Produkte für qualifizierte elektronische Signaturen

- (1) 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.
- (3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um
 1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen, ...

SigV

§15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

- (1) 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 [...] angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. [...] Die 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 Signaturprüfchlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.
- (4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

3.2 Einsatzbedingungen

Die Bestätigung gilt unter der Voraussetzung, dass die folgenden Einsatzbedingungen gewährleistet sind.

Auflagen für die Nutzung der Signaturkarte für den Initialisierer

- Die von Sagem Orga entwickelten und ausgelieferten Initialisierungstabellen sind durch den Kunden (einen der o.g. Verlage der Kreditwirtschaft) sowie beim Initialisierer in ausreichend sicherer Art und Weise zu behandeln. Dies betrifft insbesondere das Post-Processing der Initialisierungstabellen (Eintrag von

Prüfdaten). Ferner sind die Sicherheitsdaten für die Generierung der auf die Initialisierungstabellen bezogenen Prüfdaten durch den Kunden mit geeigneter Sicherheit zu behandeln.

- Das Handling der (finalisierten) Initialisierungstabellen sowie der Transfer dieser Daten zwischen den verschiedenen Produktionsstätten ist mit dem Ziel der Datenintegrität und –authentizität durchzuführen.
- Für die Sicherheit des Initialisierungsprozesses ist eine ausreichend sichere Initialisierungsumgebung mit geeigneten personellen, organisatorischen und technischen Sicherheitsmaßnahmen aufzusetzen. Ausschließlich autorisiertes und erfahrenes Personal, das für die definierten Sicherheitsmaßnahmen ausreichend geschult ist, darf in den Initialisierungs- und Testaktivitäten eingesetzt werden. Das Sicherheitskonzept für die Initialisierung und Personalisierung der ZKA-Chipkarte muss als Anlage zum Sicherheitskonzept des Zertifizierungsdiensteanbieters angefügt werden, das zur Akkreditierung bei der Bundesnetzagentur notwendig ist.
- Für den Initialisierungsprozess dürfen ausschließlich sichere Systeme innerhalb eines separaten Netzwerks, die unautorisierten Zugriff verhindern, eingesetzt werden.
- Gemäß dem zusammen mit der Signaturkarte ausgelieferten Data Sheet sind bei der RSA-Schlüsselgenerierung Abwehrmaßnahmen gegen SPA/DPA Angriffe deaktiviert. Daher muss der Initialisierer externe geeignete Sicherheitsmaßnahmen treffen, um das Produkt während der Erzeugung der Signatur-Schlüssel gegen solche Angriffe zu schützen. Hierbei sind die Vorgaben aus der User Guidance für den Initialisierer⁵ zu beachten.
- Der Initialisierungsprozeß selbst und die vorangehende Finalisierung der Initialisierungstabellen durch den Kunden ist gemäß den Beschreibungen und Vorgaben im Konzept zur Personalisierung¹⁶ und der Schnittstellenspezifikation der ZKA-Chipkarte⁷ aufzusetzen und durchzuführen. Die entsprechenden Vorgaben in der User Guidance⁵ (s. Tabelle 1) müssen beachtet werden.
- Geheime kryptographische Schlüssel, die während der Initialisierung für die Absicherung des Initialisierungsprozesses eingesetzt werden, müssen vertraulich und integer behandelt werden. Kunde und Initialisierer müssen den im Konzept zur Personalisierung¹⁶, Kap. 10 beschriebenen Prozess für den Schlüsselaustausch umsetzen.
- Das Passwort zur Authentisierung des Initialisierers/Personalisierers (Chippasswort) ist vertraulich zu behandeln.

Auflagen für die Nutzung der Signaturkarte für den Personalisierer

- Für die Personalisierung der Signaturkarte sind sichere Personalisierungsprozesse im SECCOS Betriebssystem vorbereitet bzw. werden von den vordefinierten Applikationen unterstützt. Das Konzept zur Personalisierung von ZKA-Chipkarten¹⁶, Kap. 5 und der dazugehörige Anhang zur Signaturkarte¹⁷ muss entsprechend beachtet und angewendet werden. Die

¹⁷ Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Anhang - Debitkarte mit EMV-GA/Maestro- und Signatur-Anwendung, Version 1.2 vom 27.09.2005, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH und Bundesverband Öffentlicher Banken-ZVD GmbH

Vorgaben in der User Guidance für den Personalisierer¹² (s. Tabelle 1) müssen beachtet werden.

