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
STARCOS 3.0
with Electronic Signature Application V3.0, Type 3B

der

Giesecke & Devrient GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.09399.TE.10.2005

registriert.

Essen, 21.10.2005 **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.09399.TE.10.2005 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

STARCOS 3.0 with Electronic Signature Application V3.0, Type 3B (nachfolgend auch STARCOS_ESA genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von Philips P5CC072V0M) 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 STARCOS 3.0 with EU compliant Electronic Signature Application V3.0 Type 3, version 1.3, 2005-09-13,
- User Guidance STARCOS 3.0 with EU compliant Electronic Signature Application V3.0 (Type2+3), version 1.0, 2005-09-13
- Generic Signature Application STARCOS 3.0 with EU compliant Electronic Signature Application, version 0.8, 2005-09-13,
- Installation, generation and start up STARCOS 3.0, Type 3, version 1.2, 2005-09-13.

Hersteller:
Giesecke & Devrient GmbH
Prinzregentenstraße 159
81677 München

2 Funktionsbeschreibung

STARCOS_ESA 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 STARCOS_ESA sowie die Ausstellung und ggf. Einbringung (Personalisierung) der qualifizierten Zertifikate erfolgen durch einen Zertifizierungsdiensteanbieter.

STARCOS_ESA 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.

STARCOS_ESA kann RSA-Schlüsselpaare mit Schlüssellängen von 1024 Bit bis 1976 Bit generieren und diese dann zur Signaturerzeugung verwenden. Die Signaturerzeugung erfolgt gemäß DIN V 66291-4 entweder nach PKCS#1 oder nach ISO/IEC 9796-2 unter Verwendung von Zufallszahlen mit jeweils SHA-1 oder RIPEMD-160. Ferner stellt STARCOS_ESA die Hash-Verfahren SHA-1 und RIPEMD-160 bereit.

Das initiale Filesystem der STARCOS_ESA 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 der Signaturschlüssel kann 1024 bis 1976 betragen. Es können maximal 8 unterschiedliche Signaturschlüssel generiert und im Filesystem unauslesbar gespeichert werden. Sie werden in der Vorpersonalisierungs- oder Personalisierungsphase generiert und sind mit jeweils einer explizit zugeordneten (individuellen) Transport-PIN zur Sicherung der Nutzung des jeweiligen Schlüssels versehen.

   Die Anzahl der Signaturen, die mit einem Signaturschlüssel insgesamt erzeugt werden können, lässt sich durch einen Bedienungszähler auf einen Wert zwischen 1 und 65535 begrenzen. Der dem jeweiligen Signaturschlüssel zugeordnete 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

   Jedem Signaturschlüssel ist eine individuelle Transport-PIN zugeordnet. Die 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 Signatur-PIN hat einen Mindestlänge von 6 Stellen und besteht entweder aus dezimalen Ziffern mit einer Maximallänge von 12 Stellen oder aus ASCII-Zeichen mit einer Maximallänge von 8 Stellen. Die Signatur-PIN besitzt in beiden Fällen 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 jeweiligen 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 65535 oder eine beliebige Anzahl von Signaturen erzeugt werden. Sofern ein Bedienungszähler (siehe 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

   STARCOS_ESA beinhaltet keinen Resetting Code (PUK).

Innerhalb der Initialisierungstabelle gibt es für die Signaturapplikation fünf Konfigurationsmöglichkeiten:

A. zur Schlüssellänge (1024 Bit bis maximal 1976 Bit)

B. zur Anzahl der Signaturschlüssel (1 bis maximal 8)

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

D. zum Format der Signatur-PIN (dezimal mit maximal 12 Stellen oder ASCII mit maximal 8 Stellen)

E. zur Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN (unbegrenzt 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. Durch den Zertifizierungsdiensteanbieter können innerhalb dieses Verzeichnisses weitere Datenfelder (EF) und DF angelegt sowie einzelne EF ergänzt werden. Diese Erweiterungen und Ergänzungen durch den Zertifizierungsdiensteanbieter sind nicht Gegenstand dieser Bestätigung. Sie müssen die im Dokument *Generic Signature Application* (siehe Kapitel 1) enthaltenen Anforderungen erfüllen und dürfen insbesondere nicht die Signatur-PIN verwenden.

