Sicherheitsbestätigung und Bericht

T-Systems.02166.TE.07.2008

ACOS EMV-A04V1

Austria Card
Plastikkarten und Ausweissysteme GmbH

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 und 15 Signaturverordnung[2]

T-Systems GEI GmbH
- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §§ 15 Abs. 1 und 4, § 11 Abs. 3 SigV,
dass die

Signaturerstellungseinheit
„ACOS EMV-A04V1“

der

Austria Card Plastikkarten und Ausweissysteme GmbH

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02166.TE.07.2008

Bonn, den 18.07.2008

(Dr. Heinrich Kersten)

Die T-Systems GEI GmbH – Zertifizierungsstelle - ist gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

[1] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer T-Systems.02166.TE.07.2008 besteht aus 10 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit „ACOS EMV-A04V1“,
im Folgenden als SSEE bezeichnet.

Die SSEE besitzt die beiden Konfigurationen `Configuration A` und `Configuration B` (s. Funktionsbeschreibung), die vom Hersteller festgelegt werden und bei Auslieferung als Zusatz zur Handelsbezeichnung angegeben werden.

Die vorliegende Bestätigung betrifft beide Konfigurationen.

1.2 Auslieferung

Die verschiedenen Schritte und Formen der Auslieferung der SSEE und die dazu gehörenden Verfahren der Initialisierung und Personalisierung sind in [6] (s. Tabelle unten) in englischer Sprache beschrieben. Die Beschreibung enthält folgende Abschnitte:

ROM-FILE GENERATION
DELIVERY DVL → CHIP MANUFACTURER
DELIVERY CHIP MANUFACTURER → CARD MANUFACTURER
DELIVERY DEVELOPER → CARD MANUFACTURER
DELIVERY CARD MANUFACTURER → TRUST CENTER (FOR PRE-PERSONALIZATION)
DELIVERY TRUST CENTER → CARDHOLDER
DELIVERY CARDHOLDER → TC-RA
DELIVERY TC-RA → CARDHOLDER

(DVL = Entwickler, TC-RA = RA des ausgebenden ZDA)

1.3 Lieferumfang

Der Lieferumfang ist für beide Konfigurationen der SSEE identisch:

Nr.	Typ	Name	Art der Auslieferung
1	HW/SW	NXP SmartMx P5CC037V0A mit Austria Card ROM Maske AC_A04_V1R1.hex vom 18.12.2007	Smartcard mit ROM Code

Nr.	Typ	Name	Art der Auslieferung
2	SW	Digital Signature Application (gemäß Spezifikation Nr. 5)	EEPROM
3	Dok	Administrator Guidance (AGD_ADM), Version 1.2, Austria Card, 2008	Papier oder pdf
4	Dok	User Guidance (AGD_USR), Version 1.0, Austria Card, 2008	Papier oder pdf
5	Dok	Specification of the generic Secure Signature Application for ACOS EMV-A04, Version 1.1, Austria Card, 2008	Papier oder pdf
6	Dok	Delivery and Operation Documentation – Delivery, Installation and Generation, Version 1.2, Austria Card, 2008	Papier oder pdf
7	Dok	ACOS EMV-A04 Commands, Version 2.1, Austria Card, 2008	Papier oder pdf
8	Dok	ACOS EMV-A04 Init-Pers-Concept, Version 1.3, Austria Card, 2008	Papier oder pdf

HW=Hardware, SW=Software, Dok=Dokumentation

1.4 Hersteller

Austria Card Plastikkarten und Ausweissysteme GmbH

Lamezanstr. 4-8

A-1232 Wien, Österreich

2. Funktionsbeschreibung

Die Komponente ist eine Signaturerstellungseinheit in Chipkartenform.

Sie besteht aus dem Controller NXP SmartMX P5CC037V0A, ausführbarem Code auf der Karte sowie den benötigten Daten für die „digital signature application“.

Die Erzeugung von Signaturen erfolgt bei Nutzung von

- RSA (Schlüssellänge 1280 bis 2048 Bit) konform zu PKCS#1, bei Nutzung von

- ECC (DSA-Variante basierend auf einer Gruppe $E(F_p)$, Schlüssellänge 192 bis 256 Bit) konform zu ECDSA[3] .

Unter Nutzung des Zufallszahlengenerators des Controllers ist die SSEE in der Lage, alternativ RSA-Schlüsselpaare oder ECC-Schlüsselpaare zu erzeugen.

Das Hashen von zu signierenden Daten kann extern durch eine Applikation, durch die SSEE selbst oder in einem kombinierten Modus[4] erfolgen.

