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 3.1 ECC with EU compliant Electronic Signature Application V4.0, Version 2.0

der

Giesecke & Devrient GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93118.TU.01.2006

registriert.

Essen, 30.01.2006

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.93118.TU.01.2006 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturerstellungseinheit STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, Version 2.0 (nachfolgend auch STARCOS 3.1 ECC genannt)

Auslieferung:

an Zertifizierungsdiensteanbieter

Der Auslieferungsumfang umfasst den Prozessorchip (Prozessor von Infineon SLE66CX360PE / m1536a13) 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 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.3, 2006-01-09,
- User Guidance STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.6, 2006-01-09,
- Generic Signature Application STARCOS 3.1 ECC with EU compliant Electronic Signature Application, version 1.3, 2005-12-20,
- Installation, generation and start-up STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.0, 2005-06-22.

Hersteller:
Giesecke & Devrient GmbH
Prinzregentenstraße 159
81677 München

2 Funktionsbeschreibung

STARCOS 3.1 ECC 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 des Signaturschlüssels auf STARCOS 3.1 ECC sowie die Ausstellung des qualifizierten Zertifikates und ggf. Einbringung in STARCOS 3.1 ECC (Personalisierung) erfolgen durch einen Zertifizierungsdiensteanbieter.

STARCOS 3.1 ECC 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 3.1 ECC kann Schlüssel für drei festgelegte elliptische Kurven mit Schlüssellängen von 192, 224 und 256 Bit erzeugen und diese dann zur Signaturerzeugung verwenden. Ferner stellt STARCOS 3.1 ECC die Hash-Verfahren SHA-1 und RIPEMD-160 bereit.

Das initiale Filesystem von STARCOS 3.1 ECC 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. Parameter der elliptischen Kurven / Bedienungszähler

   Es sind 3 elliptische Kurven mit möglichen Schlüssellängen von 192, 224 und 256 Bit festgelegt. Der Signaturschlüssel ist im Filesystem unauslesbar gespeichert. Er wird in der Vorpersonalisierungs- oder Personalisierungsphase generiert und ist mittels eines PIN-Initialisierungs-Mechanismus (siehe Punkt 2) 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. PIN-Initialisierungs-Mechanismus

   STARCOS 3.1 ECC hat einen PIN-Initialisierungs-Mechanismus zum erstmaligen Setzen der Signatur-PIN, der gewährleistet, dass vor dem Setzen der Signatur-PIN keine Signaturen erzeugt werden können. Nach dem Setzen der Signatur-PIN ist der PIN-Initialisierungs-Mechanismus deaktiviert und kann nicht mehr aktiviert werden.

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 von STARCOS 3.1 ECC beinhaltet keinen Resetting Code (PUK).

Innerhalb der Initialisierungstabelle gibt es für die Signaturapplikation nur Konfigurationsmöglichkeiten zur Wahl der Kurve mit Schlüssellänge und zum

Bedienungszähler des Signaturschlüssels. 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 Zertifizierungsdienstenabieter sind nicht Gegenstand dieser Bestätigung. Sie müssen die im Dokument *Generic Signature Application STARCOS 3.1 ECC* (siehe Kapitel 1) enthaltenen Anforderungen erfüllen und dürfen insbesondere nicht die Signatur-PIN verwenden.

STARCOS 3.1 ECC 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 3.1 ECC erlaubt optional eine Absicherung mit Secure Messaging für die Eingabe der PIN und Übertragung der zu signierenden Daten.

STARCOS 3.1 ECC 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

STARCOS 3.1 ECC 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 3.1 ECC ist in Verbindung mit dem Prozessor SLE66CX360PE / m1536a13 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 Sicherheits-funktionalitäten in ein umfassendes Sicherheitssystem integriert worden.

Diese Bestätigung ist ohne Reevaluation nur mit dem Prozessor SLE66CX360PE / m1536a13 und mit dem Betriebssystem von STARCOS 3.1 ECC sowie mit dem in der Initialisierungstabelle enthaltenen EEPROM-Anteil des Betriebssystem „BLD_CIB3BSCSI31-1-2V21x“ gültig.

