Anhang Nr. 1 vom 30.04.2004
zum Zertifizierungsreport
T-Systems-DSZ-ITSEC-04084-2002 vom 24.09.2002

1 Gegenstand des Anhangs

1 Dieser Anhang beschreibt

- alle vom Hersteller vorgenommenen Änderungen an dem seinerzeit zertifizierten EVG, seiner Dokumentation, seiner Entwicklungsumgebung und seiner Einsatzumgebung, seinem Auslieferungsverfahren, sowie
- den Umfang und die Ergebnisse der Re-Evaluierung,
- ggf. zu beachtende Hinweise und Auflagen,
- die Re-Zertifizierung.

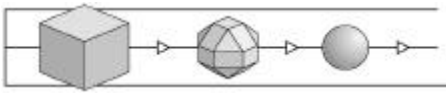
2 Beschreibung der Änderungen

2 Der EVG „CardOS/M4.01A mit Applikation für digitale Signatur“ hat folgende Änderungen erfahren:

1. Als technische Einsatzumgebung wird nun die Hardware SLE66CX322P, Designstand b14 zugrunde gelegt.
2. In den EVG wurde die Firmware RMS+ Super Slim Version 1.3 einbezogen, die Bestandteil der neuen Hardware SLE66CX322P, Designstand b14 ist. Diese Firmware realisiert keine sicherheitsspezifischen Funktionen; sie ist jedoch sicherheitsrelevant.

3 Die mit dem EVG ausgelieferte Dokumentation besteht aus (Änderungen / Ergänzungen **fett**):

Nr.	Art	Bezeichnung	Version	Datum	Auslieferung
1	Software (Operating System)	CardOS/M4.01A	C804	**25.11.2003** (compilation date of the current HEX-file for the ROM-mask)	loaded in ROM / EEPROM
2	Software (Application / Data Structure)	SigG application	2.1	29.07.2002	loaded in EEPROM
3	Documentation	CardOS/M4 User’s Manual	1.0	10/2001	Paper form or PDF-File



Nr.	Art	Bezeichnung	Version	Datum	Auslieferung
4	Documentation	CardOS/M4 User's Manual – Correction Sheet	2.0	06/2002	Paper form or PDF-File
5	Documentation	CardOS/M4.01 Benutzerdokumentation für Kartenhalter	1.02	27.02.2002	Paper form or PDF-File
6	Documentation	CardOS/M4.01A Benutzerdokumentation für Kartenhalter	2.1	08.07.2002	Paper form or PDF-File
7	Documentation	CardOS/M4.01 Benutzerdokumentation für Terminalentwickler	1.12	27.02.2002	Paper form or PDF-File
8	Documentation	CardOS/M4.01A Benutzerdokumentation für Terminalentwickler	2.0	17.06.2002	Paper form or PDF-File
9	Documentation	CardOS/M4.01 Dokumentation für Trust Center	1.02	27.02.2002	Paper form or PDF-File
10	Documentation	CardOS/M4.01A Dokumentation für Trust Center	2.0	17.06.2002	Paper form or PDF-File
11	Documentation	CardOS/M4.01 Auslieferung, Generierung und Konfiguration	1.1	18.12.2001	Paper form or PDF-File
12	Documentation	CardOS/M4.01A Auslieferung, Generierung und Konfiguration	2.0	17.06.2002	Paper form or PDF-File

4 Das Betriebssystem CardOS/M4.01A, die „Applikation für digitale Signatur", die Entwicklungsumgebung und das Auslieferungsverfahren des EVG wurden **nicht** geändert.

5 Die Sicherheitsvorgaben für den EVG tragen die neue Versionsnummer 3.0 (Datum 18.03.2004) und unterscheiden sich von der bisherigen Version 2.2 lediglich durch die geänderte Tabelle der Dokumentation und die Referenz auf den neuen Designstand des Chips.

3 Re-Evaluierung

6 Die im vorangehenden Abschnitt beschriebenen Änderungen machen eine Re-Evaluierung des EVG erforderlich, da sich der Umfang des EVG und seine technische Einsatzumgebung geändert haben.

7 Die Re-Evaluierung wurde durch die Siemens AG (ICN EN SEC, Charles-de-Gaulle Strasse 2, 81737 München) bei der Prüfstelle für IT-Sicherheit der T-Systems GEI GmbH, BU ITC Security beauftragt.

8 Die Prüfstelle ist nach ISO 17025 akkreditiert und besitzt eine gültige Lizenz der Zertifizierungsstelle und des BSI für das hier vorliegende Prüfgebiet.

