

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 Signaturgesetz¹ sowie § 11 Abs. 3 Signaturverordnung²,
dass die

Signaturerstellungseinheit
ZKA-Signaturkarte, Version 6
der
Gemalto GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93143.TE.11.2007

registriert.

Essen, 06.11.2007

gez. Dr. Sutter

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 26.02.2007 (BGBl. I S. 179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch Artikel 2 des Gesetzes vom 04.01.2005 (BGBl. I S. 2)

Die Bestätigung zur Registrierungsnummer TUVIT.93143.TE.11.2007 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturerstellungseinheit ZKA-Signaturkarte, Version 6
(nachfolgend auch ZKA-SK genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von Infineon SLE66CX680PE / m1534a13) 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 Signaturecard, version 1.2, 2007-09-25,
- User Guidance – ZKA SignatureCard, version 1.2, 2007-09-18,
- Life Cycle Description for DigSig Confirmation – ZKA Signature Card, version 1.0, 2007-06-29.

Hersteller:

Gemalto GmbH
Adalperostraße 45
85737 Ismaning

2 Funktionsbeschreibung

Die ZKA-SK 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 ZKA-SK sowie die Ausstellung der qualifizierten Zertifikate und ggf. Einbringung in die ZKA-SK (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 ZKA-SK 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 ZKA-SK kann RSA-Schlüsselpaare mit Schlüssellängen von 1024 Bit bis 2048 Bit generieren und kann diese dann zur Signaturerzeugung verwenden (Option b gemäß der oben genannten Dokumentation und des Security Targets). Der Import des Signaturschlüsselpaares von einem externen Schlüsselgenerator (Option a) fällt nicht unter diese Bestätigung.

Die Signaturerzeugung erfolgt entweder nach PKCS#1-V15 und PKCS#1-PSS mit SHA-1, SHA-256, SHA-384 oder SHA-512 oder nach ISO/IEC 9796-2 unter Verwendung von Zufallszahlen mit RIPEMD-160. Die Berechnung des Hashwertes erfolgt entweder:

- a. vollständig durch eine Signaturanwendungskomponente oder eine technische Komponente für Zertifizierungsdienste,
- b. vollständig durch die ZKA-SK oder
- c. teilweise durch ZKA-SK indem die letzte Runde der Berechnung des Hashwertes durch die ZKA-SK durchgeführt wird.

Für die Fälle b. und c. stellt die ZKA-SK die Hash-Verfahren SHA-1, SHA-256, SHA-384, SHA-512 und RIPEMD-160 bereit.

Das Filesystem der ZKA-SK und damit auch die Signaturapplikation werden durch die Initialisierungstabelle festgelegt. Die Initialisierungstabelle wird in der Vorphase 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 1024 bis 2048 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 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 Fehlbedienungsähler von 3. Ein Wechsel der Signatur-PIN ist möglich. Bei abgelaufenem Fehlbedienungsähler 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 ZKA-SK beinhaltet keinen Resetting Code (PUK).

Innerhalb der Initialisierungstabelle gibt es für die Signaturapplikation zwei Konfigurationsmöglichkeiten:

- A. zur Schlüssellänge (1024 Bit bis maximal 2048 Bit) und
- B. zum Bedienungsähler (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 löscherbar. 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 ZKA-SK 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 ZKA-SK erlaubt optional eine Absicherung mit Secure Messaging für die Eingabe der PIN und Übertragung der zu signierenden Daten.

Die ZKA-SK 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 ZKA-SK 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 ZKA-SK ist in Verbindung mit dem Prozessor SLE66CX680PE / m1534a13 von Infineon durchgeführt worden. Für diesen Prozessor liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0322-2005 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 SLE66CX680PE / m1534a13 und mit dem Betriebssystem der ZKA-SK sowie mit dem in der Initialisierungstabelle enthaltenen EEPROM-Anteil des Betriebssystems „G167_FILT003“ gültig.

