Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die

Signaturerstellungseinheit
ZKA Banking Signature Card, Version 7.6

der

Giesecke & Devrient GmbH

den nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93185.TU.03.2011

registriert.

Essen, 31.03.2011

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch die Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Die Bestätigung zur Registrierungsnummer TUVIT.93185.TU.03.2011 besteht aus 11 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang

Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.6 (nachfolgend auch ZBSC genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von NXP P5CC052V0A) mit Chipkartenbetriebssystem – Auslieferung per Sicherheitstransport – sowie die zur Fertigstellung der Signaturerstellungseinheit notwendige Initialisierungstabelle – Auslieferung verschlüsselt per E-Mail oder auf Datenträger.

Darüber hinaus wird folgende Dokumentation ausgeliefert:

- Administrator guidance ZKA Banking Signature Card V7.6 – Specific Part, version 1.4, 2011-03-10,
- Administrator guidance ZKA Banking Signature Card V7.x – Common Part, version 1.1, 2007-05-09,
- User Guidance ZKA Banking Signature Card V7.6, version 1.3, 2011-03-10,
- Generic Signature Application ZKA Banking Signature Card V7.6 – Specific Part, version 1.1, 2011-03-10,
- Generic Signature Application ZKA Banking Signature Card V7.x – Common Part, version 1.4, 2007-07-25,
- Installation, generation and start up, ZKA Banking Signature Card V7.6, version 1.4, 2011-03-10.

Hersteller:
Giesecke & Devrient GmbH
Prinzregentenstraße 159
81677 München

2 Funktionsbeschreibung

Die ZBSC ist bei Einhaltung aller dafür geltenden Bedingungen eine sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG (nachfolgend auch SSEE genannt). Die Einbringung der Initialisierungstabelle und die Erzeugung der Signaturschlüssel auf der ZBSC sowie die Ausstellung der qualifizierten Zertifikate und ggf. Einbringung in die ZBSC (Personalisierung) erfolgen durch einen Zertifizierungsdiensteanbieter.

Das Chipkartenbetriebssystem stellt die Kommandos der SECCOS-Spezifikation und darüber hinaus zusätzliche Kommandos der Bankenapplikationen wie beispielsweise Geldkarte und EMV zur Verfügung. Diese zusätzlichen Kommandos sind nicht Gegenstand dieser Bestätigung.

Die ZBSC stellt für sicherheitsrelevante Anwendungen Sicherheitsfunktionen zur Verfügung, die insbesondere die Authentifizierung, die sichere Datenspeicherung (insbesondere von Signaturschlüsseln und Identifikationsdaten), die Sicherung der Kommunikation zwischen einer (externen) Anwendung (hier: Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG oder technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12 SigG) und dem Betriebssystem sowie Kryptofunktionen zum Signieren von Daten – z. B. zur Bereitstellung einer elektronischen Signatur – umfassen.

Die ZBSC kann RSA-Schlüsselpaare mit Schlüssellängen von 1976 Bit bis 4000 Bit generieren und kann diese dann zur Signaturerzeugung verwenden. Die Signaturerzeugung erfolgt gemäß DIN V 66291-4 nach RSASSA-PKCS1-V1_5 mit SHA-256, SHA-384 oder SHA-512, nach RSASSA-PSS mit SHA-256, SHA-384 oder SHA-512 oder nach „DSI according to ISO/IEC 9796-2 with Random Number“ gemäß DIN V66291-4 mit RIPEMD160. Ferner stellt die ZBSC die Hash-Verfahren SHA-256, SHA-384 und SHA-512 bereit.

Das Filesystem der ZBSC und damit auch die Signaturapplikation werden durch die Initialisierungstabelle festgelegt. Die Initialisierungstabelle wird in der Vorpersonalisierungsphase geladen. Danach können keine weiteren Initialisierungstabellen geladen werden. Sicherheitsanforderungen an die Initialisierungstabelle sind in der o. g. Dokumentation enthalten. Die Signaturapplikation wird durch folgende Elemente charakterisiert:

1. Signaturschlüssel / Bedienungszähler

   Die Bitlänge des Modulus des Signaturschlüssels kann 1976 bis 4000 betragen. Der Signaturschlüssel ist im Filesystem unauslesbar gespeichert. Er wird nach Abschluss der Initialisierungsphase generiert und ist mit einer explizit zugeordneten Transport-PIN zur Sicherung der Nutzung dieses Schlüssels versehen.

