



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

Homepage: www.a-sit.at

E-Mail: office@a-sit.at

A-8010 Graz, Inffeldgasse 16a

Tel.: ++43 316 – 873 5514

Fax: ++43 316 – 873 5520

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 bescheinigten 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-22505 Hamburg
- Betriebssystem: STARCOS SPK 2.3 Version 6
 - Hersteller: Giesecke & Devrient GmbH, Prinzregentenstraße 159, D-81607 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“).

2. Erfüllung der Anforderungen des SigG und der SigV

Die Chipkarte erfüllt

- Anforderungen nach §18(1) und §18(2) SigG,
- Anforderungen nach §7(3) SigV ausgenommen Anforderungen an die Hostanwendung, und

- die Anforderung nach §9(2) SigV an die Prüfung der für die Erzeugung und Speicherung von Signaturerstellungsdaten und für die Erstellung sicherer elektronischer Signaturen eingesetzten technischen Komponenten und Verfahren, dass die Evaluationsstufe ITSEC E3 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein muss.

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 bis 30.6.2004 gültig. Die Bescheinigung endet jedenfalls, sofern die deutsche Bestätigung debisZERT.02036.TE.03.2001 vom 5.4.2001 in Deutschland die Gültigkeit verliert. Die Gültigkeit dieser Bescheinigung ist an die unter Einsatzbedingungen genannten Auflagen gebunden.

4. Einsatzbedingungen

Die deutsche Bestätigung debisZERT.02036.TE.03.2001 vom 5.4.2001 nennt eine Reihe von Auflagen, die auch die organisatorische Umgebung, insbesondere vor dem Einsatz zur Signaturerstellung, miteinbeziehen. Diese Bestätigung ist integraler Bestandteil der vorliegenden Bescheinigung gemäß §18 (5) SigG. Dabei soll beachtet werden, dass alle Einsatzbedingungen, die sich auf die Signaturanwendung StarCert beziehen, auch für die Signaturanwendung TrustSign gültig sind.

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 Chipkarte 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.

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 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. Die Unterschiede zwischen der zertifizierten Signaturanwendung StarCert und der A-Trust Signaturanwendung TrustSign bestehen ausschließlich in Dateistruktur und Dateiinhalten.

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, 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).

Für die Smart Card mit Chip Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 (auch Einsatz der Applikation StarCert in unveränderter Weise) liegt die Bescheinigung nach §18(5) SigG vom 12.06.2001 vor.

Wien, 22.10.2001

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand