T · · Systems ·

Nachtrag Nr. 3 zur Sicherheitsbestätigung

T-Systems.02166.TE.07.2008

ACOS EMV-A04V1 (r029)

Austria Card 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]

Gültig bis: 01.01.2017

Nachtrag Nr. 3 zur Bestätigung
T-Systems.02166.TE.07.2008 vom 18.07.2008

T-Systems GEI GmbH
- Zertifizierungsstelle -

Vorgebirgsstr. 49, 53119 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 (r029)“

der

Austria Card GmbH

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

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02225.TU.07.2012

Bonn, den 11.07.2012

Dr. Igor Furgel
Leiter der Zertifizierungsstelle

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] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) (BGBl. I S. 1542)

Der Nachtrag Nr. 3 zur Bestätigung T-Systems.02166.TE.07.2008 besteht aus 7 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit „ACOS EMV-A04V1 (r029)“, 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 (r029).

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 r029	-	EEPROM
3	SW	Digital Signature Application	1.1	EEPROM
4	Dok	Administrator Guidance	1.6	Papier / pdf
5	Dok	User Guidance	1.6	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

Hinweis: Die Produktversion kann mit der Hilfe des Kommandos GET DATA wie folgt festgestellt werden:

Versionsinformation kodiert in der Antwort auf GET DATA	Produktversion
0x0401	ACOS A04V1 (r029), Configuration A
0x8401	ACOS A04V1 (r029) Configuration B

1.4 Antragsteller dieser Bestätigung und Hersteller des Produkts

Der Antragsteller für das aktuelle Bestätigungsverfahren und der Hersteller der SSEE ist

Austria Card GmbH
Lamezanstr. 4-8
A-1232 Wien

2. Beschreibung der Änderungen

Folgende Änderungen sind an der SSEE im Vergleich zum Nachtrag Nr. 2[4] vom 19.05.2009 vorgenommen worden:

1. Für die Rückgabewerte (status words) ‚64 00' und ‚65 00' wurde der Aufruf einer Routine eingeführt, die eine sicherere Behandlung von Störungen implementiert.

2. Der Rückgabewert ‚6A 88' wurde als Reaktion auf einen Zugriff auf nicht-initialisierte Personalisierungsdaten neu eingeführt und ersetzt nun in dieser Bedeutung den alten Rückgabewert ‚64 00'.

[4] zur Bezugsbestätigung T-Systems.02166.TE.07.2008 vom 18.07.2008

3. Für die Digital Signature Application (DSA), die für die Erzeugung qualifizierter elektronischer Signaturen verwendet wird, wurden alle Signaturalgorithmen deaktiviert, die den Hash-Algorithmus SHA-1 verwenden (vgl. Abschn. 3.3).

4. Für die Digital Signature Application (DSA), die für die Erzeugung qualifizierter elektronischer Signaturen verwendet wird, wurde die Ausführung des Kommandos PSO: COMPUTE DIGITAL SIGNATURE bei Nutzung ECC insofern ergänzt, dass die erzeugte Signatur vor der Herausgabe intern verifiziert wird.

Hinweis: Es wurden noch weitere Änderungen am Produkt vorgenommen, die seine Services als SSEE nicht tangieren. Konkret wurde die Common Payment Application (CPA[5]) an relevante Spezifikationsaktualisierungen angepasst.

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.

[5] CPA ist Teil des Produkts, aber nicht des Evaluierungsgegenstands (EVG)

3.3 Algorithmen und zugehörige Parameter im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Für die Version ACOS EMV-A04V1 (r029) der SSEE gelten die Ausführungen im Abschnitt 3.3 der Bezugsbestätigung mit folgenden Änderungen fort:

a) Zur Erzeugung qualifizierter elektronischer Signaturen[6]:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[7]	Gültigkeit gem. aktuellen Festlegungen[7]
~~SHA-1~~	n.a.	n.a.	nicht geeignet	-
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2018
RSA	Parameter n: 1976 ≤ n ≤ 2048	„Signature Schemes with Appendix“ PKCS#1-v1_5[8]	geeignet	Für Zertifikatssignaturen: bis 2017 Für alle anderen Anwendungen: bis Ende 2015
		„Signature Schemes with Appendix“ PSS[9]	geeignet	bis Ende 2018
ECDSA[10] basierend auf Gruppen $E(F_p)$	224 ≤ q < 250 Bit	n.a.	geeignet	bis Ende 2015

6 Durchgestrichene Algorithmen stehen für den angegebenen Service nicht mehr zur Verfügung

7 Vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243.

8 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002, Abschn. 8.2 und 9.2

9 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002, Abschn. 8.1 und 9.1

10 ANSI X9.62-2005: Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[7]	Gültigkeit gem. aktuellen Festlegungen[7]
ECDSA[10] basierend auf Gruppen $E(F_p)$	$250 \leq q \leq 256$ Bit	n.a.	geeignet	bis Ende 2018

b) Zur Prüfung qualifizierter elektronischer Signaturen:

Dieser Service ist für die SSEE nicht anwendbar.