   Die Anzahl der Signaturen, die mit dem Signaturschlüssel insgesamt erzeugt werden können, lässt sich durch einen (optionalen) Bedienungszähler auf einen Wert zwischen 1 und 4294967295 begrenzen. Der Bedienungszähler wird bei jeder Anwendung des Signaturschlüssels um eins erniedrigt. Die Anwendung des Signaturschlüssels wird permanent gesperrt, wenn der Bedienungszähler den Wert 0 erreicht. Danach können, auch nach erfolgreicher Authentifizierung mit der Signatur-PIN, keine Signaturen mehr erzeugt werden.

2. Transport-PIN

   Die dezimale Transport-PIN ist 5-stellig und besitzt einen Fehlbedienungszähler von 3. Bei abgelaufenem Fehlbedienungszähler ist die Inbetriebnahme der Signaturfunktionalität permanent gesperrt. Mit der Transport-PIN kann keine Signaturerstellung erfolgen, sie dient ausschließlich der Setzung einer Signatur-PIN. Die 5-stellige Transport-PIN muss vor der ersten Nutzung des Signaturschlüssels durch den Signaturschlüssel-Inhaber in eine Signatur-PIN (mindestens 6-stellig) geändert werden. Eine Rückkehr zu einer weniger als 6-stelligen PIN oder zu einer Transport-PIN ist danach nicht mehr möglich.

3. Signatur-PIN

   Die dezimale Signatur-PIN hat eine Mindestlänge von 6 und eine Maximallänge von 12 Stellen. Sie besitzt einen Fehlbedienungszähler von 3. Ein Wechsel der Signatur-PIN ist möglich. Bei abgelaufenem Fehlbedienungszähler ist die Signaturfunktionalität permanent gesperrt. Die Signatur-PIN ist ausschließlich dem Signaturschlüssel zugeordnet. Weitere Applikationen, wie z. B. eine Display Message, werden nicht durch die Signatur-PIN geschützt.

   Nach erfolgreicher Authentifizierung mit der Signatur-PIN kann je nach Konfiguration entweder eine genau definierte Anzahl von einer bis 254 oder eine beliebige Anzahl von Signaturen erzeugt werden (Multisignatur-SSEE). Sofern ein Bedienungszähler (siehe Punkt 1.) zusätzlich die Gesamtzahl der Signaturen des Signaturschlüssels begrenzt, können jedoch nicht mehr Signaturen, als durch den aktuellen Bedienungszähler noch möglich sind, erzeugt werden.

4. Resetting Code (PUK) der Signatur-PIN

   Die Signaturapplikation der ZBSC kann einen (optionalen) Resetting Code (PUK) zur Aufhebung der Blockade der PIN-Eingabe nach drei Fehlversuchen enthalten. Der dezimale PUK hat eine Mindestlänge von 8 und eine Maximallänge von 12 Stellen. Er besitzt einen Fehlbedienungszähler von maximal 3. Insgesamt ist die Anzahl der Anwendungen auf maximal 10 begrenzt. Ein Wechsel der PUK ist nicht möglich. Die Eingabe des PUK dient ausschließlich der Rücksetzung des Fehlbedienungszählers der Signatur-PIN, lässt jedoch keine Neusetzung der PIN zu.

5. Absicherung der Datenübertragung mit Secure Messaging

   Die Signaturapplikation der ZBSC vom „Typ C“ erlaubt optional eine Absicherung mit Secure Messaging für die Eingabe der PIN und Übertragung der zu signierenden Daten, während „Typ A“ für diese Datenübertragung kein Secure Messaging unterstützt.

6. Nachladen von Programmcode

   Die Signaturapplikation der ZBSC vom Typ „PIL“ erlaubt das mittels Secure Messaging gesicherte Nachladen von Programmcode. Das zur Absicherung des Kommandos benötigte Geheimnis wird im Rahmen der Personalisierung in die SSEE eingebracht.

Innerhalb der Initialisierungstabelle gibt es für die Signaturapplikation sechs Konfigurationsmöglichkeiten:

A. zur Schlüssellänge (1976 Bit bis maximal 4000 Bit),

B. zum Bedienungszähler (keiner oder 1 bis maximal 4294967295),

C. zur Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN (unbegrenzt oder 1 bis maximal 254),

D. zur Anzahl der PUK (0 oder 1) zur Aufhebung der Blockade der PIN-Eingabe,

E. zur Unterstützung von Secure Messaging zur Datenübertragung von PIN und zu signierenden Daten (Typ A: nein oder Typ C: optional) und

F. zum Nachladen von Programmcode (Typ „PIL“: ja, sonst: nein).

Jede Initialisierungstabelle muss vor Auslieferung dahingehend überprüft werden, dass die in der o. g. Dokumentation und die in dieser Bestätigung angegebenen Anforderungen an die möglichen Konfigurationen erfüllt sind. Im Rahmen dieser Bestätigung wurden die im Anhang genannten Initialisierungstabellen auf Erfüllung dieser Anforderungen überprüft. Zukünftig können weitere Initialisierungstabellen nach Überprüfung durch die Bestätigungsstelle in den Anhang zu dieser Bestätigung aufgenommen werden.

Das Verzeichnis (DF) für die Signaturapplikation selbst ist nach Einbringung der Initialisierungstabelle nicht löschbar. Es können auch innerhalb dieses Verzeichnisses weder vorhandene Datenfelder gelöscht noch neue Datenfelder angelegt werden. Insbesondere besteht nicht die Möglichkeit, die vorhandenen Datenfelder unbefugt zu manipulieren oder komplett auszutauschen.

Die ZBSC enthält Funktionen, die eine sichere Identifizierung als sichere Signaturerstellungseinheit im Sinne von § 5 Abs. 6 SigG ermöglichen. Die für diese Funktionen verwendeten Datenfelder zur Speicherung geheimer Daten können nicht ausgelesen, gelöscht oder manipuliert werden.

Die ZBSC enthält neben der Signaturapplikation mit dem Signaturschlüsselpaar für die qualifizierte elektronische Signatur weitere Applikationen mit weiteren Schlüsselpaaren und Daten, welche die Sicherheit der Signaturapplikation nicht beeinträchtigen. Diese zusätzlichen Applikationen selbst sind jedoch nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die ZBSC erfüllt in ihrer Ausprägung als SSEE die Anforderungen nach § 17 Abs. 1 (Signaturfälschungen und Verfälschung signierter Daten erkennbar, Schutz vor unberechtigter Nutzung des Signaturschlüssels) und Abs. 3 Nr. 1 SigG (Einmaligkeit und Geheimhaltung des Signaturschlüssels, keine Speicherung außerhalb der SSEE) sowie § 15 Abs. 1 (Signatur erst nach Identifikation, keine Preisgabe des Signaturschlüssels, Signaturschlüssel nicht aus Signaturprüf-schlüssel oder Signatur berechenbar, Signaturschlüssel nicht duplizierbar) und Abs. 4 SigV (sicherheitstechnische Veränderungen erkennbar).

3.2 Einsatzbedingungen

Diese Bestätigung gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Die der Bestätigung zugrunde liegende Prüfung der ZBSC ist in Verbindung mit dem Prozessor P5CC052V0A von NXP durchgeführt worden. Für diesen Prozessor liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0466-2008

vor. Der Prozessor ist vom Kartenhersteller unter Ausnutzung der zur Verfügung gestellten Sicherheitsfunktionalitäten in ein umfassendes Sicherheitssystem integriert worden.

Diese Bestätigung ist ohne Reevaluation nur mit dem Prozessor P5CC052V0A und mit dem Betriebssystem der ZBSC sowie mit dem in der Initialisierungstabelle enthaltenen EEPROM-Anteil des Betriebssystems „ZKA V1.04 LC“ gültig.

Die im Rahmen dieser Bestätigung überprüften Initialisierungstabellen sind im Anhang aufgeführt.

Die ZBSC ist nach der Vorpersonalisierung („Initialisation and Personalisation“ gemäß der o. g. Dokumentation „Administrator guidance ZKA Banking Signature Card V7.x – Common Part“ mit Einbringung einer Initialisierungstabelle und Signaturschlüsselerzeugung) so geschützt, dass eine Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem der ZBSC ist derart eingestellt, dass, bevor eine Aktion durchgeführt wird, die den geschützten Signaturschlüssel oder das zugehörige Passwort (PIN) nutzt, der Nachweis der Berechtigung zu einer solchen Aktion über eine Passwort-Eingabe obligatorisch ist. Dies betrifft alle (externen) Anwendungen zur Nutzung des Signaturschlüssels und zur Änderung des Passworts.

