Nachtrag Nr. 2 zur Sicherheitsbestätigung

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]

Nachtrag Nr. 2 zur Bestätigung
T-Systems.02166.TE.07.2008 vom 18.07.2008

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 für die

Signaturerstellungseinheit
„ACOS EMV-A04V1“

der

Austria Card Plastikkarten und Ausweissysteme GmbH

die o.g. Bestätigung wie nachfolgend beschrieben erweitert wurde.

Bonn, den 19.05.2009

(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)

Der Nachtrag Nr. 2 zur Bestätigung T-Systems.02166.TE.07.2008 besteht aus 4 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. Bezugsbestätigung T-Systems.02166.TE.07.2008 vom 18.07.2008); diese Konfigurationen werden vom Hersteller bei der Produktion festgelegt.

Zur Abgrenzung gegenüber früheren Versionen der SSEE wird der Produktname um die Release-Nummer ergänzt: ACOS EMV-A04V1 (r018).

1.2 Auslieferung

Keine Änderungen gegenüber der Bezugsbestätigung.

1.3 Lieferumfang

Die SSEE hat folgenden Lieferumfang:

Nr.	Typ[3]	Bezeichnung	Version	Auslieferung
1	HW/SW	NXP SmartMX P5CC037V0A with Austria Card ROM Mask AC_A04_V1R1.hex	-	Smart card with ROM code
2	SW	Patch code loaded in EEPROM for Release Number r018	-	EEPROM
3	SW	Digital Signature Application	1.1	EEPROM
4	Dok	Administrator Guidance	1.2	Papier / pdf
5	Dok	User Guidance	1.2	Papier / pdf
6	Dok	Specification of the generic Secure Signature Application for ACOS EMV-A04	1.1	Papier / pdf

[3] HW = Hardware, SW = Software, Dok = Dokumentation

Nr.	Typ[3]	Bezeichnung	Version	Auslieferung
7	Doc	Delivery & Operation Documentation	1.2	Papier / pdf
8	Doc	ACOS EMV-A04 Commands (Command specification)	2.2	Papier / pdf
9	Doc	ACOS EMV-A04 Init-Pers-Concept	1.3	Papier / pdf

Die Deaktivierung der „Inverse EEPROM Error Correction Attack Detection“ (vgl. Nachtrag 1 vom 18.12.2008 zur Bezugsbestätigung T-Systems.02166.TE.07.2008) fällt ebenfalls unter die vorliegende Bestätigung.

1.4 Hersteller

Austria Card Plastikkarten und Ausweissysteme GmbH
Lamezanstr. 4-8
A-1232 Wien

2. Beschreibung der Änderungen

Gegenüber der Bezugsbestätigung T-Systems.02166.TE.07.2008 vom 18.07.2008 sind folgende Änderungen vorgenommen worden:

1. Fehlerbehebung für das Kommando “get processing options” (GPO) der “common payment application” (CPA).

2. Fehlerbehebung beim start-up code im Hinblick auf 16 Bit-/24 Bit-Adressierung.

3. Drei Korrekturen im Rahmen des T=1 Protokolls (wegen Rückgabe falscher Fehlercodes).

Hinweis: In der Dokumentation wurde ein Hinweis auf die beschränkte Verwendung von SHA-1 im Rahmen des deutschen Signaturgesetzes aufgenommen.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Keine Änderungen gegenüber der Bezugsbestätigung.

3.2 Einsatzbedingungen

Keine Änderungen gegenüber der Bezugsbestätigung.

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[4] führt zur folgender Gültigkeit der Sicherheitsbestätigung (mit den in der Tabelle angegebenen Schlüssellängen):

alternativ			
RSA	ECC	SHA-1	SHA-224, -256
1280		nicht mehr zugelassen	31.12.2008
1536	192	beschränkt zugelassen[5]	31.12.2009
1728		beschränkt zugelassen[6]	31.12.2010
≥1976	≥224	beschränkt zugelassen[6]	31.12.2015

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 in der Variante r018 und mit beiden Konfigurationen Configuration A und Configuration B erfolgreich nach der Prüfstufe **EAL4+** der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV re-evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke "**hoch**".

Ende des Nachtrags Nr. 2

---

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

5 Nur für die Erzeugung qualifizierter Zertifikate bis 31.12.2009.

6 Nur für die Erzeugung qualifizierter Zertifikate bis 31.12.2009, bei mindestens 20 Bit Entropie der Seriennummer bis 31.12.2010.

Nachtrag Nr. 2 zur Bestätigung
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