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

STARCOS 3.1 ECC ist nach der Vorpersonalisierung („Initialisation and Personalisation“ gemäß der o. g. Dokumentation „Administrator Guidance STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0“ mit Einbringung einer Initialisierungstabelle und optional der Signaturschlüssel-erzeugung) so geschützt, dass eine Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem von STARCOS 3.1 ECC 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 3.1 ECC muss vom Zertifizierungsdiensteanbieter vorpersonalisiert werden. Die Initialisierungstabelle wird in die Prozessorchipkarte eingebracht. Das Signaturschlüsselpaar wird unter Anwendung der vom Betriebssystem von STARCOS 3.1 ECC angebotenen Schlüsselgenerierungsfunktion (unter Zuhilfenahme des physikalischen Zufallszahlengenerators des Chips SLE66CX360PE / m1536a13 der Infineon Technologies AG) erzeugt und in einem gesicherten Filesystem gespeichert (optional in der Personalisierungs-phase). Zusätzlich werden die zur Authentifizierung benötigten Schlüssel und Geheimnisse 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 von STARCOS 3.1 ECC 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 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 (optional nach vorheriger Signaturschlüsselerzeugung), 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 von STARCOS 3.1 ECC sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind **nicht** Gegenstand dieser Bestätigung.

STARCOS 3.1 ECC 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 3.1 ECC 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 von STARCOS 3.1 ECC erforderlich sind.
- Der Zertifizierungsdiensteanbieter hat in seinem Sicherheitskonzept die Maßnahmen darzulegen, die sicherstellen, dass der Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit erzeugt wird.

c) Nutzung als SSEE

Der Zertifizierungsdiensteanbieter hat beim Anlegen bzw. Ergänzen von Datenfeldern und Verzeichnissen die im Dokument *Generic Signature Application STARCOS 3.1 ECC* (siehe Kapitel 1) enthaltenen Anforderungen zu erfüllen. Hierbei darf insbesondere die Signatur-PIN nicht verwendet 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 ist vor seiner ersten Nutzung mit dem PIN-Initialisierungs-Mechanismus geschützt, mit dem nur der Wechsel zu einer individuellen mindestens 6-stelligen Signatur-PIN möglich ist. Dieser Wechsel ist durch den Signaturschlüssel-Inhaber vorzunehmen, sobald er die SSEE besitzt, spätestens jedoch vor Ausstellung des qualifizierten Zertifikates; hierbei hat er zu prüfen, ob die SSEE mit dem PIN-Initialisierungs-Mechanismus 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 STARCOS 3.1 ECC die DSA-Variante basierend auf elliptischen Kurven der Gruppen $E(F_p)$ eingesetzt. Es werden drei definierte Kurven mit Bitlängen der Systemparameter: p,q =192, 224 und 256 verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für die Systemparameter p,q = 192 bis Ende des Jahres 2009 sowie für p,q = 224 und 256 bis Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Ferner werden zur Signaturerzeugung von STARCOS 3.1 ECC 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 Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Diese Bestätigung von STARCOS 3.1 ECC ist somit, abhängig von der Mindest-schlüssellänge, 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.

3.4 Prüfstufe und Mechanismenstärke

STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, Version 2.0 wurde mit dem Prozessor SLE66CX360PE / m1536a13 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 SLE66CX360PE / m1536a13 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 zu STARCOS 3.1 ECC wurde überprüft. Gleichfalls geprüft wurde die sicherheitstechnisch korrekte Erzeugung und Speicherung des Signaturschlüssels in der Signaturapplikation von STARCOS 3.1 ECC.

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:

- CIB3BSCSI31-1-2211V001 und CIB3BSCSI31-1-2212V001

  Diese beinhalten jeweils eine Signaturapplikation mit einer DSA-Variante basierend auf elliptischen Kurven der Gruppen $E(F_p)$ mit Parameter p und q von 192, 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 von STARCOS 3.1 ECC mit diesen Initialisierungstabellen ist somit unter Maßgabe des Abschnitts 3.3 gültig bis 31.12.2009.

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

Ende der Bestätigung