STARCOS_ESA 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.

STARCOS_ESA erzwingt eine Absicherung mit Secure Messaging für die Eingabe der PIN und Übertragung der zu signierenden Daten.

STARCOS_ESA kann neben der Signaturapplikation mit maximal 8 Signaturschlüsselpaaren für die qualifizierte elektronische Signatur weitere Applikationen mit weiteren Schlüsselpaaren und Daten enthalten, welche die Sicherheit der

Signaturapplikation nicht beeinträchtigen. Diese zusätzlichen Applikationen sind jedoch **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

STARCOS_ESA 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 von STARCOS_ESA ist in Verbindung mit dem Prozessor P5CC072V0M von Philips durchgeführt worden. Für diesen Prozessor liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0227-2004 vor. Der Prozessor ist vom Kartenhersteller unter Ausnutzung der zur Verfügung gestellten Sicherheitsfunktionalitäten in ein umfassendes Sicherheitssystem integriert worden.

Das kontaktlose Interface ist beim vorliegenden Prozessor P5CC072V0M von Philips so deaktiviert, dass keine Datenübertragung über dieses Interface erfolgen kann. Insbesondere können mit dem kontaktlosen Interface weder eine Authentifizierung mit der Transport- bzw. Signatur-PIN durchgeführt noch Signaturen erzeugt werden.

Diese Bestätigung ist ohne Reevaluation nur mit dem Prozessor P5CC072V0M und mit dem Betriebssystem von STARCOS_ESA sowie mit dem in den Initialisierungstabellen enthaltenen EEPROM-Anteil des Betriebssystems „BLD_CPAZ0SCSI30-01A-0V410“ gültig.

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

STARCOS_ESA ist nach der Vorpersonalisierung („Initialisation and Personalisation“ gemäß der o. g. Dokumentation „Administrator Guidance STARCOS 3.0“ mit Einbringung einer Initialisierungstabelle und Signaturschlüsselerzeugung) so geschützt, dass eine Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem von STARCOS_ESA 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.

STARCOS_ESA muss vom Zertifizierungsdiensteanbieter vorpersonalisiert werden. Die Initialisierungstabelle wird in die Prozessorchipkarte eingebracht und die Signaturschlüsselpaare unter Anwendung der vom Betriebssystem von STARCOS_ESA angebotenen Schlüsselgenerierungsfunktion (unter Zuhilfenahme des physikalischen Zufallszahlengenerators des Chips P5CC072V0M der Philips Semiconductors GmbH) erzeugt und in einem gesicherten Filesystem gespeichert. Zusätzlich werden die zur Authentifizierung benötigten Schlüssel und Geheimnisse im Filesystem sicher gespeichert. In der Personalisierungsphase können später weitere Signaturschlüsselpaare erzeugt werden.

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

- Die während der Vorpersonalisierung von STARCOS_ESA zur Authentifizierung benötigten Geheimnisse und Schlüssel sowie insbesondere auch die Transport-PINs sind sicher zu erzeugen und vertraulich zu halten.
- Sofern in der Initialisierungstabelle Daten-Felder (EF_RCD, EF_RCZ, EF_RC) für den PUK angelegt sind, dürfen diese nicht belegt werden, damit die PUK-Funktionalität deaktiviert bleibt.
- Der Zertifizierungsdiensteanbieter hat in seinem Sicherheitskonzept die Maßnahmen darzulegen, die sicherstellen, dass während der Vorpersonalisierung Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit erzeugt werden.

b) Personalisierung

Die Personalisierung durch den Zertifizierungsdiensteanbieter umfasst die Generierung weiterer Signaturschlüssel (optional), das Lesen eines oder mehrerer öffentlicher Schlüssel von der SSEE, die Erstellung eines oder mehrerer qualifizierten Zertifikate und ggf. deren 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 von STARCOS_ESA 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.

STARCOS_ESA 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 von STARCOS_ESA zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Der Zertifizierungsdiensteanbieter hat in seinem Sicherheitskonzept die Maßnahmen darzulegen, die sicherstellen, dass während der Personalisierung weitere Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit erzeugt werden.
- Der Zertifizierungsdiensteanbieter muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung von STARCOS_ESA erforderlich sind. Insbesondere ist sicherzustellen, dass alle Signaturschlüssel einer SSEE stets demselben Signaturschlüsselinhaber (durch qualifizierte Zertifikate) zugeordnet werden.
- Sofern die Signaturapplikation von STARCOS_ESA mehr als einen Signaturschlüssel enthält, ist das folgende Auslieferungsverfahren einzuhalten: alle Signaturschlüssel, zugehörigen qualifizierten Zertifikate und Transport-PINs sind vom Zertifizierungsdiensteanbieter vor Ausgabe der SSEE an den Antragsteller zu generieren und an diesen gemäß § 5(2) SigV zu übergeben. Zukünftig können bei Bedarf weitere Auslieferungsverfahren nach Überprüfung durch die Bestätigungsstelle in Nachträge zu dieser Bestätigung aufgenommen werden.

c) Nutzung als SSEE

Der Zertifizierungsdiensteanbieter hat beim Anlegen bzw. Ergänzen von Datenfeldern und Verzeichnissen die im Dokument *Generic Signature Application* (siehe Kapitel 1) enthaltenen Anforderungen zu erfüllen. Hierbei darf insbesondere die Signatur-PIN nicht verwendet werden.

Der Zertifizierungsdiensteanbieter ist verpflichtet, die SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit nach erfolgreicher Authentifizierung (Multisignatur-SSEE) ausschließlich persönlich an Antragsteller zu übergeben und diese auch über die besonderen Sicherheitsanforderungen für die Einsatzumgebung zu unterrichten. Diese Multisignatur-SSEE darf ausschließlich in einer besonders gesicherten Umgebung (z. B. in einem Trust Center) und in Verbindung mit hinreichend geprüften Signaturanwendungskomponenten eingesetzt werden.

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

- Jeder 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. Sofern die SSEE mehrere Signaturschlüssel enthält, so sind die Signatur-PINs für alle Signaturschlüssel unterschiedlich zu wählen.
- 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 Signaturschlüssel-Inhaber 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

Bei der Erzeugung einer qualifizierten elektronischen Signatur wird von STARCOS_ESA das RSA-Verfahren eingesetzt. Die möglichen Schlüssellängen (Modulus) betragen 1024 bis 1976 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 STARCOS_ESA 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 STARCOS_ESA ist somit, abhängig von Mindestschlüssellänge, maximal gültig bis 31.12.2010; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

STARCOS_ESA wurde mit dem Prozessor P5CC072V0M 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 P5CC072V0M 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-0227-2004 vom 16.09.2004 mit Assurance Continuity Maintenance Report MA-01 vom 14.03.2005 vor.

Die sicherheitstechnisch korrekte Integration des Betriebssystems, der Initialisierungstabelle und des Prozessors zu STARCOS_ESA wurde überprüft. Gleichfalls geprüft wurde im Rahmen der Evaluierung die sicherheitstechnisch korrekte Erzeugung und Speicherung der Signaturschlüssel in der Signaturapplikation von STARCOS_ESA.

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 STARCOS_ESA liegt zusätzlich das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-CC-9232-2005 vom 16.09.2005 vor. Ferner ist STARCOS_ESA konform zum vom BSI unter BSI-PP-0006-2002 zertifizierten Schutzprofil *Protection Profile – Secure Signature-Creation Device Type 3*, Version 1.05, 25.07.2001.

Anhang

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

- TypB_S-Conf5_V

  Diese beinhaltet eine Signaturapplikation mit drei Signaturschlüsseln der Längen 1024, 1536 und 1976 Bit, keinen Bedienungszähler, drei 6-12-stelligen dezimale Signatur-PINs sowie genau einer Signaturerzeugung nach erfolgreicher PIN-Authentifizierung.

  Die Bestätigung der STARCOS_ESA mit dieser Initialisierungstabelle ist somit für die Schlüssellänge 1024 Bit gültig bis 31.12.2007, für die Schlüssellänge 1536 gültig bis 31.12.2009 und für die Schlüssellänge 1976 Bit gültig bis 31.12.2010.

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

Ende der Bestätigung