



Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at

DVR: 1035461

ZVR: 948166612

BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

Sichere Signaturerstellungseinheit **STARCOS 3.1 ECC with EU compliant Electronic Signature** **Application V4.0, Version 1.0**

Antragsteller:
Giesecke & Devrient GmbH
Prinzregentenstraße 159
D-81677 München

Bescheinigung ausgestellt am: 03.09.2009
Referenznummer A-SIT-1.085

1. Beschreibung der zu bescheinigenden Komponente

STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, Version 1.0 ist eine Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus:

Hardware:

- Prozessorchip Philips SmartMX P5CC036V1C¹, Hersteller: NXP Semiconductors Germany GmbH², Stresemannallee 101, 22529 Hamburg

Eingebettete Software:

- Betriebssystem STARCOS 3.1 ECC, Hersteller: Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 München
- Applikation für digitale Signatur gemäß „Generic Signature Application STARCOS 3.1 ECC with EU compliant Electronic Signature Application version 1.11“

Mit der Signaturkarte wird die folgende Dokumentation laut Zertifizierungsbericht TUVIT-DSZ-CC-9238 geliefert:

- Administrator guidance STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.2, 2005-03-31
- User Guidance STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.2, 2005-03-09
- Generic Signature Application STARCOS 3.1 ECC with EU compliant Electronic Signature Application version 1.11, 2005-04-01
- Installation, generation and start-up STARCOS 3.1 ECC with EU compliant Electronic Signature Application V4.0, version 1.2, 2005-03-31.

¹ Der Prozessorchip Phillips P5CC036V1C wurde vom BSI zertifiziert. Das Zertifikat BSI-DSZ-CC-0244-2004 vom 11.11.2004 weist der Komponente eine Konformität zum Schutzprofil BSI-PP-0002-2001, sowie die erfolgreiche Evaluierung nach der Prüfstufe EAL5+ (Erweiterungen: ALC_DVS.2: Lebenszyklus-Unterstützung - Ausreichende Sicherheitsmaßnahmen, AVA_MSU.3: Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände, AVA_VLA.4: Schwachstellenbewertung – Hohe Widerstandsfähigkeit) aus. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke „hoch“.

² Ehem.: Philips Semiconductors GmbH

Der Auslieferungsumfang der Signaturkarte umfasst den Prozessorchip mit implementierter ROM-Maske sowie die zur Fertigstellung der Signaturerstellungseinheit notwendige Initialisierungstabelle, die den im EEPROM des Chips implementierten Teil der eingebetteten Software "BLD_CPA4xSCSI31-1-2V100" enthält. In diese Bescheinigung eingeschlossen sind die vier Initialisierungstabellen laut Zertifizierungsbericht TUVIT-DSZ-CC-9238: CPA4xSCSI31-1-2101V001, CPA4xSCSI31-1-2101V003, CPA4xSCSI31-1-2102V001 und CPA4xSCSI31-1-2102V003. Diese beinhalten jeweils eine ECDSA³-Signaturapplikation, keinen Bedienungsähler für den Signaturschlüssel und keinen PUK für die Signatur-PIN. Die Einbringung der Initialisierungstabelle sowie die Erzeugung der Signaturerstellungs- und Signaturprüfdaten auf der Signaturkarte erfolgt im Rahmen der Initialisierung. Danach können keine weiteren Initialisierungstabellen geladen werden.

Die Signaturkarte basiert auf dem Schutzprofil BSI-PP-0006-2002⁴ und erfüllt alle Aspekte dieses Schutzprofils bis auf den Aspekt, dass die Bereitstellung eines vertrauenswürdigen Kanals bzw. Pfades zur Übertragung der Signaturprüfdaten, der zu signierenden Daten und der Autorisierungscode nicht von der Signaturkarte selbst, sondern durch den Benutzer erzwungen wird. Beim Einsatz der Signaturkarte in einer nicht vertrauenswürdigen Einsatzumgebung muss sich der Benutzer durch das Anzeigen einer „Display Message“ vom Vorhandensein eines vertrauenswürdigen Kanals bzw. Pfades überzeugen. Die „Display Message“ ist eine vom Benutzer selbst gewählte auf der Signaturkarte gespeicherte Zeichenfolge, die nur nach erfolgreicher gegenseitiger Authentisierung von Signaturkarte und externer Anwendung mittels Secure Messaging Protokoll ausgelesen werden kann.