Die ZBSC muss vom Zertifizierungsdiensteanbieter vorpersonalisiert werden. Die Initialisierungstabelle wird in die Prozessorchipkarte eingebracht und das Signaturschlüsselpaar unter Anwendung der vom Betriebssystem der ZBSC angebotenen Schlüsselgenerierungsfunktion (unter Zuhilfenahme des physikalischen Zufallszahlengenerators des Chips P5CC052V0A der NXP Semiconductors Germany GmbH) erzeugt und in einem gesicherten Filesystem gespeichert. Zusätzlich werden die zur Authentifizierung benötigten Schlüssel und Geheimnisse sowie die Transport-PIN und PUK im Filesystem sicher gespeichert.

Vom Zertifizierungsdiensteanbieter sind die folgenden Bedingungen für die Vorpersonalisierung einzuhalten und die folgenden Anforderungen an das Sicherheitskonzept zu erfüllen:

- Die während der Vorpersonalisierung der ZBSC zur Authentifizierung benötigten Geheimnisse und Schlüssel sowie insbesondere auch die Transport-PIN und PUK sind sicher zu erzeugen und vertraulich zu halten.
- Der Zertifizierungsdiensteanbieter hat in seinem Sicherheitskonzept die Maßnahmen darzulegen, die sicherstellen, dass der Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit erzeugt wird.

b) Personalisierung

Die Personalisierung durch den Zertifizierungsdiensteanbieter umfasst das Lesen des öffentlichen Schlüssels von der SSEE, die Erstellung des qualifizierten Zertifikates und ggf. dessen Einbringung in die SSEE. Entwickler und Administratoren von (externen) Anwendungen müssen die folgenden Bedingungen einhalten:

- Bei der Entwicklung und Administration von (externen) Anwendungen für die Personalisierung und die Anwendung der SSEE ist stets zu gewährleisten, dass diese die Sicherheitsfunktionen des Betriebssystems der ZBSC sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind nicht Gegenstand dieser Bestätigung.

Die ZBSC muss vom Zertifizierungsdiensteanbieter personalisiert werden. Dabei sind die folgenden Bedingungen für die Personalisierung einzuhalten und die folgenden Anforderungen an das Sicherheitskonzept zu erfüllen:

- Die während der Personalisierung der ZBSC zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Der Zertifizierungsdiensteanbieter muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung der ZBSC erforderlich sind.

Ferner sind die folgenden Anforderungen für die Absicherung der Funktionalität zum Nachladen von Programmcode einzuhalten und im Sicherheitskonzept des Zertifizierungsdiensteanbieters zu berücksichtigen (Typ „PIL“):

- Das zur Absicherung des SECCOS-Kommandos zum Nachladen von Programmcode benötigte Geheimnis muss sicher vom Zertifizierungsdiensteanbieter generiert, in die SSEE eingebracht und verwahrt werden.
- Es darf nur authentischer Programmcode vom Hersteller Giesecke & Devrient GmbH unter Kontrolle des Zertifizierungsdiensteanbieters nachgeladen werden.
- Der Programmcode muss vor dem Nachladen evaluiert und nach SigG für die ZBSC (im Form eines Nachtrags zur dieser Bestätigung) bestätigt worden sein.
- Es dürfen nur neuere Versionen (Patch-Level) des Programmcodes nachgeladen werden.
- Das Nachladen von Programmcode darf keine Objekte, wie bspw. Signaturschlüssel, Bedienungszähler, Signatur-PIN und Fehlbedienungszähler der ZBSC korrumpieren. Insbesondere soll auch die Signaturfunktionalität des neuen Programmcodes unverändert sein.
- Vor dem Nachladen muss das Einverständnis des Signaturschlüssel-Inhabers vorliegen.

c) Nutzung als SSEE

Der Zertifizierungsdiensteanbieter ist verpflichtet, den Antragsteller über die besonderen Sicherheitsanforderungen für die Einsatzumgebung der SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit (Multisignatur-SSEE) im Rahmen des § 6 Abs. 1 SigG zu unterrichten.

Die Einsatzumgebung muss durch den Signaturschlüssel-Inhaber unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität der Multisignatur-SSEE und die Ausspähung der zugehörigen Identifikationsdaten (Signatur-PIN) sowie der PUK praktisch ausgeschlossen und damit die alleinige Kontrolle des Signaturschlüssel-Inhabers über den Prozess der Signaturerzeugung gegeben ist. In der Unterrichtung des Zertifizierungsdiensteanbieters gemäß § 6 Abs. 2 SigG soll in diesem Zusammenhang auf die Zurechnung einer qualifizierten elektronischen Signatur besonders hingewiesen werden.