Bei allen drei Verfahren sind die Hashalgorithmen SHA-1, SHA-224 und SHA-256 nutzbar. Die Auswahl eines Hashalgorithmus erfolgt durch das Kommando `MANAGE SECURITY ENVIRONMENT`, das vor der jeweiligen Operation an die SSEE zu senden ist (und als Default bis zur nächsten Änderung bzw. einem Reset erhalten bleibt). Unterbleibt die Auswahl eines Hashalgorithmus wird ersatzweise SHA-256 genutzt.

Die SSEE besitzt zwei Konfigurationen (`Configuration A`, `Configuration B`), die sich in der Nutzung von Secure Messaging unterscheiden:

Bei der Erzeugung von qualifizierten Signaturen wird

- in der `Configuration A` die Verwendung von Secure Messaging zwischen der SSEE und der SAK[5] erzwungen,
- in der `Configuration B` die Verwendung von Secure Messaging zwischen der SSEE und der SAK unterstützt; jedoch ist unter der Voraussetzung einer besonders gesicherten Einsatzumgebung auch eine Kommunikation ohne Secure Messaging möglich.

Bei der Generierung von Zertifikaten erzwingt die SSEE in beiden Konfigurationen die Verwendung von Secure Messaging zwischen der SSEE und der CA-Anwendung (Auslesen des öffentlichen Schlüssels, Schreiben des erzeugten Zertifikats).

Die SSEE stellt einen Transport-PIN-Mechanismus bereit (in den Unterlagen des Herstellers als PUK0-Verfahren bezeichnet); nach korrekter Eingabe der PUK0 kann erstmalig und einmalig eine (Signatur-)PIN gesetzt werden.

Die SSEE verfügt über einen PUK-Mechanismus zum Entsperren der SSEE nach wiederholt fehlerhafter PIN-Eingabe; dieser Mechanismus kann nicht zum Neusetzen der PIN genutzt werden.

---

3 American National Standards Institute, ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999

4 Der erste Teil des Hashwertes wird außerhalb der SSEE, der zweite innerhalb der SSEE berechnet.

5 Signaturanwendungskomponente

Gemäß den Unterlagen [3] und [5] (s. Tabelle in Abschnitt 1.3) sollen nach Vorgaben des Herstellers folgende Parameter eingestellt werden:

	Länge	Fehlbedienungszähler	Nutzungszähler
PUK0	≥ 5	≤ 3	1
PIN	≥ 6	≤ 10	-
PUK	≥ 8	≤ 3	≤ 3

Die Längen von PUK0 und PIN müssen verschieden gewählt werden.

Die SSEE folgt der Regel "Eine erfolgreiche PIN-Eingabe erlaubt genau eine Signatur".

In den Unterlagen des Herstellers werden zwei Verfahren für den Correspondence Proof beim ZDA beschrieben, der die Zugehörigkeit eines vorher exportierten öffentlichen Schlüssels bzw. eines dazu generierten Zertifikats zu einer SSEE verifizierbar macht:

C1. Mit der betreffenden SSEE wird ein Prüftext signiert[6]. Durch Prüfung der erzeugten Signatur mit dem exportierten öffentlichen Schlüssel des Signaturschlüsselinhaber kann sichergestellt werden, dass SSEE und Zertifikat zueinander passen.

C2. Unter Anwendung des `APDU` Kommandos `CORRESPONDENCE PROOF` signiert[7] die SSEE ihren öffentlichen Schlüssel[8] mit dem zugehörigen privaten Schlüssel. Diese „technische Signatur“ wird analog zu Fall 1 zu Prüfzwecken genutzt.

Die SSEE bietet bei der Initialisierung die Option, das Kommando `CORRESPONDENCE PROOF` zu aktivieren bzw. zu deaktivieren.

---

6 nach initialer Eingabe der PUK0 und Setzen einer PIN, sowie einer weiteren Eingabe der PIN zur Signatur des Prüftextes (jeweils durch den Signaturschlüsselinhaber)

7 Eine PIN-Eingabe des Signaturschlüsselinhabers ist zu diesem Zeitpunkt nicht gefordert.

8 Die Signatur anderer Daten ist zu diesem Zeitpunkt nicht möglich.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „ACOS EMV-A04V1“ erfüllt die Anforderungen von §17(1) SigG, §17(3) Nr. 1 SigG sowie §15(1) Satz 1, 2, 4 SigV und §15(4) SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Bedingungen eingehalten werden:

a) Anforderungen an den Hersteller

1. Die Rolle “Card Manufacturer” in [3] – und damit auch die Durchführung der Initialisierung – darf ausschließlich durch den Hersteller “Austria Card Plastikkarten und Ausweissysteme GmbH“ übernommen werden.
2. Bei der Initialisierung durch den Hersteller wird die Konfiguration `Configuration A` bzw. `Configuration B` (s. Abschnitt 2) festgelegt. Ebenso sind bei der Initialisierung der Signaturalgorithmus (RSA oder ECC) und die verwendeten Schlüssellängen festzulegen (s. Abschnitt 3.3).
3. Weiterhin kann das `APDU` Kommando `CORRESPONDENCE PROOF` aktiviert bzw. deaktiviert werden (Methode C2 in Abschnitt 2). Zur Erfüllung des deutschen Signaturgesetzes ist das Kommando zu deaktivieren (d. h. die Methode C2 für den Correspondence Proof fällt nicht unter diese Sicherheitsbestätigung).
4. Mit Auslieferung der SSEE hat der Hersteller dem ZDA Informationen über die Konfigurationseinstellungen (`Configuration A` oder `Configuration B`, Status von `APDU CORRESPONDENCE PROOF`) zu übergeben und diesen zu verpflichten, die Signaturschlüsselinhaber entsprechend zu informieren.
5. Weiterhin ist entweder das *Security Target*, Version 1.7, oder eine CC-konforme “ST-lite” Fassung auszuliefern, um über die SSEE, ihre Sicherheitsfunktionen und insbesondere über die (evaluierten) Einsatzbedingungen zu informieren.
6. Gemäß den Feststellungen aus der Evaluierung der SSEE sind folgende Punkte durch den Hersteller besonders zu beachten:
   - Die Konfigurationsdateien `filesys.fsd`, `buergerk.fsd` und `profile.h` sind nach Änderungen auf “malicious links” zu prüfen, bevor sie für die SSEE verwendet werden.

- Bei Änderungen an `filesys.fsd` und `buergerk.fsd` sind die Anforderungen in *Secure Patching for ACOS A04*, Version 1.2, zu beachten.
- Die Datei `profile.h` enthält „Schalter“ zur einfachen Konfiguration verschiedener Optionen; bei Änderung dieser Schalter sind die Anforderungen aus [5], Kap. 7 zu beachten.
- 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.
- 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 SSEE sind die Testprotokolle zu archivieren; die Testprotokolle müssen hinreichend aussagekräftig sein, um feststellen zu können, ob verwendete SSEEen zur einer evaluierten Konfiguration gehören oder nicht.
- Das Kommando `LOAD COMPLETION DATA` darf bei der Initialisierung der SSEE nicht verwendet werden.

7. Die Auslieferung der SSEE hat im Einklang mit den Vorgaben in [6] zu erfolgen.

b) Anforderungen an den ZDA

1. Der ZDA muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung erforderlich sind. Die Einhaltung der Vorgaben aus den Dokumenten [3], [5], [6] und [8] ist sicherzustellen.
2. In [6] ist für die Auslieferung der SSEE von der RA des ZDA zum Signaturschlüsselinhaber die Vorgabe enthalten, dass die sichere Auslieferung im Sicherheitskonzept des ZDA zu beschreiben ist. Die Prüf- und Bestätigungsstelle hat bei den Prüfungen gemäß § 15(2) SigG dieses Auslieferungsverfahren zu überprüfen und ggf. seine Sicherheit explizit zu bestätigen.
3. Das Auslesen der Signaturprüfschlüssel aus der SSEE darf in der Konfiguration `Configuration A` (mit Secure Messaging) ausschließlich in einem geschützten Einsatzbereich[9] und mittels einer vertrauenswürdigen[10] SAK vorgenommen werden.
4. Das Auslesen der Signaturprüfschlüssel von der SSEE und das Erzeugen von elektronischen Signaturen darf in der Konfiguration `Configuration B` (ggf.

---

9 Gemäß „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“, Version 1.4, Bundesnetzagentur

10 sicherheitsbestätigt oder mit Hersteller-Erklärung nach §17 (4) SigG

ohne Secure Messaging) ausschließlich in einem geschützten Einsatzbereich[9] und mittels einer vertrauenswürdigen SAK[10] vorgenommen werden.

5. Die Vorgaben (s. Abschnitt 2) zu den Mindestlängen, maximalen Werten für die Fehlbedienungszähler und Nutzungszähler erfüllen die Stärke „hoch“ der Common Criteria für die entsprechenden Sicherheitsfunktionen. Nach den Vorgaben der Bundesnetzagentur[11] ist jedoch für den Geltungsbereich des deutschen Signaturgesetzes abweichend davon für die PIN der maximale Wert des Fehlbedienungszählers auf 3 einzustellen.

6. Der ZDA muss Maßnahmen vorsehen, um sicherzustellen, dass die während der Produktion der SSEE generierten PUK zufällig und unabhängig voneinander für verschiedene SSEE gewählt werden. Weiterhin sind Maßnahmen einzurichten, die eine Weitergabe der PUK an eine Person außer dem Signaturschlüsselinhaber ausschließen. Die geforderten Maßnahmen sind im Sicherheitskonzept darzulegen.

Mit Auslieferung der SSEE an den ZDA ist dieser auf die Einhaltung der genannten Einsatzbedingungen hinzuweisen.

c) Nutzung des Produktes

1. Für die sicherheitsbestätigte Nutzung der SSEE ist die Einhaltung der Vorgaben aus [4] sowie der Vorgaben aus dem *Security Target*, Version 1.7, an die Einsatzumgebung sicherzustellen.

2. Das Auslesen der Signaturprüfschlüssel aus der SSEE darf in der Konfiguration `Configuration A` (mit Secure Messaging) ausschließlich in einem vertrauenswürdigen Einsatzbereich und mittels einer vertrauenswürdigen SAK vorgenommen werden (s. Abschnitt 3.2 b).

3. Das Auslesen der Signaturprüfschlüssel von der SSEE und das Erzeugen von elektronischen Signaturen dürfen in der Konfiguration `Configuration B` (ggf. ohne Secure Messaging) ausschließlich in einem vertrauenswürdigen Einsatzbereich und mittels einer vertrauenswürdigen SAK vorgenommen werden (s. Abschnitt 3.2 b).

4. Alle in Abschnitt 2 genannten Verfahren der Hashwertberechnung (extern, intern, kombiniert) stehen im Einklang mit den gesetzlichen Vorgaben. Hinsichtlich der zulässigen Hashalgorithmen s. Abschnitt 3.3.

Mit Auslieferung der SSEE an den Signaturschlüsselinhaber ist dieser auf die Einhaltung der genannten Einsatzbedingungen sowie der nachfolgenden allgemeinen Bedingungen hinzuweisen.

---

[11] s. „Auszug aus dem verabschiedeten Protokoll der 25. Sitzung der Arbeitsgemeinschaft anerkannter Bestätigungsstellen (AGAB) vom 17.07.2003“, veröffentlicht unter www.bundesnetzagentur.de

Allgemeine Anforderungen an den Anwender (Signaturschlüsselinhaber)

- Der Signaturschlüsselinhaber muss die SSEE so benutzen und aufbewahren, dass Missbrauch und Manipulation vorgebeugt wird.
- Der Signaturschlüsselinhaber benutzt die Signaturerzeugungsfunktion nur für solche Daten, deren Integrität oder Authentizität er sicherstellen will.
- Der Signaturschlüsselinhaber hält seine Identifikationsdaten für die SSEE geheim.
- Der Signaturschlüsselinhaber ändert seine Identifikationsdaten für die SSEE in regelmäßigen Abständen.
- Der Signaturschlüsselinhaber verwendet die SSEE nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

Anwendungen

Anwendungen, die die SSEE nutzen, sind nicht Gegenstand dieser Bestätigung.

3.3 Algorithmen und zugehörige Parameter

Die SSEE verwendet die für die Erzeugung elektronischer Signaturen die folgenden Algorithmen

- RSA mit Schlüssellängen von 1280 bis 2048 Bit,
- ECC mit Schlüssellängen von 192 bis 256 Bit,
- sowie die Hashverfahren SHA-1, SHA-224 und SHA-256.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung der genannten Algorithmen[12] führt zur folgender Gültigkeit der Sicherheitsbestätigung (mit den in der Tabelle angegebenen Schlüssellängen):

alternativ			
RSA	ECC	SHA-1	SHA-224, -256
1280		30.06.2008[13]	31.12.2008
1536	192	30.06.2008[14]	31.12.2009
1728		30.06.2008[15]	31.12.2010
≥1976	≥224	30.06.2008[15]	31.12.2014

[12] gemäß Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. Dezember 2007

[13] Bis 31.12.2008 für die Erzeugung qualifizierter Zertifikate.

[14] Bis 31.12.2009 für die Erzeugung qualifizierter Zertifikate.

[15] Bis 31.12.2009 für die Erzeugung qualifizierter Zertifikate, bis 31.12.2010 für die Erzeugung qualifizierter Zertifikate bei mindestens 20 Bit Entropie der Seriennummer.

Die Gültigkeit kann verlängert oder verkürzt werden, sobald neue Erkenntnisse hinsichtlich der Sicherheit der SSEE oder ihrer Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Die Signaturerstellungseinheit „ACOS EMV-A04V1“ wurde erfolgreich nach der Prüfstufe **EAL4+** der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke "**hoch**". Hierfür liegt das Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-CC-04164/04165-2008 vom 11.07.2008 vor.

Ende der Bestätigung

Sicherheitsbestätigung:
T-Systems.02166.TE.07.2008

Hrsg.:	T-Systems GEI GmbH
Adresse:	Rabinstr.8, 53111 Bonn
Telefon:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-60
Web:	www.t-systems.de/ict-security
	www.t-systems-zert.com