Zum erstmaligen Setzen der Signatur-PIN ist ein PIN-Initialisierungs-Mechanismus implementiert, der gewährleistet, dass vor dem Setzen der Signatur-PIN keine Signaturen erzeugt werden können. Nach dem Setzen der Signatur-PIN ist dieser Mechanismus deaktiviert und kann nicht mehr aktiviert werden. Ein Wechsel der Signatur-PIN ist möglich. Die dezimale Signatur-PIN hat eine Mindestlänge von 6, eine Maximallänge von 12 Stellen und besitzt einen Fehlbedienungsähler von 3. Bei abgelaufenem Fehlbedienungsähler ist die Signaturfunktionalität permanent gesperrt. Die Signatur-PIN ist ausschließlich den Signaturerstellungsdaten zugeordnet, nach erfolgreicher Authentisierung mit der Signatur-PIN kann vom Signator genau eine Signatur erstellt werden.

Neben der Signaturapplikation mit den Signaturerstellungsdaten für qualifizierte elektronische Signaturen können auf der Signaturkarte weitere Applikationen mit weiteren Schlüsselpaaren und Daten vorhanden sein. Diese zusätzlichen Applikationen sind nicht Gegenstand dieser Bescheinigung.

³ DSA-Variante mit elliptischen Kurven basierend auf einer Gruppe $E(F_p)$ mit Länge der Parameter p und q von jeweils 192 Bit.

⁴ Dieses Schutzprofil entspricht dem CWA 14169 (Protection Profile for the SSCD Type 3) im „Verzeichnis allgemein anerkannter Normen für Produkte für elektronische Signaturen, die von den Mitgliedsstaaten angenommen werden sollen in Übereinstimmung mit den Anforderungen des Anhangs III der Richtlinie 1999/93/EG.“, veröffentlicht im Amtsblatt der Europäischen Union L 175/45 vom 15.7.2003

2. Erfüllung der Anforderungen des SigG⁵ und der SigV⁶

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1⁷ und § 18 Abs. 2 zweiter Satz⁸ SigG,
- Anforderungen nach § 3 Abs. 1⁹ und § 3 Abs. 2¹⁰ SigV und
- Anforderungen nach § 6 Abs. 1¹¹ und § 6 Abs. 2¹² SigV.

Die Signaturkarte ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signaturerstellungsdaten und
- Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

Die Gültigkeit endet jedenfalls, wenn das IT-Sicherheitszertifikat TUVIT-DSZ-CC-9238-2005 vom 8.4.2005 seine Gültigkeit verliert.

4. Einsatzbedingungen

Die Gültigkeit dieser Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden:

- (1) Die mit der Signaturkarte ausgelieferte Dokumentation (siehe Kapitel 1 dieser Bescheinigung) enthält die notwendigen Anweisungen für den sicheren Gebrauch der Signaturkarte. Zusätzlich sind für den sicheren Gebrauch der Signaturkarte die Annahmen über die Einsatzumgebung im Security Target, sowie das Security Target als Ganzes in Betracht zu ziehen. Diesen Anweisungen und Annahmen sowie den Einsatzbedingungen dieser Bescheinigung ist in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen
 - durch das Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters entsprechend § 12 SigV sicherzustellen,
 - in der Belehrung des Signators entsprechend zu übernehmen
 - und deren Wirkung im Wege der Aufsicht sicherzustellen.
- (2) Der Hersteller der Signaturkarte muss eine Möglichkeit¹³ bereitstellen, durch die der Benutzer der Signaturkarte überprüfen kann, ob er die Signaturkarte mit den in Kapitel 1 genannten Initialisierungstabellen verwendet.

⁵ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008 vom 22. April 2008.

⁶ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)

⁷ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindern

⁸ Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muss sichergestellt sein.

⁹ Die technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

¹⁰ Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

¹¹ Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es können insbesondere Schutzprofile (Protection Profiles) herangezogen werden, die nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Security Evaluation – ISO/IEC 15408)“ oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (Information Technology Security Evaluation Criteria – ITSEC)“ erstellt wurden. (...)

¹² Bei den Prüfungen nach Abs. 1 sind insbesondere Referenznummern zu beachten, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrechtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices – SSCD) oder vertrauenswürdige Systeme oder Produkte des ZDA veröffentlicht wurden.