Zu den physischen Sicherungsmaßnahmen gehört der Schutz gegen unbefugten Zugriff zur SSEE, insbesondere bei einem unbeaufsichtigten Betrieb.

Zu den logischen Sicherungsmaßnahmen gehören die Sicherstellung, dass ausschließlich bestätigte Produkte oder hinreichend geprüfte Produkte mit Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG zur Signaturanwendung eingesetzt werden sowie zusätzlich die folgenden Punkte:

- Ordnungsgemäße Installation des Produktes und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,
- regelmäßige Überprüfung der Integrität des Produktes und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur, falls der Einsatz der SSEE in einem IT-Netz erfolgt und
- vertrauenswürdige Anbindung an externe Kommunikationsnetze, falls die SSEE in einem IT-Netz mit Anbindung an externe Kommunikation eingesetzt wird.

Der Zertifizierungsdiensteanbieter sollte den Signaturschlüssel-Inhaber einer Multisignatur-SSEE darauf hinweisen, dass er bei Zweifeln an der ausreichenden Sicherheit seiner Einsatzumgebung eine anerkannte Prüf- und Bestätigungsstelle gemäß § 18 SigG kontaktieren möge.

Vom Signaturschlüssel-Inhaber ist ferner für den sachgemäßen Einsatz der SSEE zu beachten:

- Der Signaturschlüssel-Inhaber ist verpflichtet sich vor und regelmäßig während des Einsatzes einer Multisignatur-SSEE von der Wirksamkeit der getroffenen Sicherheitsmaßnahmen zu überzeugen.

- Der Signaturschlüssel ist vor seiner ersten Nutzung mit einer 5-stelligen Transport-PIN geschützt, mit der nur der Wechsel zu einer individuellen mindestens 6-stelligen Signatur-PIN möglich ist. Dieser Wechsel ist durch den Signaturschlüssel-Inhaber unverzüglich vorzunehmen, sobald er SSEE und Transport-PIN besitzt; hierbei hat er zu prüfen, ob die SSEE mit dieser 5-stelligen Transport-PIN geschützt ist, da nur dann sichergestellt werden kann, dass mit dem Signaturschlüssel noch keine Signaturen erzeugt wurden.
- Wird die SSEE als multifunktionale Karte eingesetzt, so ist die Signatur-PIN unterschiedlich zu den PINs der anderen Applikationen zu wählen.
- Das individuelle Identifikationsmerkmal Signatur-PIN muss vertraulich behandelt und darf nicht weitergegeben werden. Die Signatur-PIN muss unverzüglich geändert werden, wenn die Vermutung besteht, dass sie Dritten bekannt geworden sein könnte.
- Der PUK zur Aufhebung der Blockade der PIN-Eingabe ist vertraulich zu halten. Wenn die Vermutung besteht, dass der PUK Dritten bekannt geworden sein könnte, muss dieser durch dreimalige Fehleingabe unbrauchbar gemacht werden, da eine Änderung nicht möglich ist.
- Die SSEE muss verantwortungsvoll verwahrt und eingesetzt werden. Für den verantwortungsvollen Einsatz muss sich der Benutzer über die Signaturgesetzeskonformität der Einsatzumgebung vergewissern.
- Beschädigungen an der SSEE oder ein Funktionsversagen der SSEE können Hinweise auf eine Verletzung der Geheimhaltung von Schlüssel- oder Passwortdateien sein. In diesen Fällen ist unverzüglich mit dem zuständigen Zertifizierungsdiensteanbieter Kontakt aufzunehmen.

3.3 Algorithmen und zugehörige Parameter

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der ZBSC das RSA-Verfahren eingesetzt. Die möglichen Schlüssellängen (Modulus) betragen 1976 bis 4000 Bit. Die unterstützten Formatierungsverfahren (Padding) sind RSASSA-PSS und RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002 sowie „DSI according to ISO/IEC 9796-2 with Random Number“ nach DIN V66291-4.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für Mindestschlüssellängen von 1976 Bit bis Ende des Jahres 2017 (siehe BAnz. Nr. 17 vom 01.02.2011, Seite 383). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 ausschließlich für Zertifikats-signaturen noch bis Ende 2016 und sonst nur bis Ende 2014 geeignet ist.

