



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-A03V0 Konfiguration B

Antragsteller:

A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH
Landstraßer Hauptstraße 5
1030 Wien

Bescheinigung ausgestellt am: 17.12.2008
Referenznummer A-SIT-1.080

1. Beschreibung der zu bescheinigenden Komponente

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

- Smart Card IC NXP SmartMX P5CC036V0M, Hersteller: NXP Semiconductors Germany GmbH¹, 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

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 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 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 SigG² und der SigV³

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1⁴ und § 18 Abs. 2 zweiter Satz⁵ SigG,
- Anforderungen nach § 3 Abs. 1⁶ und § 3 Abs. 2⁷ SigV und
- Anforderungen nach § 6 Abs. 1⁸ und § 6 Abs. 2⁹ 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

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-0221-2004 vom 24.11.2004 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

² Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008 vom 22. April 2008.

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

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.

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 qualifizierten 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 Evaluierung¹⁰ 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 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 X9.62¹¹ mit Schlüssellängen¹² von 160 bis 256 Bit bereit gestellt.

Zur Berechnung des Hashwertes wird von der Signaturkarte der Algorithmus SHA-1 nach FIPS 180-1 bereitgestellt.¹³

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV¹⁴ 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.

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“.

¹⁰ Durch den Evaluator: T-Systems GEI GmbH, Business Unit ITC-Security, Rabinstraße 8, 53111 Bonn

¹¹ DSA basierend auf einer Gruppe $E(F_p)$

¹² Parameter q


¹³ Anmerkung: Zur Eignung der Hashfunktion SHA-1 kann zum Zeitpunkt der Ausstellung dieser Bescheinigung auf Grund neuer Methoden zur Kollisionssuche keine Prognose bezüglich des uneingeschränkten Einsatzes bei der Erstellung von qualifizierten elektronischen Signaturen gegeben werden. Es wird daher empfohlen, die Berechnung des Hashwertes nicht von der Signaturerstellungseinheit selbst sondern durch eine Applikation in der Systemumgebung der Signaturerstellungseinheit durchführen zu lassen und dabei andere Hashfunktionen, die für einen längeren Zeitraum als geeignet betrachtet werden können, einzusetzen.


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

Unterschriften:

Signaturwert	LmltaCXxT6RBwMWsfisDOJBhoYeOfz/ti/DExC682wKeScl/tpnikJ687YDCrX19	
	Unterzeichner	serialNumber=332198315605,givenName=Manfred,SN=Holzbach,CN=Manfred Holzbach,C=AT
	Datum/Zeit-UTC	2008-12-17T12:54:22Z
	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.	261828
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1229518462-20445484@15711-11924-0-26054-20208
Prüfhinweis	Prüfservice: http://demo.a-sit.at/el_signatur/verification	

Signaturwert	JeJtMmhRl9sPxvwAIXfusMfA2HlzCPL6DiSDj0VGG8bSV84He0moC6AA1ZSO5SG0	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2008-12-17T14:29:48Z
	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@1229524188-1333656@2393-26636-0-17854-14520
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	