- (3) Die Signaturerstellungsdaten sind vor ihrer ersten Anwendung mit einem PIN-Initialisierungs-Mechanismus geschützt. Der Signator muss sich nach Erhalt der Signaturkarte und vor Ausstellung eines qualifizierten Zertifikats über die Signaturprüfdaten mit Hilfe dieses Mechanismus vergewissern, dass die Signaturerstellungsdaten noch nicht verwendet worden sind.
- (4) Die Vertraulichkeit und Integrität der eingegebenen Autorisierungs-codes sowie die Integrität der zu signierenden Daten bei der Übertragung zwischen externer Anwendung und Signaturkarte muss durch einen vertrauenswürdigen Pfad bzw. Kanal geschützt sein. Vor dem Einsatz der Signaturkarte zur Erstellung von qualifizierten Signaturen muss der Signator entscheiden, ob die Einsatzumgebung vertrauenswürdig ist oder nicht. Beim Einsatz der Signaturkarte in einer nicht vertrauenswürdig Umgebung muss sich der Signator durch das Anzeigen der „Display Message“ davon überzeugen, dass ein vertrauenswürdiger Pfad bzw. Kanal zwischen externer Anwendung und Signaturkarte durch kryptographische Mittel aufgebaut wurde.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur wird von der Signaturkarte der ECDSA¹⁴ Algorithmus nach ISO/IEC 15946-2 bereitgestellt. Es werden drei definierte Kurven¹⁵ mit Längen der Parameter p , q von 192, 224 bzw. 256 Bit verwendet. Die in Kapitel 1 dieser Bescheinigung genannten Initialisierungstabellen verwenden die definierte Kurve mit Längen der Parameter p , q von 192 Bit.

Zur Berechnung des Hashwertes werden von der Signaturkarte die Algorithmen SHA-1 und RIPEMD-160 nach ISO/IEC 10118-3 bereitgestellt.¹⁶

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV¹⁷ erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-CC-9238-2005 vor, ausgestellt durch die Zertifizierungsstelle der TÜV Informationstechnik GmbH¹⁸, in Essen am 8.4.2005. Die materiellen Prüfungen sind im Zertifizierungsbericht „Certification Report: STARCOS 3.1 ECC Version 1.0 (TUVIT-DSZ-CC-9238)“ beschrieben.

Das Zertifikat weist der Signaturkarte die erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA_MSU.3¹⁹, AVA_VLA.4²⁰) der Common Criteria (CC, Version 2.1) aus.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke „hoch“.

¹³ Laut Zertifizierungsbericht TUVIT-DSZ-CC-9238 muss der Hersteller auf seiner Webseite (<http://www.gi-de.com>) bei einer Suche nach dem Begriff „STARCOS31ECCTABLES“ die notwendigen Informationen bereitstellen.

¹⁴ DSA basierend auf einer Gruppe $E(F_p)$

¹⁵ Die Parameter entsprechen den in FIPS 186-2 definierten Kurven P-192, P-224 bzw. P-256.

¹⁶ Die Auswahl einer gemäß § 3 Abs. 2 SigV geeigneten Hashfunktion hat durch die in der Systemumgebung der Signaturkarte eingesetzte Software zu erfolgen und ist nicht Gegenstand dieser Bescheinigung.

Anmerkung: Zur Eignung der Hashfunktion SHA-1 kann zum Zeitpunkt der Ausstellung dieser Bescheinigung auf Grund neuer Methoden zur Kollisionssuche keine Prognose bezüglich des uneingeschränkten Einsatzes bei der Erstellung von qualifizierten elektronischen Signaturen gegeben werden. Es wird daher empfohlen, zur Berechnung des Hashwertes andere Hashfunktionen, die für einen längeren Zeitraum als geeignet betrachtet werden können, einzusetzen.


¹⁷ Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.


¹⁸ TÜV Informationstechnik GmbH, Langemarckstr. 20, 45141 Essen

¹⁹ Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände

²⁰ Schwachstellenbewertung – Hohe Widerstandsfähigkeit

Unterschriften:

Signaturwert	KCF4pOG2YrTvzbErayKJEZfmbFagsy+4RISVDEuGrJZSyILWLI0ddbmInMBOuOEx	
	Unterzeichner	Manfred Holzbach, geschäftsführender Vorstand
	Datum/Zeit-UTC	2009-09-03T07:57:19Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	261828
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1251964639-6604250@5630-4720-0-17868-10623
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	

Signaturwert	jAoGok4bH5t6ek7pr/nL080fFfggwZii+jB6zqYueDs+teII8vWifDOsPPBRR59r	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2009-09-03T11:21:28Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	221297
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1251976888-977655@10118-3923-0-17160-7694
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	