



## 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](mailto:office@a-sit.at)

DVR: 1035461

ZVR: 948166612

### BESCHEINIGUNG NACH §18(5) SIGG

## Sichere Signaturerstellungseinheit Smart Card mit Chip „Philips Smart Card Controller P8WE5032VOG“ und Betriebssystem „STARCOS SPK 2.3“ Version 6 und Signaturanwendung TrustSign Version 1.2

Antragsteller:

A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH  
Landstraßer Hauptstraße 5  
1030 Wien

**Bescheinigung ausgestellt am: 11.12.2007**  
**Referenznummer A-SIT-1.071**

### 1. Beschreibung der zu bescheinigenden Komponente

Die Komponente ist eine Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus

- Prozessorchip (ICC, Prozessor P8WE5032VOG, Hersteller: NXP Semiconductors Germany GmbH<sup>1</sup>, Stresemannallee 101, D-22529 Hamburg) mit
- Betriebssystem (STARCOS SPK2.3 Version 6, Hersteller: Giesecke&Devrient GmbH, Prinzregentenstraße 159, D-81677 München) und
- Signaturapplikation (TrustSign Version 1.2, Hersteller: A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH, Landstraßer Hauptstraße 5, A-1030 Wien) in der Betriebsart *limited signature generation configuration*; Anzahl der Signaturerstellung pro Authentifizierung ist 1.

Die Signaturkarte wurde zuvor mit "Bescheinigung nach §18(5) SigG: Smart Card mit Chip Philips Smart Card Controller P8WE5032VOG und Betriebssystem STARCOS SPK2.3 und Digital Signature Application TrustSign" am 22.10.2001 (Gültigkeit endete am 30.06.2004), am 20.08.2004 (Gültigkeit endete am 30.06.2005) und am 25.7.2005 (Gültigkeit endete am 24.07.2007) bescheinigt.

STARCOS steuert den Datenaustausch und die Speicherbereiche und verarbeitet Informationen im ICC. Als Ressourcenmanager stellt STARCOS die notwendigen Funktionen für Operation und Management einer jeden Anwendung bereit. STARCOS SPK2.3 ist eine Weiterentwicklung von STARCOS S2.1, die die gesamte Funktionalität von STARCOS S2.1 beinhaltet und die für asymmetrische Kryptographie benötigten Funktionen hinzufügt.

STARCOS SPK 2.3 implementiert den symmetrischen Verschlüsselungsalgorithmus DEA (Data Encryption Algorithm) und seine Spezialform Triple-DES (nicht Gegenstand dieser Bescheinigung), sowie die asymmetrischen Kryptoalgorithmen RSA und DSA. Die Algorithmen RSA und DSA als auch das Hashverfahren SHA-1 können benutzt werden, um elektronische Signaturen zu erzeugen. Das benutzte Padding-Verfahren entspricht PKCS 1.0 Version 1.5 und ISO/IEC 9796-2. STARCOS SPK2.3 unterstützt die gegenseitige Geräteauthentisierung und Secure Messaging gemäß ISO/IEC 7816-4 (diese beiden Funktionalitäten sind nicht Gegenstand dieser Bescheinigung).

<sup>1</sup> Ehem.: Philips Semiconductors GmbH

Derzeit ist nicht geplant Secure Messaging zwischen Signaturkarte und Kartenterminal/PC bei der Signaturerstellung zu verwenden.

In Verbindung mit der Signaturanwendung TrustSign V1.2 ermöglicht STARCOS SPK 2.3 die Erzeugung und Speicherung der Signaturstellungsdaten und die Erstellung sicherer elektronischer Signaturen. Die Anzahl der Signaturen, die nach einer erfolgreichen Benutzerauthentifizierung erzeugt werden können, ist auf eine Signatur begrenzt („limited signature generation configuration“). TrustSign verwendet ausschließlich RSA als Signaturalgorithmus und SHA-1 als Hashverfahren.

Der ICC kann als multifunktionale Chipkarte benutzt werden. In diesem Fall können andere Anwendungen während der Phase der operationellen Nutzung in den ICC geladen werden. STARCOS SPK 2.3 mit der Signaturanwendung TrustSign V1.2 (limited signature generation configuration) kann ein bis maximal zehn Schlüsselpaare generieren und speichern.

## 2. Erfüllung der Anforderungen des SigG<sup>2</sup> und der SigV<sup>3</sup>

Die Signaturerstellungseinheit erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1)<sup>4</sup> und §18(2)<sup>5</sup> zweiter Satz SigG,
- Anforderungen nach §3(1)<sup>6</sup> und §3(2)<sup>7</sup> SigV und
- Anforderungen nach §9(1)<sup>8</sup> SigV

Die Signaturerstellungseinheit ist daher in folgenden Kategorien bescheinigt:

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

## 3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist bis 31.12.2008 gültig. Die Gültigkeit endet jedenfalls, wenn zumindest eines der zugrunde liegenden IT-Sicherheitszertifikate (BSI-DSZ-ITSEC-0158-2001 vom 17.1.2001 bzw. debisZERT-DSZ-ITSEC-04020-2001 vom 21.3.2001) seine Gültigkeit verliert.