Ferner werden zur Signaturerzeugung von der ZBSC die Hash-Verfahren SHA-256, SHA-384 und SHA-512 bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen reicht für SHA-256, SHA-384 sowie SHA-512 bis Ende des Jahres 2017 (siehe BAnz. Nr. 17 vom 01.02.2011, Seite 383).

Die Gültigkeit der Bestätigung der ZBSC in Abhängigkeit von Hash-Algorithmus, RSA-Mindestschlüssellänge und Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge Padding-Verfahren	SHA-256, SHA-384, SHA-512
1976 – 4000 RSASSA-PKCS1-V1_5	2014 (2016*)
1976 – 4000 RSASSA-PSS	2017
1976 – 4000 DSI according to ISO/IEC 9796-2 with Random Number	2017

*) Gültigkeit bis Ende 2016 ausschließlich für Zertifikatssignaturen

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der ZBSC ist somit, abhängig vom Hash-Verfahren, der Mindestschlüssellänge und dem Padding-Verfahren, maximal gültig bis 31.12.2017; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Die ZKA Banking Signature Card Version 7.6 wurde mit dem Prozessor P5CC052V0A erfolgreich nach der Prüfstufe **EAL4+** mit AVA_MSU.3 (vollständige Missbrauchsanalyse und AVA_VLA.4 (hohes Angriffspotential) der Common Criteria (CC) V2.3 evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Der Prozessor P5CC052V0A wurde erfolgreich nach der Prüfstufe **EAL5+** mit ALC_DVS.2, AVA_MSU.3 (vollständige Missbrauchsanalyse) und AVA_VLA.4 (hohes Angriffspotential) der CC V2.3 evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**. Hierfür liegen das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0466-2008 vom 25.06.2008 und der Assurance Continuity

Maintenance Report MA-01 vom 08.09.2009 sowie ein aktualisierter Prüfbericht („ETR for Composition“) vor.

Die sicherheitstechnisch korrekte Integration des Betriebssystems, der Initialisierungstabelle und des Prozessors zur ZBSC wurde überprüft. Gleichfalls geprüft wurde die sicherheitstechnisch korrekte Erzeugung und Speicherung des Signaturschlüssels in der Signaturapplikation der ZBSC.

Die für die SSEE nach SigV maßgebende Evaluierungsstufe **EAL4+** mit AVA_MSU.3 (vollständige Missbrauchsanalyse) und AVA_VLA.4 (hohes Angriffspotential) wird damit erreicht.

Anhang

Die folgende Initialisierungstabelle wurde im Rahmen dieser Bestätigung dahingehend überprüft, dass die Anforderungen aus der in Kapitel 1 genannten Dokumentation erfüllt sind:

- SDP6GE01E_0 (alternativ als geteilte Tabelle: E10 und E20).

  Diese beinhaltet jeweils eine Signaturapplikation mit einer Bitlänge des Signaturschlüssels (Modulus) von 2048, keinen Bedienungszähler für den Signaturschlüssel, genau eine Signaturerzeugung nach erfolgreicher PIN-Authentifizierung, keinen Resetting Code (PUK) für die Signatur-PIN, die optionale Unterstützung von Secure Messaging zur Datenübertragung von PIN und zu signierenden Daten (Typ C) und keine Möglichkeit zum Nachladen von Programmcode. Zusätzlich beinhaltet sie jeweils weitere Bankenapplikationen, die nicht Gegenstand dieser Bestätigung sind.

  Die Bestätigung der ZBSC mit dieser Initialisierungstabelle ist somit unter Maßgabe des Abschnitts 3.3 für die Signaturerzeugung mit SHA-256, SHA-384 sowie SHA-512 gültig bis 31.12.2014 bei Verwendung des Padding-Verfahrens RSASSA-PKCS1-V1_5 bzw. gültig bis 31.12.2016 bei Verwendung des Padding-Verfahrens RSASSA-PKCS1-V1_5 für Zertifikatssignaturen bzw. gültig bis 31.12.2017 bei Verwendung des Padding-Verfahrens RSASSA-PSS oder „DSI according to ISO/IEC 9796-2 with Random Number“.

Zukünftig können weitere Initialisierungstabellen nach Überprüfung durch die Bestätigungsstelle in diesen Anhang aufgenommen werden.

Ende der Bestätigung