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

Die ZKA-SK ist nach der Vorphersonalisierung („Card initialization / Phase 5“ und „Card personalization / Phase 6“) gemäß der o.g. Dokumentation „Administrator guidance – ZKA Signaturecard“ mit Einbringung einer Initialisierungstabelle und Signaturschlüsselerzeugung) so geschützt, dass eine Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem der ZKA-SK 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 ZKA-SK muss vom Zertifizierungsdiensteanbieter vorphersonalisiert werden. Die Initialisierungstabelle wird in die Prozessorchipkarte eingebracht und das Signaturschlüsselpaar unter Anwendung der vom Betriebssystem der ZKA-SK angebotenen Schlüsselgenerierungsfunktion 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 ZKA-SK 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 ZKA-SK, die Erstellung des qualifizierten Zertifikates und ggf. dessen Einbringung in die ZKA-SK. 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 ZKA-SK ist stets zu gewährleisten, dass diese die Sicherheitsfunktionen des Betriebssystems der ZKA-SK sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind **nicht** Gegenstand dieser Bestätigung.

Die ZKA-SK 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 ZKA-SK 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 ZKA-SK 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.
- 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 ZKA-SK das RSA-Verfahren eingesetzt. Die möglichen Schlüssellängen (Modulus) betragen 1024 bis 2048 Bit.

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 2012, für Mindestschlüssellängen von 1728 Bit bis Ende des Jahres 2010, für Mindestschlüssellängen von 1536 Bit bis Ende des Jahres 2009, für Mindestschlüssellängen von 1280 Bit bis Ende des Jahres 2008 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Ferner werden zur Signaturerzeugung von der ZKA-SK die Hash-Verfahren SHA-1, SHA-256, SHA-384, SHA-512 und RIPEMD-160 bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen reicht für SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010), für RIPEMD-160 bis Ende des Jahres 2010 und für SHA-256 SHA-384 sowie SHA-512 bis Ende des Jahres 2012 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die Gültigkeit der Bestätigung der ZKA-SK in Abhängigkeit von Hash-Algorithmus und RSA-Mindestschlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus Schlüssellänge	SHA-1	RIPEMD-160, SHA-1 bei Anwendung bei qualifizierten Zertifikaten	SHA-256, SHA-384, SHA-512
1024	2007	2007	2007
1280	2008	2008	2008
1536	2009	2009	2009
1728	2009	2010	2010
1976	2009	2010	2012

Diese Bestätigung der ZKA-SK ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, maximal gültig bis 31.12.2012; 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-Signaturkarte Version 6 wurde mit dem Prozessor SLE66CX680PE / m1534a13 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 SLE66CX680PE / m1534a13 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-0322-2005 vom 14.09.2005 vor.

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

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.

Anhang

Die folgenden Initialisierungstabellen wurden im Rahmen dieser Bestätigung dahingehend überprüft, dass die Anforderungen aus der in Kapitel 1 genannten Dokumentation erfüllt sind:

- SDI3P801.E_0 und SWI3P821.E_0

Diese beinhalten jeweils eine Signaturapplikation mit einer Bitlänge des Signaturschlüssels (Modulus) von 2048, keinen Bedienungszähler für den Signaturschlüssel und keinen Resetting Code (PUK) für die Signatur-PIN. Zusätzlich beinhalten sie weitere Applikationen, die **nicht** Gegenstand dieser Bestätigung sind.

Die Bestätigung der ZKA-SK mit diesen Initialisierungstabellen ist somit unter Maßgabe des Abschnitts 3.3 für die Signaturerzeugung mit SHA-1 gültig bis 31.12.2009, für die Signaturerzeugung mit RIPEMD-160 sowie mit SHA-1 zur Anwendung bei qualifizierten Zertifikaten gültig bis 31.12.2010 und für die Signaturerzeugung mit SHA-256, SHA-384 und SHA-512 gültig bis 31.12.2012.

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

Ende der Bestätigung