



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

DVR: 1035461

ZVR: 948166612

BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

Sichere Signaturerstellungseinheit ACOS EMV-A03V1 Konfiguration A

Antragsteller:
Austria Card Plastikkarten und Ausweissysteme GmbH
Lamezanstraße 4-8
A-1232 Wien

Bescheinigung ausgestellt am: 07.02.2008
Referenznummer A-SIT-1.073

1. Beschreibung der zu bescheinigenden Komponente

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

- Smart Card IC Philips SmartMX P5CC036V1D, Hersteller: NXP Semiconductors Germany GmbH¹, Stresemannallee 101, D-22529 Hamburg
- Betriebssystem ACOS EMV-A03 (ROM Maske AC000004.hex vom 19.12.2003), 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 EMVA03, Version 1.7“, Hersteller Austria Card Plastikkarten und Ausweissysteme GmbH, Lamezanstraße 4-8, 1232 Wien

Mit der Signaturkarte wird die folgende Dokumentation laut Zertifizierungsbericht BSI-DSZ-CC-0346-2006 geliefert:

- Administrator Guidance – Evaluation of ACOS EMV-A03V0, Version 1.20, Austria Card GmbH, 28.07.2004
- User Guidance – Evaluation of ACOS EMV-A03V0, Version 1.10, Austria Card GmbH, 26.07.2004
- Specification of the generic Signature Application for ACOS EMV-A03, Version 1.7, Austria Card GmbH, 16.09.2004
- ADO_DEL.2, ADO_IG1, BSI-DSZ-CC-0220 and BSI-DSZ-CC-0221, Version 1.20, Austria Card GmbH, 23.06.2004
- Commands for ACOS EMV-A03, Version 1.2-Release, Austria Card GmbH, 31.03.2004
- ACOS EMV-A Init-Pers-Concept, Version 3.04, Austria Card GmbH, Revised on 27.07.2004

¹ Ehem.: Philips Semiconductors GmbH

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 ausschließlich für Konfiguration A gültig.

Die Signaturkarte verwendet zur Erstellung qualifizierter Signaturen entweder das RSA Verfahren mit Schlüssellängen von 1024 Bit bis 2048 Bit oder das ECDSA Verfahren mit Schlüssellängen von 160 Bit bis 256 Bit (siehe Punkt 5). Das verwendete Verfahren und die zugehörigen Parameter sind vom Zertifizierungsdiensteanbieter im Zuge der Signaturschlüsselgenerierung zu wählen.

2. Erfüllung der Anforderungen des SigG² und der SigV³

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Die Anforderung⁴ nach § 18 Abs. 6 SigG.

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

Diese Bescheinigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

Die Gültigkeit endet jedenfalls, wenn das IT-Sicherheitszertifikat BSI-DSZ-CC-0346-2006 vom 20.1.2006 seine Gültigkeit verliert.

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 § 12 SigV des Zertifizierungsdiensteanbieters sicherzustellen,
 - in der Belehrung des Signators entsprechend zu übernehmen
 - und deren Wirkung im Wege der Aufsicht sicherzustellen.
- (2) Der Benutzer der Signaturkarte muss in geeigneter Weise davon in Kenntnis gesetzt werden, dass er die Signaturkarte in Konfiguration A (siehe Kapitel 1 dieser Bescheinigung) verwendet.

² Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 8/2008 vom 7. Jänner 2008.

³ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)

⁴ Entsprechen technische Komponenten und Verfahren den allgemein anerkannten Normen, die von der Europäischen Kommission nach Art. 3 Abs. 5 der Signaturrechtlinie festgelegt werden, so gelten die entsprechenden Sicherheitsanforderungen nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen als erfüllt.

- (3) Neben der Applikation für digitale Signatur dürfen nur solche Applikationen mit ausführbarem Code auf die Signaturkarte geladen werden, die keinen negativen Einfluss auf die Applikation für digitale Signatur haben. Diese Eigenschaft ist durch einen Evaluator in geeigneter Form nachzuweisen. Eine Liste der Applikationen, die im Zuge der Evaluierung⁵ der Signaturkarte getestet wurden, ist im Anhang A dieser Bescheinigung wiedergegeben.
- (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. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur werden von der Signaturkarte entweder der RSA Algorithmus nach PKCS #1, Version 1.5 mit Schlüssellängen von 1024 bis 2048 Bit oder der ECDSA Algorithmus nach ANSI X9.62⁶ mit Schlüssellängen⁷ von 160 bis 256 Bit bereit gestellt.

Zur Berechnung des Hashwertes wird von der Signaturkarte der Algorithmus SHA-1 nach FIPS 180-1 bereitgestellt.

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV⁸ erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0346-2006 vor, ausgestellt durch das Bundesamt für die Sicherheit in der Informationstechnik (BSI), in Bonn am 20.1.2006. Die materiellen Prüfungen sind im Zertifizierungsbericht „Certification Report BSI-DSZ-0346-2006“ beschrieben.

Das Zertifikat weist der Signaturkarte die Konformität zum Schutzprofil BSI-PP-0006-2002⁹ aus. Dadurch ist die Anforderung gemäß § 18 Abs. 6 SigG erfüllt.

Das Zertifikat weist der Signaturkarte die erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA_MSU.3¹⁰, AVA_VLA.4¹¹) der Common Criteria (CC) aus.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke „hoch“.