**Anmerkung:** Das Zertifikat debisZERT-DSZ-ITSEC-04020-2001 fordert eine neuerliche Überprüfung der Ergebnisse bezgl. der Sicherheitsziele SO6 und SO7 bis Mitte 2005. A-SIT liegt eine Stellungnahme des Evaluators (T-Systems GEI GmbH, 53111 Bonn, Rabinstraße 8<sup>9</sup>) vor. Diese besagt, dass die Gültigkeit seinerzeit auf den 30.06.2005 begrenzt wurde, da die eingesetzten Algorithmen und Schlüssellängen durch die in Deutschland zuständige Regulierungsbehörde RegTP zum Ausstellungszeitpunkt des o.g. Zertifikats nur bis zu diesem Datum freigegeben worden waren.

Die verwendeten Algorithmen RSA und SHA-1 und die Schlüssellänge von 1024 Bit für den RSA-Signaturschlüssel sind zum Zeitpunkt der Ausstellung der gegenständlichen

<sup>2</sup> Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl. I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 164/2005 vom 30. Dezember 2005.

<sup>3</sup> Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV, BGBl. II Nr. 30/2000 vom 2. Februar 2000) in der Fassung BGBl. II Nr. 527/2004 vom 30. Dezember 2004.

<sup>4</sup> Für die Erzeugung und Speicherung von Signaturstellungsdaten sowie für die Erstellung sicherer 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 Signaturstellungsdaten verlässlich verhindern.

<sup>5</sup> Die Signaturstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.

<sup>6</sup> Die technischen Komponenten und Verfahren, die bei der Erzeugung und Speicherung von Signaturstellungsdaten für sichere elektronische Signaturen zum Einsatz kommen, müssen im Hinblick auf das Erfordernis ihrer Überprüfung nach § 18 Abs. 5 SigG den Anforderungen des § 9 entsprechen. Dasselbe gilt hinsichtlich der Signaturerstellungseinheit für sichere elektronische Signaturen, und zwar für solche technische Komponenten und Verfahren, die zur Verarbeitung der Signaturstellungsdaten verwendet werden.

<sup>7</sup> Für sichere elektronische Signaturen dürfen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die für die technische Sicherheit dieser Algorithmen und Parameter geltenden Randbedingungen sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

<sup>8</sup> Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Hierbei 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.

(...)

<sup>9</sup> vormals debis Systemhaus Information Security Services GmbH – Zertifizierungsstelle debisZERT

Bescheinigung weiterhin gemäß der österreichischen Rechtslage (§3(2)<sup>10</sup> SigV) als geeignet anzusehen (siehe auch Kapitel 5).

#### 4. Einsatzbedingungen

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

- (1) Der Signator darf die Signaturkarte zur Erstellung von sicheren Signaturen nur mit geeigneten und nicht-manipulierten Signaturprodukten in einer sicheren und kontrollierten Einsatzumgebung verwenden.
- (2) Der Signator muss seinen Autorisierungscode (PIN) vertraulich halten und in regelmäßigen Abständen ändern.
- (3) Der Signator darf denselben Autorisierungscode nicht für unterschiedliche Kartenapplikationen vereinbaren.
- (4) Der Signator muss die Signaturkarte so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- (5) Die Signaturerstellungsdaten sind vor ihrer ersten Anwendung mit einer Initial-PIN (auch „transport PIN“ genannt) geschützt. Bei Erhalt einer Signaturkarte muss der Signator die voreingestellte Initial-PIN auf einen geheimen und individuellen Wert (Signatur-PIN, mindestens 6-stellig) setzen.
- (6) Die personalisierte Signaturkarte muss vom Zertifizierungsdiensteanbieter dem Signator persönlich ausgehändigt werden.
- (7) Der Zertifizierungsdiensteanbieter muss die Signaturkarte direkt beim Hersteller abholen.
- (8) Die öffentlichen Signatur- oder Authentisierungsschlüssel des Zertifizierungsdiensteanbieters und ihre Zertifikate sowie das Zertifikat über den öffentlichen Signaturschlüssel des Signators müssen authentisch und unverändert in die Signaturkarte eingebracht werden.
- (9) Zum Abschluss der Erstpersonalisierung muss das Passwort des Herstellers (PIN.GD.PERS) dauerhaft gesperrt werden.
- (10) Die Zertifizierungsberichte debisZERT-DSZ-ITSEC-04020-2001 und BSI-DSZ-ITSEC-0158-2001 beinhalten auch betriebliche und organisatorische Randbedingungen, die nicht direkt durch die Signaturerstellungseinheit abgedeckt werden können. Soweit die dort genannten organisatorischen Einsatzbedingungen betroffen sind, ist diesen in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen
  - durch das Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters entsprechend §15 SigV sicherzustellen,
  - in der Belehrung des Signators entsprechend zu übernehmen
  - und deren Wirkung im Wege der Aufsicht sicherzustellen.

