Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
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

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

Sichere Signaturerstellungseinheit ACOS EMV-A04V1, Konfiguration A+B

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

Bescheinigung ausgestellt am: 23.06.2016
Referenznummer A-SIT-VI-15-061

1. Beschreibung der zu bescheinigenden Komponente

Die zu bescheinigende Komponente ist eine Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus:

- Smart Card IC NXP SmartMX P5CC037V0A[1], Hersteller: NXP Semiconductors Germany GmbH, Stresemannallee 101, 22529 Hamburg
- Betriebssystem ACOS EMV- A04V1 (ROM Maske AC_A04_V1R1.hex vom 18.12.2007), Hersteller Austria Card Plastikkarten und Ausweissysteme GmbH, Lamezanstraße 4-8, 1232 Wien
- Applikation für digitale Signatur gemäß „Specification of the generic Secure Signature Application for ACOS EMV-A04, Version 1.1", Hersteller Austria Card Plastikkarten und Ausweissysteme GmbH, Lamezanstraße 4-8, 1232 Wien

Mit der Signaturkarte wird die folgende Dokumentation laut Nachtrag Nr. 3 zur Sicherheitsbestätigung T-Systems.02166.TE.07.2008 geliefert:

- Administrator Guidance – Version 1.6, Austria Card GmbH
- User Guidance – Version 1.6, Austria Card GmbH
- Specification of the generic Secure Signature Application for ACOS EMV-A04, Version 1.1, Austria Card GmbH, 2008
- Delivery and Operation Documentation – Delivery, Installation and Generation, Version 1.2, Austria Card GmbH, 03.04.2008
- ACOS EMV-A04 Commands (Command specification), Version 2.2, Austria Card GmbH
- ACOS EMV-A04 Init-Pers-Concept, Version 1.3, Austria Card GmbH, 2008

[1] Der Prozessorchip NXP SmartMX P5CC037V0A wurde vom BSI zertifiziert. Der Zertifizierungsreport BSI-DSZ-CC-0465-2008 vom 20.6.2008 (ergänzt um BSI-DSZ-CC-0465-2008-MA-01 vom 7.9.2009, BSI-DSZ-CC-0465-2008-MA-02 vom 31.7.2012 und BSI-DSZ-CC-0465-2008-MA-04 vom 19.12.2013) weist der Komponente eine Konformität zum Schutzprofil BSI-PP-0002-2001 (Smartcard IC Platform Protection Profile, Version 1.0) sowie die erfolgreiche Evaluierung nach der Prüfstufe EAL5+ (Erweiterungen: ALC_DVS.2: Lebenszyklus-Unterstützung – Ausreichende Sicherheitsmaßnahmen, AVA_MSU.3: Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände und AVA_VLA.4: Schwachstellenbewertung – Hohe Widerstandsfähigkeit) aus.

Die Applikation für digitale Signatur ist in einer von zwei möglichen Konfigurationen („Konfiguration A“ bzw. „Konfiguration B“) in den EEPROM der Signaturkarte geladen. Konfiguration A erzwingt die Verwendung von Secure Messaging zwischen der Signaturkarte und der IT-Einsatzumgebung. Konfiguration B unterstützt Secure Messaging aber gestattet auch die Verwendung der Signaturkarte ohne Secure Messaging in einer vertrauenswürdigen Einsatzumgebung. Die Konfiguration wird während der Initialisierung der Signaturkarte beim Hersteller Austria Card bestimmt und kann nicht mehr verändert werden. Die gegenständliche Bescheinigung ist für Konfiguration A und Konfiguration B gültig.

Die Signaturkarte verwendet zur Erstellung sicherer Signaturen entweder das RSA Verfahren mit Schlüssellängen von 1280 Bit bis 2048 Bit oder das ECDSA Verfahren mit Schlüssellängen von 192 Bit bis 256 Bit (siehe Kapitel 5 dieser Bescheinigung). Das verwendete Verfahren und die zugehörigen Parameter sind vom Zertifizierungsdiensteanbieter im Zuge der Signaturschlüsselgenerierung zu wählen.

2. Erfüllung der Anforderungen des SigG[2] und der SigV[3]

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1[4] und § 18 Abs. 2 zweiter Satz[5] SigG,
- Anforderungen nach § 3 Abs. 1[6] und § 3 Abs. 2[7] SigV und
- Anforderungen nach § 6 Abs. 1[8] und § 6 Abs. 2[9] SigV.

Die Signaturkarte 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

Die Gültigkeit dieser Bescheinigung gilt bis auf Widerruf durch A-SIT. A-SIT führt bei Beauftragung eine laufende Evidenthaltung und ein Monitoring hinsichtlich der Sicherheit der eingesetzten Produkte und Verfahren sowie der kryptografischen Algorithmen und Parameter durch. Mit der Ausstellung dieser Bescheinigung ist ein Monitoring für zwei Jahre verbunden. Der Widerruf erfolgt sofern die Sicherheit der eingesetzten Produkte und Verfahren sowie der kryptografischen Algorithmen und Parameter nicht mehr dem Stand der Technik entsprechen bzw. kein weiteres Monitoring beauftragt wird.

---

[2] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19.August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 75/2010 vom 18. August 2010.

[3] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)) in der Fassung BGBl. II Nr. 401/2010 vom 9. Dezember 2010.

[4] Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter 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 technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

[7] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

[8] Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es 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. (...)

[9] Bei den Prüfungen nach Abs. 1 sind insbesondere Referenznummern zu beachten, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrichtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices – SSCD) oder vertrauenswürdige Systeme oder Produkte des ZDA veröffentlicht wurden.

