



## 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)

### **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 bescheinigter Komponente**

Die Komponente (nachstehend Chipkarte genannt) ist eine Prozessorchipkarte mit Betriebssystem und Signaturanwendung (Digital Signature Application) bestehend aus:

- Prozessorchipkarte: Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G
  - Hersteller: Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, Stresemannallee 101, D-22529 Hamburg
- Betriebssystem: STARCOS SPK 2.3 Version 6
  - Hersteller: Giesecke & Devrient GmbH, Prinzregentenstraße 159, D-81677 München
- Digital Signature Application: TrustSign Version 1.2 in der Betriebsart *limited signature generation configuration*
  - Hersteller: A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH, Landstraßer Hauptstraße 5, A-1030 Wien

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 mit der "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 erstmals bescheinigt.

## 2. Erfüllung der Anforderungen des SigG<sup>1</sup> und der SigV<sup>2</sup>

Die Chipkarte erfüllt

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

Die Chipkarte ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung und Speicherung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Erzeugen des Hashwertes aus dem Dokument,
- Komponenten und Verfahren zur Verwahrung der Signaturerstellungsdaten und zur Sicherstellung des autorisierten Zuganges, und
- Komponenten und Verfahren zur Anwendung der Signaturerstellungsdaten und zur Erzeugung der Signaturformate.

## 3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig. Die Gültigkeit endet jedenfalls, wenn

- die eingesetzten Algorithmen<sup>7</sup> und deren Parameter nicht mehr als sicher anzusehen sind (aufgrund SigG und SigV in der jeweils gültigen Fassung; zum Zeitpunkt der Ausstellung der gegenständlichen Bescheinigung sind die eingesetzten Algorithmen und deren Parameter bis 31.12.2005 als sicher anzusehen) oder
- die deutsche Bestätigung debisZERT.02036.TE.03.2001 vom 5.4.2001 ihre Gültigkeit verliert (am 30.06.2005, sofern keine Verlängerung erfolgt)<sup>8</sup> oder

<sup>1</sup> 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.

<sup>2</sup> Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 vom 2. Februar 2000.

<sup>3</sup> 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.

<sup>4</sup> Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, dass die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, daß dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. 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.

<sup>5</sup> Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungs-codes (zB PIN-Eingabe, Fingerabdruck) auslösbar sein. Die Anzahl der Signaturen, die mit einer Autorisierung des Signators gegenüber seiner Signaturerstellungseinheit ausgelöst wird, muss dem Signator bekannt gegeben werden. Das unbefugte Erfahren der Autorisierungs-codes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (zB Signatur- und Bankomatfunktion) verwendbar sein. Signaturerstellungseinheiten, die mehrere Anwendungen zulassen, wie zB Multiapplikationskarten oder Multiapplikationsterminals, dürfen nur verwendet werden, wenn die Maßnahmen und Methoden, die das Auslösen unterschiedlicher Anwendungen mit denselben Autorisierungs-codes verhindern, im Sicherheitskonzept beschrieben sind. Die eingegebenen Autorisierungs-codes dürfen von den verwendeten Systemelementen nicht gespeichert werden. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes müssen ausgeschlossen sein. Zu besonderen Sicherheitszwecken können die Autorisierungs-codes auf mehrere Systemelemente verteilt werden. Der Signator ist über die zur Auslösung der Signaturfunktion erforderlichen Maßnahmen zu unterrichten (§ 10 Abs. 7).

<sup>6</sup> Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) oder dem British Standard (BS) 7799, erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten sein.

<sup>7</sup> siehe auch Kapitel 5.

<sup>8</sup> Die Gültigkeit der deutschen Bestätigung debisZERT.02036.TE.03.2001 vom 5.4.2001 endet am 30.06.2005, sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

- 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. (Die Gültigkeit des Zertifikates debisZERT-DSZ-ITSEC-04020-2001 endet Mitte des Jahres 2005, sofern keine Reevaluierung und-zertifizierung durchgeführt wird)<sup>9</sup>.

## 4. Einsatzbedingungen

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

Die vorgelegte deutsche Bestätigung debisZERT.02036.TE.03.2001 nennt eine Reihe von Auflagen, die auch die Einsatzumgebung insbesondere vor dem Einsatz zur Signaturerstellung miteinbeziehen. Diese deutsche Bestätigung ist integraler Bestandteil der gegenständlichen Bescheinigung gemäß §18 (5) SigG, mit folgenden Hinweisen/Ergänzungen:

- alle Einsatzbedingungen, die sich auf die Signaturanwendung StarCert beziehen, sind auch für die Signaturanwendung TrustSign gültig
- Sofern für Komponenten eine Sicherheitsbestätigung nach dem deutschen Signaturgesetz gefordert wird, ist diese Forderung auch erfüllt, wenn die genannten Komponenten den Anforderungen des österreichischen Signaturgesetzes und der österreichischen Signaturverordnung in der jeweils gültigen Fassung genügen.

Die Einsatzbedingungen der deutschen Bestätigung beinhalten auch betriebliche und organisatorische Randbedingungen, die unter Berücksichtigung der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen 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 entsprechend §15 SigV des Zertifizierungsdiensteanbieters 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 bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 SigV erfüllt.

Zur Berechnung des Hashwertes wird optional vom Betriebssystem STARCOS SPK 2.3 der SHA-1 Algorithmus bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 2 Punkt 2 SigV erfüllt.

<sup>9</sup> Eine Reevaluierung und –zertifizierung für die Sicherheitsziele SO6 und SO7 bis Mitte des Jahres 2005 ist erforderlich.

## 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>10</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.

### 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.

Die Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK2.3 und Digital Signature Application StarCert ist von der deutschen Bestätigungsstelle debis Systemhaus Information Security Services GmbH<sup>11</sup>, Rabinstraße 8, D-53111 Bonn, gemäß §14 (4) Gesetz zur digitalen Signatur und §§16 und 17 Signaturverordnung in Deutschland bestätigt worden (Bestätigung debisZERT.02036.TE.03.2001 vom 5.4.2001).

Wien, 20.08.2004

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach  
Geschäftsführender Vorstand

<sup>10</sup> heute T-Systems GEI GmbH, Rabinstraße 8, 53111 Bonn

<sup>11</sup> heute T-Systems GEI GmbH, Rabinstraße 8, 53111 Bonn