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-Signaturkarte, Version 6.32 M

der

Gemalto GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93176.TU.05.2011

registriert.

Essen, 19.05.2011

Joachim Faulhaber
stellv. 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.93176.TU.05.2011 besteht aus 10 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang

Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M
(nachfolgend auch ZKA-SK genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von STMicroelectronics ST23ZL48A (ASD, Maske K320ACA)) mit Chipkartenbetriebssystem – Auslieferung per Kurier – 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 Signaturecard 6.32M, version 1.1, 2011-03-16,
- User guidance – ZKA Signaturecard 6.32 M, version 1.1, 2011-03-16,
- Life Cycle Description for DigSig Confirmation – ZKA Signaturecard 6.32 M, version 1.0 2011-02-14.

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 1976 Bit bis 2048 Bit auf der SSEE 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 nach RSASSA-PKCS1-V1_5 und RSASSA-PSS mit SHA-256, SHA-384 oder SHA-512. 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-256, SHA-384 und SHA-512 bereit.

Das Filesystem der ZKA-SK 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 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 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 eine beliebige Anzahl von Signaturen erzeugt werden (Multisignatur-SSEE).

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 (1976 Bit bis maximal 2048 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 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 stellt das SECCOS-Kommando zur Verfügung, mit dem der Zertifizierungsdiensteanbieter mittels Secure Messaging gesichert Programmcode nachladen kann. Das zur Absicherung des Kommandos benötigte Geheimnis wird im Rahmen der Personalisierung in die SSEE eingebracht.

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 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 ZKA-SK ist in Verbindung mit dem Prozessor ST23ZL48A (ASD, Maske K320ACA) von STMicroelectronics durchgeführt worden. Für diesen Prozessor liegt das IT-Sicherheitszertifikat ANSSI-CC-2010/07 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 ST23ZL48A (ASD, Maske K320ACA) und mit dem SECCOS Betriebssystem der ZKA-SK sowie mit dem in der Initialisierungstabelle enthaltenen EEPROM-Anteil des Betriebssystems „STM011_FILT002“ gültig.

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

Die ZKA-SK ist nach der Vorpersonalisierung („Card initialization / Phase 5“ und „Card personalization / Phase 6“) gemäß der o. g. Dokumentation „Administrator guidance – ZKA Signaturecard 6.32M“ 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 vorpersonalisiert 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.

Ferner sind die folgenden Anforderungen für die Absicherung der Funktionalität zum Nachladen von Programmcode einzuhalten und im Sicherheitskonzept des Zertifizierungsdiensteanbieters zu berücksichtigen:

- Das zur Absicherung des SECCOS-Kommandos zum Nachladen von Programmcode benötigte Geheimnis muss sicher vom Zertifizierungs-diensteanbieter generiert, in die SSEE eingebracht und verwahrt werden.

- Es darf nur authentischer Programmcode vom Hersteller Gemalto GmbH unter Kontrolle des Zertifizierungsdiensteanbieters nachgeladen werden.
- Der Programmcode muss vor dem Nachladen evaluiert und nach SigG für die ZKA-SK (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 ZKA-SK korrumpieren. Insbesondere soll auch die Signaturfunktionalität des neuen Programmcodes identisch zu vorliegenden ZKA-SK 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 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 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.
- 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 1976 bis 2048 Bit. Die unterstützten Formatierungsverfahren (Padding) sind RSASSA-PSS und RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

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 ZKA-SK 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 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 ZKA-SK in Abhängigkeit von Hash-Algorithmus und RSA-Mindestschlüssellänge und Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / **Schlüssellänge Padding-Verfahren**	**SHA-256, SHA-384, SHA-512**
1976 – 2048 RSASSA-PKCS1-V1_5	**2014 (2016*)**
1976 – 2048 RSASSA-PSS	**2017**

*) Gültigkeit bis Ende 2016 ausschließlich für Zertifikatssignaturen

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

Diese Bestätigung der ZKA-SK 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-Signaturkarte Version 6.32 M wurde mit dem Prozessor ST23ZL48A (ASD, Maske K320ACA) erfolgreich nach der Prüfstufe **EAL4+** mit AVA_MSU.3 (vollständige Missbrauchsanalyse) und AVA_VLA.4 (hohes Angriffspotential) der Common Criteria (CC) V2.3 evaluiert.