4. Einsatzbedingungen

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

(1) Die mit der Signaturkarte ausgelieferte Dokumentation (siehe Kapitel 1 dieser Bescheinigung) enthält die notwendigen Anweisungen für den sicheren Gebrauch der Signaturkarte. Zusätzlich sind für den sicheren Gebrauch der Signaturkarte die Annahmen über die Einsatzumgebung im Security Target, sowie das Security Target als Ganzes in Betracht zu ziehen. Diesen Anweisungen und Annahmen ist 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 der Signatorin bzw. des Signators entsprechend zu übernehmen
- und deren Wirkung im Wege der Aufsicht sicherzustellen.

(2) Die Benutzerin bzw. der Benutzer der Signaturkarte muss in geeigneter Weise davon in Kenntnis gesetzt werden, dass sie bzw. er die Signaturkarte in Konfiguration A oder Konfiguration B (siehe Kapitel 1 dieser Bescheinigung) verwendet.

(3) Die Signaturkarte in Konfiguration B darf zur Erstellung von qualifizierten Signaturen nur in einer vertrauenswürdigen Einsatzumgebung verwendet werden. Diese Einsatzumgebung muss die Vertraulichkeit und Integrität der von der Signatorin bzw. vom Signator eingegebenen Autorisierungscodes sowie die Integrität der zu signierenden Daten bei deren Übermittlung an die Signaturkarte schützen.

(4) Bei der Generierung der Signaturerstellungsdaten auf der Signaturkarte sind der Signaturalgorithmus und die Signaturschlüssellänge so zu wählen, dass diese für die gesamte vorgesehene Einsatzdauer der Signaturkarte den gesetzlichen Anforderungen entsprechen.

(5) Die folgenden Einsatzbedingungen sind gemäß der Evaluierung der Signaturkarte durch den Hersteller einzuhalten:

a. Die Konfigurationsdateien filesys.fsd, buergerk.fsd und profile.h sind nach Änderungen auf “malicious links” zu prüfen, bevor sie für die Signaturkarte verwendet werden.

b. Bei Änderungen an filesys.fsd und buergerk.fsd sind die Anforderungen in Secure Patching for ACOS A04, Version 1.2, zu beachten.

c. Die Datei profile.h enthält „Schalter“ zur einfachen Konfiguration verschiedener Optionen; bei Änderung dieser Schalter sind die Anforderungen aus *Specification of the generic Secure Signature Application for ACOS EMV-A04*, Kap. 7 zu beachten.

d. Die Festlegung von Configuration A oder Configuration B erfolgt durch Anpassung des Schalters CONF_A in profile.h; dies darf nicht durch direkte Modifikation der Sicherheitsattribute von filesys.fsd oder buergerk.fsd erfolgen.

e. Bei einer Änderung in filesys.fsd, buergerk.fsd oder profile.h, die zu einer Änderung der Datei filesys.a51 führt, sind alle Tests aus *Testplan Common Criteria*, Version 1.2, zu wiederholen; für jede so entstehende Variante der Signaturkarte sind die Testprotokolle zu archivieren; die Testprotokolle müssen hinreichend aussagekräftig sein, um feststellen zu können, ob verwendete Signaturkarten zur einer evaluierten Konfiguration gehören oder nicht.

f. Das Kommando LOAD COMPLETION DATA darf bei der Initialisierung der Signaturkarte nicht verwendet werden.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur werden von der Signaturkarte entweder der RSA Algorithmus nach PKCS #1, Version 2.1 mit Schlüssellängen von 1280 bis 2048 Bit oder der ECDSA Algorithmus nach ANSI X9.62[10] mit Schlüssellängen[11] von 192 bis 256 Bit bereit gestellt.[12]

Zur Berechnung des Hashwertes werden von der Signaturkarte die Algorithmen SHA-1, SHA-224 und SHA-256 nach FIPS PUB 180-4 bereitgestellt.[13]

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV[14] erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifkat T-Systems-DSZ-CC-04164/04165-2008 vor, ausgestellt durch die T-Systems GEI GmbH, in Bonn am 11.07.2008. Die materiellen Prüfungen sind im Zertifizierungsbericht „Certification Report T-Systems-DSZ-CC-04164/04165-2008 ACOS EMV-A04V1“ beschrieben.

Das Zertifikat weist der Signaturkarte die erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA_MSU.3[15], AVA_VLA.4[16]) der Common Criteria (CC) in Version 2.3 aus. Weiters weist es der Signaturkarte in Konfiguration A die Konformität mit dem Schutzprofil „Secure Signature-Creation Device, Type 3, Version: 1.05, EAL 4+, 25 July 2001, BSI-PP-0006-2002“ aus.

Die Signaturkarte widersteht in ihrer vorgesehenen Einsatzumgebung einem hohen Angriffspotential.

Die dieser Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VI-15-061 dokumentiert.

Unterschrift:

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2016-06-23T16:51:03+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	

[10] DSA basierend auf einer Gruppe E(F_p)
[11] Parameter q
[12] Anmerkung: Davon können zum Ausstellungszeitpunkt dieser Bescheinigung nur mehr RSA mit Schlüssellängen ab 1900 Bit, sowie ECDSA mit einer Schlüssellänge von 256 Bit als dem Stand der Technik angesehen werden (vgl. SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.0, www.sogis.org).
[13] Anmerkung: Davon kann zum Ausstellungszeitpunkt dieser Bescheinigung nur mehr SHA-256 als dem Stand der Technik angesehen werden.
[14] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.
[15] Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände
[16] Schwachstellenbewertung – Hohe Widerstandsfähigkeit