



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

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG: Prozessorchipkarte mit Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 v 7.0 und Digital Signature Application StarCert v 2.2

Antragsteller:
Datakom Austria GmbH
Wiedner Hauptstrasse 73
1040 Wien

1. Beschreibung der bescheinigten Komponente

Die bescheinigte Komponente ist eine Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus einer Prozessorchipkarte mit

- dem Smart Card Controller P8WE5032V0G von Philips Semiconductors Hamburg¹,
- dem Betriebssystem STARCOS SPK 2.3 v 7.0 von Giesecke & Devrient GmbH² und
- der Signaturanwendung (Digital Signature Application) StarCert v 2.2 von Giesecke & Devrient GmbH.

Die Signaturkarte stellt eine sichere Signaturerstellungseinheit dar und ermöglicht die Erzeugung und Speicherung der Signaturstellungsdaten und die Erstellung sicherer elektronischer Signaturen. Die Anzahl der Signaturen, die nach einer erfolgreichen Benutzerauthentifizierung mit der Signatur-PIN erstellt werden können, ist auf eine Signatur begrenzt (Grundkonfiguration K1).

Mit der Signaturkarte werden eine Komplettierungs-Datei³ v 7.0 und die Dokumentation laut Zertifizierungsbericht T-Systems-ITSEC-04075-2001⁴ geliefert.

Die Signaturanwendung StarCert v 2.2 stellt eine Kommando-Sequenz dar, die in der Initialisierungsphase angewandt wird und die ein Dateiensystem (Verzeichnis) auf die Signaturkarte lädt.

Die Signaturkarte wurde gemäß folgenden Normen implementiert:

- ISO/IEC 7816 Teile 1 bis 8,
- DIN V 66291 v 1.0 Teile 1-4,

¹ Unternehmensbereich der Philips GmbH, Business Line Identification, P.O. Box 54 02 40, D-22502 Hamburg

² Prinzregentenstraße 159, D-81607 München

³ Completion File

⁴ http://www.debiszert.de/pdf/ein_01_zer_itsec_cc/zr_04075_e.pdf

- HPC⁵ v 1.0 und
- OIC⁶ v 1.0.

2. Erfüllung der Anforderungen des SigG und der SigV

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1)⁷ und §18(2) zweiter Satz⁸ SigG,
- Anforderungen nach §7(3) SigV ausgenommen Anforderungen an die Hostanwendung⁹, 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 Signaturkarte ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung und Speicherung von Signaturerstellungsdaten,
- 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 zwei Jahre nach der Ausstellung gültig. Die Bescheinigung endet jedenfalls, sofern die deutsche Bestätigung T-Systems.02078.TE.12.2001¹⁰ vom 14.12.2001 in Deutschland die Gültigkeit verliert.

4. Einsatzbedingungen

Zusätzlich zu den Einsatzbedingungen aus der deutschen Bestätigung T-Systems.02078.TE.12.2001¹⁰ sind folgende Einsatzbedingungen gültig:

- (1) Die Signaturanwendung StarCert v 2.2 muss durch den Hersteller so konfiguriert werden, dass nach einer Eingabe der Signatur-PIN nur eine Signatur erstellt werden kann (Grundkonfiguration K1).
- (2) Es ist nicht zulässig, zusätzliche Anwendungen (d.h. ausführbare Codes) auf die Signaturkarte zu laden.
- (3) Am Ende der operationalen Nutzungsphase muss entweder die Signaturkarte physisch oder durch das TERMINATE CARD USAGE-Kommando zerstört werden oder die Signaturanwendung (StarCert) unwiderruflich unbrauchbar gemacht werden. Falls die Signaturerstellungsdaten ungültig werden, ohne dass die Nutzungsphase der Signaturkarte dadurch beendet ist, muss entweder das entsprechende Signaturschlüsselpaar dauerhaft gesperrt werden oder die Signaturanwendung (StarCert) unwiderruflich unbrauchbar gemacht werden.

⁵ Health Professional Card

⁶ Office Identity Card

⁷ 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.

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 Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungs-codes (z.B. PIN-Eingabe, Fingerabdruck) auslösbar sein. (...) Das unbefugte Erfahren der Autorisierungs-codes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (z.B. Signatur- und Bankomatfunktion) verwendbar sein. Signaturerstellungseinheiten, die mehrere Anwendungen zulassen, wie z.B. 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. (...).

