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 6.51

der

Giesecke & Devrient GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93129.TU.03.2006

registriert.

Essen, 03.03.2006 **gez. Dr. Gruschwitz**
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) 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) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Die Bestätigung zur Registrierungsnummer TUVIT.93129.TU.03.2006 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.51 (nachfolgend auch ZBSC genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von Philips P5CD036V0M) mit Chipkartenbetriebssystem – Auslieferung per Kurier – sowie die zur Fertigstellung der Signaturerstellungseinheit notwendige Initialisierungstabelle – Auslieferung verschlüsselt per E-Mail oder auf Diskette.

Darüber hinaus wird folgende Dokumentation ausgeliefert:

- Administrator guidance ZKA Banking Signature Card V6.51, version 1.1, 2006-02-20,
- User Guidance ZKA Banking Signature Card V6.51, version 1.1, 2006-02-20,
- Generic Signature Application for ZKA Banking Signature Card V6.51 – Security Relevant Sections, version 1.0, 2006-02-07,
- Installation, generation and start-up ZKA Banking Signature Card V6.51, version 1.0, 2006-02-07.

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 beinhaltet die Kommandos der SECCOS-Spezifikation und darüber hinaus zusätzliche Kommandos der Bankenapplikationen wie beispielsweise Geldkarte und EMV. Diese zusätzlichen Kommandos sind **nicht** Gegenstand dieser Bestätigung.

Ferner besitzt die ZBSC ein kontaktloses Interface. Über dieses Interface kann weder eine Authentifizierung mit der Signatur-PIN erfolgen noch können Signaturen erzeugt werden.

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 zwischen 1024 Bit und 1984 Bit generieren und kann diese dann zur Signaturerzeugung verwenden. Die Signaturerzeugung erfolgt gemäß DIN V 66291-4 entweder nach PKCS#1 mit SHA-1 oder ISO/IEC 9796-2 unter Verwendung von Zufallszahlen mit RIPEMD160. Dazu werden von der ZKA Banking Signature Card die Hash-Verfahren SHA-1 und RIPEMD-160 bereitgestellt.

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 zwischen 1024 und 1984 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 Bedienungszähler auf einen Wert zwischen 1 und 65535 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 der Signaturschlüssel genau einmal zur Erzeugung von genau einer Signatur angewendet werden.

4. Resetting Code (PUK) der Signatur-PIN

   Die Signaturapplikation der ZBSC beinhaltet keinen Resetting Code (PUK).

Innerhalb der Initialisierungstabelle gibt es für die Signaturapplikation zwei Konfigurationsmöglichkeiten:

A. zur Schlüssellänge (1024 Bit bis maximal 1984 Bit) und

B. zum Bedienungszähler (keiner oder 1 bis maximal 65535).

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 Signaturprüfschlüssel 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 P5CD036V0M von Philips durchgeführt worden. Für diesen Prozessor liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0232-2004 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 P5CD036V0M und mit dem Betriebssystem der ZBSC sowie mit dem in der Initialisierungstabelle enthaltenen EEPROM-Anteil des Betriebssystem „Completion ZKA_1.21“ 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 V6.51“ 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 P5CD036V0M der Philips

Semiconductors GmbH) erzeugt und in einem gesicherten Filesystem gespeichert. Zusätzlich werden die zur Authentifizierung benötigten Schlüssel und Geheimnisse sowie die Transport-PIN 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 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.

Entwickler und Administratoren von (externen) Anwendungen müssen die oben genannten Bedingungen einhalten. 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.

c) Nutzung als SSEE

Der Zertifizierungsdiensteanbieter muss den Signaturschlüssel-Inhaber in der nach dem jeweils geltenden Recht vorgeschriebenen Form auf die Einhaltung der nachfolgenden Einsatzbedingungen hinweisen.

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

- 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.
- 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) liegen zwischen 1024 und 1984 Bit.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für Mindestschlüssellängen von 1728 Bit bis mindestens Ende des Jahres 2010, für Mindestschlüssellängen von 1536 Bit bis mindestens Ende des Jahres 2009, für Mindestschlüssellängen von 1280 Bit bis mindestens Ende des Jahres 2008 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Ferner werden zur Signaturerzeugung von der ZBSC die Hash-Verfahren SHA-1 und RIPEMD-160 bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen reicht bis mindestens Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Diese Bestätigung der ZBSC ist somit, abhängig von der Mindestschlüssellänge, maximal gültig bis 31.12.2010; 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.

Hinweis: Zur Zeit ist auf der Webseite der BNetzA die „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 02.01.2006“ eingestellt. Mit der Veröffentlichung dieser Bekanntmachung im Bundesanzeiger gemäß Anlage I Nr. 2 SigV wird die Eignung des Hash-Algorithmus SHA-1 zum Erzeugen von qualifizierten elektronischen Signaturen auf Ende des Jahres 2009 (anstelle von 2010) festgelegt.

3.4 Prüfstufe und Mechanismenstärke

Die ZKA Banking Signature Card, Version 6.51 wurde mit dem Prozessor P5CD036V0M erfolgreich nach der Prüfstufe **EAL4+** (mit Zusatz AVA_MSU.3 und AVA_VLA.4) der Common Criteria (CC) evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Der Prozessor P5CD036V0M wurde erfolgreich nach der Prüfstufe **EAL5+** (mit Zusatz: ALC_DVS.2, AVA_MSU.3 und AVA_VLA.4) der CC evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0232-2004 vom 08.09.2004 mit Assurance Continuity Maintenance Report MA-01 vom 14.03.2005 vor.

Die sicherheitstechnisch korrekte Integration des Betriebssystems, der Initialisierungstabelle und des Prozessors zur ZBSC wurde im Rahmen der Evaluierung 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 Zusatz: AVA_MSU.3 und AVA_VLA.4) und die Stärke der Sicherheitsfunktionen **hoch** sind damit erreicht.

Für die ZKA Banking Signature Card, Version 6.51 liegt zusätzlich das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-9245-2005 vom 08.09.2005 vor.

Anhang

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

- SWP3G5J0E_1 (alternativ als geteilte Tabelle: E11 und E21)

  Diese beinhaltet eine Signaturapplikation mit einer Bitlänge des Signaturschlüssels (Modulus) von 1728 und einen Bedienungszähler für den Signaturschlüssel von 65535 und keinen Resetting Code (PUK) für die Signatur-PIN. Zusätzlich beinhaltet sie weitere Bankenapplikationen, die **nicht** Gegenstand dieser Bestätigung sind.

  Die Bestätigung der ZBSC mit dieser Initialisierungstabelle ist somit unter Maßgabe des Abschnitts 3.3 gültig bis 31.12.2010 bzw. nach Veröffentlichung der neuen Bekanntmachung im Bundesanzeiger bei Verwendung des Hash-Verfahrens SHA-1 bis 31.09.2009.

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

Ende der Bestätigung