- Der Personalisierer muß für den Personalisierungsprozess eine ausreichend sichere Personalisierungsumgebung mit geeigneten personellen, organisatorischen und technischen Sicherheitsmaßnahmen aufsetzen. Der Personalisierer muß ein sicheres Key Management (insbesondere für Authentisierungsschlüssel und Personalisierungsschlüssel) einrichten und für die ausreichende Sicherung des Datentransfers innerhalb des Personalisierungsprozesses sorgen. Ausschließlich autorisiertes und erfahrenes Personal, das für die definierten Sicherheitsmaßnahmen ausreichend geschult ist, darf in den Personalisierungs- und Testaktivitäten eingesetzt werden. Das Sicherheitskonzept für die Initialisierung und Personalisierung der ZKA-Chipkarte muss als Anlage zum Sicherheitskonzept des Zertifizierungsdiensteanbieters angefügt werden, das zur Akkreditierung bei der Bundesnetzagentur notwendig ist.
- Der Generierer der Personalisierungsdaten und der Personalisierer als Verantwortlicher für die Personalisierung der Signaturkarte (insbesondere der Signatur-Applikation) müssen die Personalisierungsdaten in ausreichend sicherer Art und Weise behandeln. Dies betrifft insbesondere sicherheitskritische Daten wie geheime kryptographische Schlüssel und PINs. Die Speicherung der Personalisierungsdaten beim Generierer und bei der Personalisierungsstelle sowie der Transfer dieser Daten zwischen den verschiedenen Produktionsstellen muss unter Berücksichtigung von Vertraulichkeit und Integrität der Daten erfolgen.
- Der Personalisierer muss alle Daten zur Sicherung des Personalisierungsprozesses, d.h. insbesondere die Personalisierungsschlüssel, ausreichend sicher behandeln.
- Gemäß dem zusammen mit der Signaturkarte ausgelieferten Data Sheet sind bei der RSA-Schlüsselgenerierung Abwehrmaßnahmen gegen SPA/DPA Angriffe deaktiviert. Daher muss der Personalisierer externe geeignete Sicherheitsmaßnahmen treffen, um das Produkt während der Erzeugung der Signatur-Schlüssel gegen solche Angriffe zu schützen. Hierbei sind die Vorgaben aus der User Guidance für den Personalisierer¹² zu beachten.
- Es liegt in der Verantwortung des Generierers der Personalisierungsdaten, für eine ausreichende Qualität der Personalisierungsdaten, insbesondere des zu personalisierenden kryptographischen Materials, zu sorgen. Der Generierer der Personalisierungsdaten muss die Personalisierungsdaten geeignet und sorgfältig vorbereiten und absichern. Insbesondere sind hierbei die vordefinierten Strukturen der Signaturkarte und die Personalisierungsanforderungen an die Signaturkarte zu berücksichtigen. Die Personalisierungsdaten müssen gemäß dem Konzept zur Personalisierung von ZKA-Chipkarten¹⁶, Kap. 5 und dem dazugehörigen Anhang zur Signaturkarte¹⁷ generiert und aufbereitet werden.
- Aus Sicherheitsgründen dürfen für den Personalisierungsprozess ausschließlich sichere Systeme innerhalb eines separaten Netzwerks, die unautorisierten Zugriff verhindern, eingesetzt werden.
- Geheime kryptographische Schlüssel, die während der Personalisierung für die Sicherung des Personalisierungsprozesses eingesetzt werden, müssen vertraulich und integer behandelt werden. Kunde und Personalisierer müssen den

in dem Konzept zur Personalisierung von ZKA-Chipkarten¹⁶, Kap. 10 beschriebenen Prozess für den Schlüsselaustausch umsetzen.

- Der Export des Signatur-Prüfchlüssels (SVD) durch den Personalisierer muss authentisch erfolgen. Der exportierte SVD muss eindeutig der Signaturkarte vom Typ ZKA SECCOS Sig v1.5.3 zugeordnet sein.
- Das Passwort zur Authentifizierung des Initialisierers/Personalisierers (Chippasswort) ist vertraulich zu behandeln.

Auflagen für die Nutzung der Signaturkarte für den Zertifizierungsdiensteanbieter (Certification Service Provider, CSP)

- Die eingesetzte Zertifizierungskomponente (Certification Generation Application, CGA) muss die Security Functional Requirements (SFRs) des Protection Profiles Secure Signature-Creation Device¹⁸, Kap. 5.3.1 erfüllen.
- Der CSP muss die Identität der Person, für die ein qualifiziertes Zertifikat ausgegeben werden soll, überprüfen. Der CSP muss überprüfen, dass diese Person in Besitz der Sicheren Signaturerstellungseinheit (SSCD) ist, das den privaten Signaturschlüssel (SCD) enthält, der zum Signatur-Prüfchlüssel (SVD) korrespondiert, der in das qualifizierte Zertifikat aufgenommen werden soll.
- Der CSP muss die kryptographischen Schlüssel, die zur Aufbringung des qualifizierten Zertifikats berechtigen, sicher und vertraulich behandeln. Hierbei sind die Regelungen aus seinem Sicherheitskonzept, das der Bundesnetzagentur vorgelegt wurde, einzuhalten.