⁵ Durch den Evaluator: T-Systems GEI GmbH, Business Unit ITC-Security, Rabinstraße 8, 53111 Bonn

⁶ DSA basierend auf einer Gruppe $E(F_p)$

⁷ Parameter q


⁸ 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.


⁹ Dieses Schutzprofil entspricht dem CWA 14169 (Protection Profile for the SSCD Type 3) im „Verzeichnis allgemein anerkannter Normen für Produkte für elektronische Signaturen, die von den Mitgliedsstaaten angenommen werden sollen in Übereinstimmung mit den Anforderungen des Anhangs III der Richtlinie 1999/93/EG.“, veröffentlicht im Amtsblatt der Europäischen Union L 175/45 vom 15.7.2003

¹⁰ Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände

¹¹ Schwachstellenbewertung – Hohe Widerstandsfähigkeit

Unterschriften:

| | | |
|---|--|--|
| Signaturwert | 9IEEnK1Rl5d9gMqubqTuUdUIoi5S0685Ykm83PN0Vint/EFHxiLNdXulWzSMBprgM | |
|  | Unterzeichner | Manfred Holzbach, Geschäftsführender Vorstand |
| | Datum/Zeit-UTC | 2008-02-07T13:49:46Z |
| | Aussteller-Zertifikat | CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT |
| | Serien-Nr. | 97349 |
| | Methode | urn:pdfsigfilter:bka.gv.at:text:v1.1.0 |
| | Parameter | etsi-bka-1.0@1202392186-3562343@28730-26910-0-26290-14800 |
| Prüfhinweis | Informationen zur Signaturprüfung finden Sie unter: www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php . | |

| | | |
|---|--|--|
| Signaturwert | IyIi24AuvAA2lY2X1cJHBHEbOoqpn7ktDUF730Ben9XUO5JtgAMdWSQo111x8HbH | |
|  | Unterzeichner | Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter |
| | Datum/Zeit-UTC | 2008-02-07T19:46:48Z |
| | Aussteller-Zertifikat | CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT |
| | Serien-Nr. | 221297 |
| | Methode | urn:pdfsigfilter:bka.gv.at:text:v1.1.0 |
| | Parameter | etsi-bka-1.0@1202413608-120320497@20114-22365-0-10677-17147 |
| Prüfhinweis | Prüfservice: http://demo.a-sit.at/el_signatur/verification | |

Anhang A – Applikationen

Die Signaturkarte wurde mit den in der folgenden Tabelle genannten Applikationen durch den Evaluator T-Systems GEI GmbH, Business Unit ITC-Security, Rabinstraße 8, 53111 Bonn getestet.

| Name der Applikation | AID (Applikation Identifier) | Kurzbeschreibung |
|--------------------------|------------------------------|---|
| EMV Maestro | A0000000043060 | Internationale EMV Applikation, Version 2.1 |
| EMV MasterCard | A0000000041010 | Internationale EMV Applikation, Version 2.1 |
| EMV ATM Maestro | D0400000190001 | Inländische EMV Applikation, Version 2.1 |
| EMV POS Maestro | D0400000190002 | Inländische EMV Applikation, Version 2.1 |
| EMV ATM MasterCard | D0400000190003 | Inländische EMV Applikation, Version 2.1 |
| EMV POS MasterCard | D0400000190004 | Inländische EMV Applikation, Version 2.1 |
| Quick (IEP) | D040000001000002 | Inländisches Zahlungssystem, Version 2.1 |
| ATM | D040000004000002 | Inländisches Zahlungssystem, Version 2.1 |
| POS | D040000003000002 | Inländisches Zahlungssystem, Version 2.1 |
| RFU | D040000002000002 | Inländisches Zahlungssystem, Version 2.1 |
| Retail | D04000000B000002 | Inländisches Loyalitätsprogramm, Version 2.1 |
| Bank_Data | D04000000C000002 | Inländisches Loyalitätsprogramm, Version 2.1 |
| Shopping | D04000000D000002 | Inländisches Loyalitätsprogramm, Version 2.1 |
| Digital ID | D0400000190010 | Inländisches Zahlungssystem, Version 2.1 |
| Digital Signature (SSCA) | A0000001184543 | Applikation für digitale Signatur |
| Encryption Application | A000000118454E | Applikation für Verschlüsselung, Version 1.10 |
| DF_UNI_Ausweis | D040000015000001 | Inländisches Loyalitätsprogramm, Version 2.0 |
| DF_UNI_Kepler1 | D040000013000001 | Inländisches Loyalitätsprogramm, Version 2.0 |
| DF_UNI_Kepler2 | D040000013000002 | Inländisches Loyalitätsprogramm, Version 2.0 |
| DF_Mensa | D040000014000001 | Inländisches Loyalitätsprogramm, Version 2.0 |
| DF_KEP_SIG | A000000118040000 | Inländisches Loyalitätsprogramm, Version 1.32 |
| DF_Ausweis | D040000015000001 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Schüler1 | D040000013000001 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Schüler2 | D040000013000002 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Verkehr | A000000118010000 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Partner | A000000118020000 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Schülerdaten | A000000118030000 | Inländisches Loyalitätsprogramm, Version 1.3 |
| DF_Schul_SIG | A000000118040000 | Inländisches Loyalitätsprogramm, Version 1.32 |