



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

BESCHEINIGUNG NACH §18(5) SIGG

Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 und Digital Signature Application TrustSign

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

1. Beschreibung der zu bescheinigenden Komponente

Die Komponente (nachstehend Chipkarte oder Karte genannt) ist

- eine Prozessorchipkarte (ICC, Prozessor P8WE5032V0G, Hersteller: Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, 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 Signaturerstellungen pro Authentifizierung ist 1.

Die Chipkarte stellt eine sichere Signaturerstellungseinheit dar und ermöglicht die Erzeugung und Speicherung der Signaturerstellungsdaten und die Erstellung sicherer elektronischer Signaturen. Die Anzahl der Signaturen, die nach einer erfolgreichen Benutzerauthentifizierung erstellt werden können, ist auf eine Signatur begrenzt („limited signature generation configuration“).

Die Chipkarte wurde zuvor mit "Bescheinigung nach §18(5) SigG: Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK2.3 und Digital Signature Application TrustSign" am 22.10.2001 (Gültigkeit endete am 30.06.2004) und am 20.08.2004 (Gültigkeit endete am 30.06.2005) bescheinigt.

2. Erfüllung der Anforderungen des SigG¹ und der SigV²

Die Chipkarte erfüllt unter nachstehenden Einsatzbedingungen die in den jeweiligen Fußnoten angeführten

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

Die Chipkarte 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

- 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 8⁸) 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 Bescheinigung weiterhin gemäß der österreichischen Rechtslage (§3(2)⁹ SigV) als geeignet anzusehen (siehe auch Kapitel 5).

¹ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

² 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.

³ Für die Erzeugung und Speicherung von Signaturerstellungsdaten 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 Signaturerstellungsdaten verlässlich verhindern.

⁴ 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.

⁵ Die technischen Komponenten und Verfahren, die bei der Erzeugung und Speicherung von Signaturerstellungsdaten 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 Signaturerstellungsdaten verwendet werden.

⁶ 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.

⁷ 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. (...)

⁸ vormals debis Systemhaus Information Security Services GmbH – Zertifizierungsstelle debisZERT

⁹ 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.

4. Einsatzbedingungen

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

- Der Signator darf die Chipkarte zur Erstellung von sicheren Signaturen nur mit geeigneten und nicht-manipulierten Signaturprodukten in einer sicheren und kontrollierten Einsatzumgebung verwenden.
- Der Signator muss seinen Autorisierungscode (PIN) vertraulich halten und in regelmäßigen Abständen ändern.
- Der Signator darf denselben Autorisierungscode nicht für unterschiedliche Kartenapplikationen vereinbaren.
- Der Signator muss die Chipkarte so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Die Signaturerstellungsdaten sind vor ihrer ersten Anwendung mit einer Initial-PIN (auch „transport PIN“ genannt) geschützt. Bei Erhalt einer Chipkarte muss der Signator die voreingestellte Initial-PIN auf einen geheimen und individuellen Wert (Signatur-PIN, mindestens 6-stellig) setzen.
- Die personalisierte Chipkarte muss vom Zertifizierungsdiensteanbieter dem Signator persönlich ausgehändigt werden.
- Der Zertifizierungsdiensteanbieter muss die Chipkarte direkt beim Hersteller abholen.
- 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 Chipkarte eingebracht werden.
- Zum Abschluss der Erstpersonalisierung muss das Passwort des Herstellers (PIN.GD.PERS) dauerhaft gesperrt werden.
- 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 Padding-Verfahren PKCS #1 Block Type 01 Version 1.5 bereitgestellt.

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

Diese Algorithmen und Parameter erfüllen die Anforderungen gemäß §3(2)¹⁰ SigV.

¹⁰ 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 GmbH¹¹ 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:

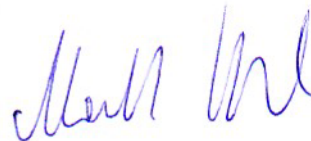
Die sicherheitstechnisch korrekte Integration der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) und des Prozessors P8WE5032V0G wurde im Rahmen der Bestätigung debisZERT.02036.TE.03.2001 überprüft. Die Unterschiede zwischen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

Wien, 25.07.2005

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter



Manfred Holzbach
Geschäftsführender Vorstand

¹¹ heute T-Systems GEI GmbH, Rabinstraße 8, 53111 Bonn