¹⁰ http://www.t-systems-zert.de/pdf/ein_02_sig_pro/zf_02078_d.pdf

- (4) Der Signator darf die Signaturkarte nur mit einem bekannten und nicht-manipulierten Chipkartenlesegerät in einer bekannten und kontrollierten Umgebung verwenden.
- (5) Die Signaturschlüsselpaare müssen in einer sicheren Umgebung erzeugt werden (z.B. bei einem Zertifizierungsdiensteanbieter oder bei einer vom Zertifizierungsdiensteanbieter autorisierten Personalisierungsstelle).
- (6) Während der Erstpersonalisierung muss die Signaturkarte durch eine Personalisierung-PIN geschützt werden. Im Sicherheitskonzept des Zertifizierungsdiensteanbieters für qualifizierte Zertifikate müssen alle für eine sichere Personalisierung erforderlichen Maßnahmen beschrieben werden.

Anmerkung: Grundkonfiguration K2 ist bei einem Zertifizierungsdiensteanbieter zum Signieren qualifizierter Zertifikate zulässig, wobei die zusätzlichen Maßnahmen zur Sicherstellung der ausschließlichen Anwendbarkeit der Signaturerstellungsdaten in der vertrauenswürdigen Signaturumgebung ausreichend geprüft werden müssen¹¹.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer sicheren elektronischen Signatur wird vom Betriebssystem STARCOS SPK 2.3 v 7.0 der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit bereitgestellt und von der Signaturanwendung StarCert v 2.2 verwendet. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Smart Card Controller (HW):

Es liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0158-2001 für „Philips Smart Card Controller P8WE5032V0G“ vor, ausgestellt durch das Bundesamt für Sicherheit in der Informationstechnik¹² am 17.01.2001. Das Zertifikat weist der Komponente die Evaluationsstufe **E4** mit der Mindeststärke der Mechanismen „**hoch**“ nach ITSEC V1.2 aus. Die materiellen Prüfungen sind im Zertifizierungsbericht BSI-DSZ-ITSEC-0158-2001¹³ vom 17.01.2001 beschrieben.

Betriebssystem und Signaturanwendung StarCert:

Es liegt das Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-ITSEC-04075-2001¹⁴ für „STARCOS SPK 2.3 v7.0 with Digital Signature Application StarCert v 2.2“ vor, ausgestellt durch die Zertifizierungsstelle der T-Systems ISS GmbH¹⁵ am 14.12.2001. Dieses Zertifikat weist der Komponente die Evaluationsstufe **E4** mit der Mindeststärke der Mechanismen „**hoch**“ nach ITSEC V1.2 aus. Die materiellen Prüfungen sind im Zertifizierungsbericht T-Systems-ITSEC-04075-2001 vom 13.12.2001 beschrieben.

Integration:

Die sicherheitstechnisch korrekte Integration der technischen Komponente „STARCOS SPK 2.3 v7.0 with Digital Signature Application StarCert v 2.2“ und der Komponente „Philips Smart Card Controller P8WE5032V0G“ wurde im Rahmen der Bestätigung T-Systems.02078.TE.12.2001 überprüft. Diese Bestätigung von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und §§ Abs. 2 und 15 Signaturverordnung wurde von T-Systems ISS GmbH – Zertifizierungsstelle¹⁵ am 14.12.2001 ausgestellt.

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 A-SIT Bescheinigung nach §18(5) SigG vom 12.06.2001 vor. Die wesentlichen Unterschiede zur hiermit bescheinigten Komponente sind wie folgt:

¹¹ In Grundkonfiguration K2 kann nach einer Eingabe der Signatur-PIN eine unbegrenzte Anzahl der Signaturen erstellt werden.

¹² Godesberger Allee 185-189, D-53175 Bonn

¹³ <http://www.bsi.bund.de/zertifiz/zert/reporte/0158a.pdf>

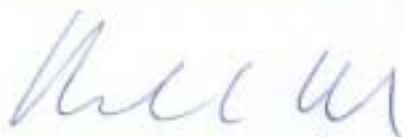
¹⁴ http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/zf_04075_e.pdf

¹⁵ Rabinstr. 8, D-53111 Bonn

- Completion Files als SW-Unterstützung für Protokolle T=0 bzw. T=0/T=1 (v 7.0¹⁶);
- StarCert v 2.2 (SW) ist eine Weiterentwicklung von StarCert, die insbesondere um die Funktionalität der SSL-Authentisierung ergänzt wurde. Die für den Zugriff auf die SSL- und/oder Entschlüsselungsschlüssel optional einzurichtende Global-PIN kann die Signaturfunktion nicht freischalten oder StarCert negativ beeinflussen; und
- Teile der Dokumentation.

Wien, 23.05.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand

¹⁶ „v 7.0“ bezieht sich auf Completion Files, und nicht auf STARCOS SPK 2.3