Auflagen für die Nutzung der Signaturkarte für den Signierer bzw. Karteninhaber

- Der Signierer muss die Signatur-PIN sowie die Transport-PIN gegen Kompromittierung schützen. Der Signator darf die Signatur-PIN und die Transport-PIN anderen Personen nicht mitteilen und muss die zuvor genannten Daten ausreichend sicher verwahren.
- Der Signator muss überprüfen, dass die Transport-PIN genau 5 Stellen lang ist. Der Signator ist verantwortlich für den Wechsel der Transport-PIN und für die Wahl einer zufälligen und geheimen Signatur-PIN, deren Mindestlänge 6 Ziffern beträgt. Ist beim Erhalt der Karte die Transport-PIN bereits 6-stellig, so muss der Signierer mit der ausgebenden Stelle in Kontakt treten, da in diesem Fall eventuell bereits Signaturen mit der Karte erstellt wurden.
- Der Signierer muss die ZKA-Chipkarte so behandeln und aufbewahren, dass Missbrauch und Manipulation nicht möglich sind.
- Zur Erstellung qualifizierter elektronischer Signaturen dürfen ausschließlich vertrauenswürdige Signaturanwendungskomponenten (Signature Creation Application, SCA) verwendet werden, die gemäß Signaturgesetz von einer Bestätigungsstelle bestätigt wurden. Bestätigte Signaturanwendungskomponenten werden auf den Internetseiten der Bundesnetzagentur (www.bundesnetzagentur.de) aufgeführt.
- Im Fall, dass kein Trusted Channel bzw. kein Trusted Path (i.e. keine Verwendung von Secure Messaging) zwischen der Signaturkarte und der

¹⁸ Protection Profile – Secure Signature-Creation Device Type 3 “EAL 4+”, Version 1.05, 25.07. 2001, CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures (Hrsg), siehe auch www.bsi.bund.de, Profiltzertifizierung BSI-PP-0006-2002

Signaturanwendungskomponente auf kryptographischem Weg eingerichtet wird, muss die Umgebung, in der die Signaturkarte genutzt wird, ausreichend bzgl. Vertraulichkeit und Integrität der Authentifikationsdaten (z.B. der PIN) sowie bzgl. Integrität der zu signierenden Daten abgesichert sein.

Auflagen für die Nutzung der Signaturkarte durch Hersteller von Signaturanwendungskomponenten

- Eine Signaturanwendungskomponente muss entsprechend der Schnittstellenspezifikation für die ZKA-Chipkarte⁸ und der Schnittstellenspezifikation für die Signatur-Anwendung auf einer ZKA-Chipkarte⁷ unter Beachtung der dort spezifizierten technischen Schnittstellen implementiert werden.

3.3 Algorithmen und zugehörige Parameter

Die ZKA-Chipkarte stellt die Hashfunktionen SHA-1, SHA-256 und RIPEMD-160 sowie den RSA-Algorithmus mit einer Schlüssellänge von 1024-1984 Bit zur Erstellung von elektronischen Signaturen bereit.

Die verwendeten kryptografischen Algorithmen sind gemäß dem Algorithmen-Katalog der Bundesnetzagentur¹⁵ als geeignet eingestuft.

Der verwendete Hashalgorithmus RIPEMD-160 ist bis **Ende 2010**, die Hashfunktion SHA-1 bis **Ende 2009** und die Hashfunktion SHA-256 bis **Ende 2011** als geeignet eingestuft.

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

- 1024 Bit bis **Ende 2007**
- 1280 Bit bis **Ende 2008**
- 1536 Bit bis **Ende 2009**
- 1728 Bit bis **Ende 2010**
- 1976 Bit bis **Ende 2011**

3.4 Prüfstufe und Mechanismenstärke

Das Produkt „ZKA SECCOS Sig v1.5.3“ wurde erfolgreich nach den Common Criteria (CC) mit der Prüfstufe **EAL4+** (EAL4 mit Zusatz¹⁹ AVA_VLA.4 (gegen ein hohes Angriffspotential), AVA_MSU.3 (eine vollständige Missbrauchsanalyse)) evaluiert.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Ende der Bestätigung

¹⁹ Gemäß § 11 Abs. 3 in Verbindung mit Anlage 1 Abschnitt I Nr. 1 SigV.