#### 5. Algorithmen und zugehörige Parameter

Zur Erstellung einer sicheren elektronischen Signatur wird vom Betriebssystem STARCOS SPK 2.3 der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit und den Padding-Verfahren nach PKCS #1 Version 1.5 (emsa-pkcs1-v1\_5) bzw. nach ISO/IEC 9796-2 unter Verwendung von Zufallszahlen (iso9796-din-rn) bereitgestellt.

Zur Berechnung des Hashwertes wird optional vom Betriebssystem STARCOS SPK 2.3 der SHA-1 Algorithmus bereitgestellt.

Dadurch sind die Anforderungen gemäß §3(2)<sup>11</sup> SigV erfüllt.

<sup>10</sup> Für sichere elektronische Signaturen dürfen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die für die technische Sicherheit dieser Algorithmen und Parameter geltenden Randbedingungen sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

<sup>11</sup> Für sichere elektronische Signaturen dürfen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die für die technische Sicherheit dieser Algorithmen und Parameter geltenden Randbedingungen sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

## 6. Prüfstufe und Mechanismenstärke

### Hardware:

Es liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0158-2001 vor, ausgestellt durch das Bundesamt für die Sicherheit in der Informationstechnik (BSI); Bonn vom 17.1.2001. Die materiellen Prüfungen sind im Zertifizierungsbericht Certification Report BSI-DSZ-ITSEC-0158-2001 for Philips Smart Card Controller P8WE5032V0G, BSI vom 17.1.2001 beschrieben. Dieses Zertifikat weist der Komponente die Evaluierungsstufe E4 mit der Mechanismenstärke „hoch“ nach ITSEC aus.

### Betriebssystem und Signaturanwendung StarCert:


Es liegt das Deutsche IT-Sicherheitszertifikat debisZERT-DSZ-ITSEC-04020-2001 vor, ausgestellt durch debis Systemhaus Information Security Services GmbH<sup>12</sup> am 21.3.2001. Die materiellen Prüfungen sind im Zertifizierungsbericht Certification Report, STARCOS SPK 2.3 with Digital Signature Application StarCert, debisZERT-DSZ-ITSEC-04020-2001, Revision 1.0, 21.3.2001 mit darin enthaltenen Einschränkungen beschrieben. Dieses Zertifikat weist der Komponente die Evaluierungsstufe E4 mit der Mechanismenstärke „hoch“ nach ITSEC aus.


Anmerkung: Das Zertifikat fordert eine neuerliche Überprüfung der Sicherheitsziele SO6 und SO7 bis Mitte 2005. A-SIT liegt eine Stellungnahme des Evaluators (T-Systems GEI GmbH, 53111 Bonn, Rabinstraße 8) vor, die besagt, dass die Gültigkeit des o.g. Zertifikats auf den 30.06.2005 begrenzt wurde, da die eingesetzten Algorithmen und Schlüssellängen durch die in Deutschland zuständige Regulierungsbehörde RegTP zum Ausstellungszeitpunkt des o.g. Zertifikats nur bis zu diesem Datum freigegeben worden waren.

### Integration:

Die sicherheitstechnisch korrekte Integration der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) und des Prozessors P8WE5032V0G wurde im Rahmen der Bestätigung debisZERT.02036.TE.03.2001 überprüft. Die Unterschiede zwischen der zertifizierten Signaturanwendung StarCert und der A-Trust Signaturanwendung TrustSign bestehen ausschließlich in Dateistruktur und Dateiinhalten.

### Unterschriften:

Signaturwert	yIrr00W6Vlg67+mmYj8vepetGn/yB1PZ6UkL2EA6plrZ8GJZ6gvJQ9emRZ6xDGJWY	
	Unterzeichner	Geschäftsführender Vorstand, Manfred Holzbach
	Datum/Zeit-UTC	2007-12-11T14:02:09Z
	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.	97349
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1197381729-2055921@16190-4076-0-14475-32402
Prüfhinweis	Informationen zur Signaturprüfung finden Sie unter: <a href="http://www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php">www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php</a> .	

Signaturwert	55LxGNmtfpNSpws7uPHHkklX4yrFKVfFBfurDCEwfkLU+AzFqxWis09MKFcgif2I	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2007-12-11T14:37:02Z
	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@1197383822-24530205@3197-27964-0-25950-4403
Prüfhinweis	Prüfservice: <a href="http://demo.a-sit.at/el_signatur/verification">http://demo.a-sit.at/el_signatur/verification</a>	

<sup>12</sup> heute T-Systems GEI GmbH, Rabinstraße 8, 53111 Bonn