



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 Smart Card IC SLE 66CX320P und Betriebssystem CardOS/M4.01 (Version C803) und Applikation für digitale Signatur Version 0.20

Antragsteller:
Datakom Austria GmbH
Wiedner Hauptstrasse 73
1040 Wien

1. Beschreibung der bescheinigten Komponente

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

- Smart Card IC SLE 66CX320P von Infineon Technologies AG¹,
- Betriebssystem CardOS/M4.01 (Version C803) von Siemens AG² und
- Applikation für digitale Signatur (SigG Applikation) Version 0.20 von Siemens AG.

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 Benutzer-authentifizierung erstellt werden können, ist auf eine Signatur begrenzt (Konfiguration „n=1“).

Mit der Signaturkarte wird die Dokumentation laut Zertifizierungsbericht T-Systems-ITSEC-04067-2002³ geliefert.

Die Signaturkarte ist konform zu folgenden Normen:

- DIN V 66291-1 (bis auf lesenden Zugriff auf das Signator-Zertifikat C.CH.DS),
- ISO 7816 Teile 3, 4, 5, 8 und 9, und
- PKCS#11 Cryptographic Token Interface Standard.

¹ St.-Martin-Straße 76, D-81617 München

² ICN EN TNA, Charles-de-Gaulle-Straße 2-4, D-81737 München

³ http://www.debiszert.de/pdf/ein_01_zer_itsec_cc/zr_04067_d.pdf

2. Erfüllung der Anforderungen des SigG und der SigV

Die Chipkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1)⁴ und §18(2) zweiter Satz⁵ SigG,
- Anforderungen nach §7(3) SigV ausgenommen Anforderungen an die Hostanwendung⁶, 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 muss⁷.

Die Chipkarte 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.

4. Einsatzbedingungen

- (1) Die Signaturkarte muss durch den Hersteller so konfiguriert werden, dass nach einer Eingabe der Signatur-PIN nur eine Signatur erstellt werden kann (Konfiguration „n=1“).
- (2) Es darf nicht möglich sein, mit dem Autorisierungscode (d.h. PIN) für Zugriff auf andere auf der Signaturkarte befindliche Daten/Anwendungen (z.B. Bankomatfunktion) eine sichere Signatur auszulösen.
- (3) Es ist nicht zulässig, zusätzliche Anwendungen, die ausführbare Codes beinhalten, auf die Signaturkarte zu laden.
- (4) Am Ende der operationalen Nutzungsphase ist sicherzustellen, dass die Signaturkarte nicht mehr anwendbar ist und der Signaturschlüssel vernichtet wird.
- (5) Der Signator darf die Signaturkarte nur mit einem ihm bekannten und nicht-manipulierten Chipkartenleser in einer sicheren und kontrollierten Umgebung verwenden. Dies bedeutet in der Praxis, dass die Sicherheit der Funktionen des Chipkartenlesers beim Einsatz gewährleistet sein muss.
- (6) Die Anforderung AE4.2 aus den Sicherheitsvorgaben (siehe Zertifizierungsbericht T-Systems-ITSEC-04067-2002⁸) muss erfüllt werden.

⁴ 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.

⁵ 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.

⁶ 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 Sperremechanismen 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. (...).

⁷ 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), (...), 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; (...).

⁸ http://www.debiszert.de/pdf/ein_01_zer_itsec_cc/zr_04067_d.pdf

- (7) Die Signaturschlüsselpaare müssen in einer sicheren Umgebung erzeugt werden (z.B. bei einem Zertifizierungsdiensteanbieter oder bei einer vom Zertifizierungsdiensteanbieter autorisierten Registrierungsstelle).
- (8) Von den Abläufen der Komplettierung, Initialisierung und Personalisierung gemäß „CardOS/M4.01 Delivery, Generation and Configuration, Version 1.1“ vom 18.12.2001 und „CardOS/M4.01 Documentation for Trust Center, Version 1.02“ vom 27.02.2002 darf nicht abgewichen werden. Diese Abläufe müssen Bestandteil des Sicherheitskonzepts des Zertifizierungsdiensteanbieters sein. Die Personalisierungsscripte dürfen nur an den durch Kommentare kenntlich gemachten Stellen im Sinne der Kommentare angepasst werden.

Anmerkung: Konfiguration „n≠1“⁹ ist bei einem Zertifizierungsdiensteanbieter für qualifizierte Zertifikate zulässig, wobei die zusätzlichen Maßnahmen zur Sicherstellung der ausschließlichen Anwendbarkeit der Signaturerstellungsdaten in der vertrauenswürdigen Signaturumgebung ausreichend geprüft werden müssen.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer sicheren elektronischen Signatur wird vom Betriebssystem CardOS/M4.01 der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit bereitgestellt und von der Applikation für digitale Signatur verwendet. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 und Anhang 2 Punkt 3 SigV erfüllt. Das CRT¹⁰ wird nicht verwendet.

6. Prüfstufe und Mechanismenstärke

Smart Card IC (HW):

Es liegt das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-ITSEC-9115-2000 für „chipcard security controller SLE 66CX320P“ (Smart Card IC SLE 66CX320P, version m1421b14) von Infineon Technologies AG vor, ausgestellt durch die TÜViT GmbH Zertifizierungsstelle¹¹ am 04.08.2000. Das Zertifikat weist der Komponente die Evaluationsstufe **E4** mit der Mindeststärke der Mechanismen „hoch“ nach ITSEC V1.2. Die materiellen Prüfungen sind im Zertifizierungsbericht TUVIT-DSZ-ITSEC-9115 vom 04.08.2000 beschrieben.

Betriebssystem und Applikation für digitale Signatur:

Es liegt das Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-CC-04067-2002 für „CardOS/M4.01 mit Applikation für digitale Signatur“ der Siemens AG vor, ausgestellt durch die Zertifizierungsstelle der T-Systems ISS GmbH¹² am 06.03.2002. Dieses Zertifikat weist der Komponente die Evaluierungsstufe **E4** mit der Mindeststärke der Mechanismen „hoch“ nach ITSEC V1.2 aus. Die materiellen Prüfungen sind im Zertifizierungsbericht T-Systems-ITSEC-04067-2002 vom 06.03.2002 beschrieben.

Integration:

Die sicherheitstechnisch korrekte Integration der technischen Komponente „chipcard security controller SLE 66CX320P“ und der Komponente „CardOS/M4.01 mit Applikation für digitale Signatur“ wurde im Rahmen der Zertifizierung von der Zertifizierungsstelle der T-Systems ISS GmbH überprüft: Das Zertifikat T-Systems-DSZ-CC-04067-2002 gilt nur für CardOS/M4.01 mit Applikation für digitale Signatur in Verbindung mit der Hardware SLE 66CX320P.

⁹ nach einer Eingabe der Signatur-PIN kann eine unbegrenzte (n=0 oder n=255) oder begrenzte (1<n<255) Anzahl der Signaturen erstellt werden

¹⁰ Chinese Remainder Theorem

¹¹ Am Technologiepark 1, D-45307 Essen

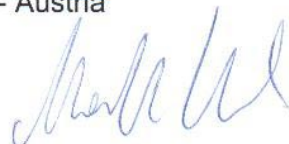
¹² Rabinstr. 8, D-53111 Bonn

Wien, 13.05.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand