



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

BESCHEINIGUNG NACH §18(5) SIGG

Sichere Signaturerstellungseinheit ACOS EMV-A03V0 Konfiguration B

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

1. Beschreibung der zu bescheinigenden Komponente

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

- Smart Card IC Philips SmartMX P5CC036V0M, Hersteller: Philips Semiconductors GmbH, Stresemannallee 101, 22529 Hamburg
- Betriebssystem ACOS EMV-A03V0 (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-0221-2004 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

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 B gültig.

Die Signaturkarte verwendet zur Erstellung sicherer 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 SigG¹ und der SigV²

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen die in den jeweiligen Fußnoten angeführten

- Anforderungen nach §18(1)³ und §18(2) zweiter Satz⁴ SigG,
- Anforderungen nach §3(3)⁵, §3(4)⁶ und §3(5)⁷ SigV,
- Anforderungen nach §4(1)⁸ SigV,
- Anforderungen nach §7(1)⁹ und §7(3)¹⁰ SigV und
- die Anforderung nach §9(2)¹¹ SigV.

Die Signaturkarte 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 für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

¹ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

² Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 vom 2. Februar 2000.

³ 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.

⁴ 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

⁵ Die Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang 1 Punkt 2 festgesetzte Mindestlänge aufweisen. (...) Die verwendeten Algorithmen müssen offengelegt sein. Die Signaturerstellungsdaten für sichere elektronische Signaturen dürfen mit an Sicherheit grenzender Wahrscheinlichkeit ausschließlich beim Signator vorkommen. Sie müssen nach dem jeweiligen Stand der Technik den eindeutigen Rückschluss auf den Signator ermöglichen. (...)

⁶ Wiederholte Anwendungen der Signaturerstellungsdaten für sichere elektronische Signaturen dürfen nicht zu einer Verminderung der Schlüsselqualität führen. Anwendungen, die die Qualität der Signaturerstellungsdaten vermindern können (zB RSA-Anwendungen auf zufällig gewählte Daten), müssen wirksam ausgeschlossen sein. Die Signaturerstellungsdaten dürfen nur für diejenigen Zwecke verwendet werden, für die sie bestimmt sind.

⁷ Die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein signatorbezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang 1 Punkt 3 festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein (qualitätsvoller Zufall). Die Zufallselemente müssen auf ihre Eignung hin ausreichend geprüft sein. Pseudozufallszahlen dürfen nicht als Ausgangsbasis verwendet werden. (...)

⁸ Die Speicherung der Signaturerstellungsdaten für sichere elektronische Signaturen hat so zu erfolgen, dass deren Bekanntwerden ausgeschlossen ist und ihre Verwendung unter der ausschließlichen Kontrolle des Signators steht. Das Duplizieren von Signaturerstellungsdaten nach deren Erzeugung ist nicht zulässig.

⁹ Die Signatoren dürfen für die Erstellung sicherer elektronischer Signaturen nur solche Hashverfahren und Verfahren zur Verschlüsselung des Hashwertes einsetzen, die im Anhang 2 Punkt 2 und 3 genannt sind.

¹⁰ Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungs-codes (zB PIN-Eingabe, Fingerabdruck) auslösbar sein. (...) Das unbefugte Erfahren der Autorisierungs-codes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. (...)

¹¹ 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), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) oder dem British Standard (BS) 7799, 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;

Anmerkung: Die Evaluierung nach der Prüfstufe EAL4+ nach Common Criteria entspricht der Evaluationsstufe E 3 nach ITSEC.

Die Gültigkeit endet jedenfalls, wenn das IT-Sicherheitszertifikat BSI-DSZ-CC-0221-2004 vom 24.11.2004 seine Gültigkeit verliert.

4. Einsatzbedingungen

Die Gültigkeit dieser Bescheinigung ist an die im Folgenden angeführten Auflagen 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 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 B (siehe Kapitel 1 dieser Bescheinigung) verwendet.
- (3) Die Signaturkarte darf zur Erstellung von sicheren Signaturen nur in einer vertrauenswürdigen Einsatzumgebung verwendet werden. Diese Einsatzumgebung muss die Vertraulichkeit und Integrität der vom Signator eingegebenen Autorisierungs-codes sowie die Integrität der zu signierenden Daten bei deren Übermittlung an die Signaturkarte schützen.
- (4) 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 Evaluierung¹² der Signaturkarte getestet wurden, ist im Anhang A dieser Bescheinigung wiedergegeben.
- (5) 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 sicheren 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 X9.62-1998¹³ mit Schlüssellängen¹⁴ von 160 bis 256 Bit bereit gestellt. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 SigV sowie Anhang 2 Punkt 3 SigV erfüllt.

Zur Berechnung des Hashwertes wird von der Signaturkarte der Algorithmus SHA-1 nach FIPS 180-1 bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 2 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0221-2004 vor, ausgestellt durch das Bundesamt für die Sicherheit in der Informationstechnik (BSI), in Bonn am 24.11.2004. Die materiellen Prüfungen sind im Zertifizierungsbericht „Certification Report BSI-DSZ-0221-2004“ beschrieben.

¹² Durch den Evaluator: T-Systems GEI GmbH, Business Unit ITC-Security, Rabinstraße 8, 53111 Bonn

¹³ DSA basierend auf einer Gruppe $E(F_p)$

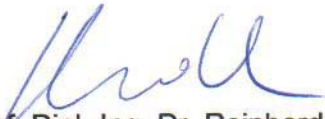
¹⁴ Parameter q

Das Zertifikat weist der Signaturkarte die erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA_MSU.3¹⁵, AVA_VLA.4¹⁶) der Common Criteria (CC) aus.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke „hoch“.

Wien, 20.12.2004

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand

¹⁵ Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände

¹⁶ Schwachstellenbewertung – Hohe Widerstandsfähigkeit

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