Der Prozessor ST23ZL48A (ASD, Maske K320ACA) wurde erfolgreich nach der Prüfstufe **EAL5+** mit ALC_DVS.2 und AVA_VAN.5 (hohes Angriffpotential einschließlich Missbrauchsanalyse) der CC V3.1 evaluiert. Hierfür liegt das IT-Sicherheitszertifikat ANSSI-CC-2010/07 vom 08.03.2010 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 Prüfstufe **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:

- SSS0PC50.E_0

  Diese beinhaltet eine Signaturapplikation mit einer Bitlänge des Signaturschlüssels (Modulus) von 2048, keinen Bedienungszähler für den Signaturschlüssel sowie eine unbegrenzte Anzahl von Signaturerzeugungen nach erfolgreicher PIN-Authentifizierung (Multisignatur-SSEE) und keinen Resetting Code (PUK) für die Signatur-PIN. Zusätzlich beinhaltet sie weitere Applikationen, die nicht Gegenstand dieser Bestätigung sind.

  Die Bestätigung der ZKA-SK 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.

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

Ende der Bestätigung

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

Nachtrag 1 zur Bestätigung TUVIT.93176.TU.05.2011 vom 19.05.2011

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

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

Signaturerstellungseinheit
ZKA-Signaturkarte, Version 6.32 M
der
Gemalto GmbH

nach einer erneuten Bewertung der Schwachstellen ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen des Kapitels 1, des Abschnittes 3.3 und des Anhangs beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 17.06.2013 festgehalten.

Essen, 17.06.2013

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)

Dieser Nachtrag zur Bestätigung TUVIT.93176.TU.05.2011 besteht aus 4 Seiten.

1 Handelsbezeichnung des Produktes und Lieferumfang

Dieses Kapitel „1 Handelsbezeichnung des Produktes und Lieferumfang“ ersetzt das Kapitel 1 der Bestätigung TUVIT.93176.TU.05.2011 vom 19.05.2011 aufgrund der geänderten Adresse der Gemalto GmbH.

Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M
(nachfolgend auch ZKA-SK genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von STMicroelectronics ST23ZL48A (ASD, Maske K320ACA)) mit Chipkarten-betriebssystem – Auslieferung per Kurier – 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 Signaturecard 6.32M, version 1.1, 2011-03-16,
- User guidance – ZKA Signaturecard 6.32 M, version 1.1, 2011-03-16,
- Life Cycle Description for DigSig Confirmation – ZKA Signaturecard 6.32 M, version 1.0 2011-02-14.

Hersteller:
Gemalto GmbH
St.-Martin-Straße 60
81541 München

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93176.TU.05.2011 vom 19.05.2011 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger AT 27.03.2013 B4.

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der ZKA-SK das RSA-Verfahren eingesetzt. Die möglichen Schlüssellängen (Modulus) betragen 1976 bis 2048 Bit. Die unterstützten Formatierungsverfahren (Padding) sind RSASSA-PSS und RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

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 2019 (siehe BAnz. AT 27.03.2013 B4). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 ausschließlich für Zertifikats-signaturen noch bis Ende 2017 und sonst nur bis Ende 2015 geeignet ist.

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

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hash-Algorithmen SHA-256, SHA-384 sowie SHA-512 bis Ende des Jahres 2019 (siehe BAnz. AT 27.03.2013 B4).

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

Hash-Algorithmus / Schlüssellänge Padding-Verfahren	SHA-256, SHA-384, SHA-512
1976 – 2048 RSASSA-PKCS1-V1_5	2015 (2017*)
1976 – 2048 RSASSA-PSS	2019

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen

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

Diese Bestätigung der ZKA-SK ist somit, abhängig vom Hash-Verfahren, der Mindestschlüssellänge und dem Padding-Verfahren, maximal gültig bis 31.12.2019; 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.

Anhang zur Bestätigung TUVIT.93176.TU.05.2011

Dieser Anhang ersetzt den Anhang zur Bestätigung TUVIT.93176.TU.05.2011 vom 19.05.2011 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger AT 27.03.2013 B4.

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

- SSS0PC50.E_0

  Diese beinhaltet eine Signaturapplikation mit einer Bitlänge des Signaturschlüssels (Modulus) von 2048, keinen Bedienungszähler für den Signaturschlüssel sowie eine unbegrenzte Anzahl von Signaturerzeugungen nach erfolgreicher PIN-Authentifizierung (Multisignatur-SSEE) und keinen Resetting Code (PUK) für die Signatur-PIN. Zusätzlich beinhaltet sie weitere Applikationen, die nicht Gegenstand dieser Bestätigung sind.

  Die Bestätigung der ZKA-SK mit dieser Initialisierungstabelle ist somit unter Maßgabe des Abschnitts 3.3 für die Signaturerzeugung mit SHA-256, SHA-384 sowie SHA-512 gültig bis 31.12.2015 bei Verwendung des Padding-Verfahrens RSASSA-PKCS1-V1_5 bzw. gültig bis 31.12.2017 bei Verwendung des Padding-Verfahrens RSASSA-PKCS1-V1_5 für Zertifikatssignaturen bzw. gültig bis 31.12.2019 bei Verwendung des Padding-Verfahrens RSASSA-PSS.

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

Ende der Bestätigung