3.4 Prüfstufe und Mechanismenstärke der Sicherheitsfunktionen

Die Signaturerstellungseinheit „ACOS EMV-A04V1 (r029)“ wurde in der Variante r029 und mit beiden Konfigurationen *Configuration A* und *Configuration B* nach der Prüfstufe EAL4+ der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV ausgehend von dem Evaluierungsergebnis für das Produkt „ACOS EMV-A04V1 (r018)“ erfolgreich re-evaluiert.

Die eingesetzten Sicherheitsfunktionen[11] erreichen die Stärke "hoch".

3.5 Bestätigungskonformer Betrieb des bestätigten Produkts

Ein **bestätigungskonformer Betrieb** der SSEE ist an die Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ der Bezugsbestätigung T-Systems.02166.TE.07.2008 vom 18.07.2008 gebunden. Die Einhaltung dieser Einsatzbedingungen liegt in der Verantwortung des Produktbetreibers (Endenutzers).

Im **bestätigungskonformen Betrieb** hat der Produktbetreiber (Endenutzer) nur solche **konformitätspflichtigen (nach SigG) Komponenten der Einsatzumgebung** zu verwenden, die zum Zeitpunkt der Nutzung über eine gültige Produktbestätigung (bzw. Herstellererklärung, solange SigG-konform) verfügen. Desweiteren hat der Produktbetreiber (Endenutzer) durch entsprechendes Monitoring dafür zu sorgen, dass dieser **bestätigungskonforme Betrieb** über die **gesamte Betriebsdauer** gewährleistet ist.

Für die SSEE „ACOS EMV-A04V1 (r029)“ wird die Nutzung einer bestimmten Signaturanwendungskomponente oder einer anderen konformitätspflichtigen (nach

[11] In Common Criteria: Strength of Functions (SOF)

SigG) Komponente der Einsatzumgebung **nicht** vorausgesetzt, vgl. Abschn. 3.2 „Einsatzbedingungen“ der Bezugsbestätigung.

3.6 Gültigkeit der Bestätigung

Die Gültigkeitsdauer der vorliegenden Bestätigung ist mit der Gültigkeit der Produktbestätigung gleichzusetzen.

Diese Produktbestätigung ist u.a. auf Grundlage

(i) der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung (s. Abschn. 3.4) und

(ii) der Angaben der aktuell gültigen „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243“

zustande gekommen, woraus sich die Bestimmung ihrer Gültigkeit ergibt.

In Bezug auf die Gültigkeitsdauer der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung – unter Berücksichtigung der bei der Implementierung des EVG verwendeten Technologie und der beabsichtigten Einsatzumgebung (Smartcard inkl. Hard- und Software, die auch im öffentlich zugänglichen, ungeschützten Einsatzbereich eingesetzt werden kann) – agiert die Bestätigungsstelle auf der **Annahme**, dass diese Ergebnisse **4,5 Jahre** ab dem Zeitpunkt des Evaluierungsabschlusses (Juni 2012) gültig bleiben.

In Bezug auf die Verwendung der Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 ergibt sich ihre Gültigkeitsdauer aus dem Abschnitt 3.3, wobei der Produktbetreiber (Endbenutzer) stets zu berücksichtigen hat, ob ein Algorithmus im Betrieb tatsächlich verwendet wird, und wenn Ja, für welche Dienste/Funktionen er verwendet wird.

Die Gültigkeitsdauer der vorliegenden Produktbestätigung ist dann auf das nächstliegende Gültigkeitsdatum beschränkt. **So ist die Gültigkeit dieser Produktbestätigung zeitlich beschränkt, und zwar bis 01.01.2017**.

Die Gültigkeit der Bestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

Ende des Nachtrags Nr. 3

Nachtrag Nr. 3 zur Bestätigung
T-Systems.02166.TE.07.2008

Hrsg.:	T-Systems GEI GmbH
Adresse:	Vorgebirgsstr. 49, 53119 Bonn
Telefon:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-6000
Web:	www.t-systems.de/ict-security
	www.t-systems-zert.com