9 Die Re-Evaluierung erfolgte im Zertifizierungsschema der T-Systems gegen die Kriterien ITSEC in der Stufe E4 / hoch.

10 Die Re-Evaluierung wurde durch die Zertifizierungsstelle kriteriengemäß begleitet.

11 Das Ergebnis der Re-Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 3.01 und das Datum 29.04.2004.

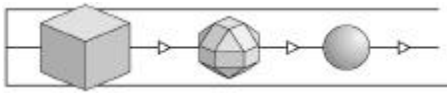
12 Die Re-Evaluierung des EVG wurde am 29.04.2004 beendet.

4 Auflagen und Hinweise

13 Die in dem Zertifizierungsreport T-Systems-DSZ-ITSEC-04084-2002 enthaltenen Auflagen und Hinweise gelten mit folgenden Änderungen / Ergänzungen (**fett**) auch für die re-zertifizierte Version des EVG:

1. Das Zertifikat T-Systems-DSZ-ITSEC-04084-2002 und dieser Zertifizierungsreport gelten für CardOS/M4.01A mit Applikation für digitale Signatur in Verbindung mit der Hardware SLE66CX322P, **Designstand b14**, deren Chip Type Identifier ‘6C’ (hexadezimal) ist und die in der Production Line Number “2” (für Dresden) hergestellt wurde. **Eine Erweiterung der Gültigkeit auf andere Produktionslinien ist möglich unter der Voraussetzung, dass die in anderen Produktionslinien produzierte Hardware SLE66CX322P nachweislich die gleiche Sicherheit aufweist.**

2. Die für die Anwendung in SigG-konformen elektronischen Signaturen geeigneten Kryptomechanismen werden gemäß /SIGV/, Anlage 1, I. 2. *Algorithmen – Veröffentlichung und Neubestimmung der Eignung* im Bundesanzeiger veröffentlicht. Nach der gegenwärtig gültigen Veröffentlichung **(Übersicht über geeignete Algorithmen, 02.01.2004, Bundesanzeiger Nr. 30 Seite 2537-2538, 13. Februar 2004)** sind die im EVG implementierten Algorithmen **geeignet, und zwar: Hash-Algorithmus SHA-1 bis Ende 2009 und RSA-Algorithmus mit 1024 Bit bis Ende 2007**. Die Eva-



luationsergebnisse zur Eignung des EVG entsprechend den Sicherheitszielen SO6 „Quality of key generation“ und SO7 „Provide secure digital signature“ sind deshalb zunächst bis **2007** gültig und müssen dann überprüft werden.

3. Eine Re-Evaluierung des EVG wird dann erforderlich, wenn sich neue Erkenntnisse über Angriffsmethoden ergeben, welche die vom EVG verwendeten kryptographischen und anderen Sicherheitsmechanismen betreffen und die erfolgreiche Angriffe auf die Sicherheit des EVG wahrscheinlich machen, so dass der Verdacht besteht, dass die Mechanismenstärke hoch nicht mehr gewährleistet ist.

4. Es wird folgendes Verfahren für die Bereitstellung der Hardware SLE66CX322P vorgeschrieben: Der Hersteller Siemens AG, ICN EN SEC muss Wafer oder Module am Infineon Warehouse in Regensburg persönlich abholen.

5. Bei der Auslieferung der Benutzerdokumentation (s. Security Target) ist darauf zu achten, dass sie vollständig ausgeliefert wird.

14 Folgende zusätzlichen Hinweise sind für den sicherheitsgerechten Einsatz des EVG zu beachten:

1. Sofern CardOS/M4.01A mit Applikation für digitale Signatur, implementiert auf der Hardware SLE66CX322P, zur Erzeugung qualifizierter elektronischer Signaturen nach dem Signaturgesetz /SigG/ verwendet werden soll, muss der Zertifizierungsdiensteanbieter in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung erforderlich sind.

2. Zum Einsatz in besonders gesicherter Umgebung bestimmte Signaturmodule (Konfiguration n ? 1) dürfen nicht als personenbezogene EVG (Konfiguration n = 1) an Endkunden (Kartenhalter) ausgeliefert werden. Es ist die Aufgabe der herausgebenden Stellen bzw. der Zertifizierungsdiensteanbieter, dies sicherzustellen.

3. Von den Abläufen der Komplettierung, Initialisierung und Personalisierung gemäß der Dokumente *CardOS/M4.01A Auslieferung, Generierung und Konfiguration* und *CardOS/M4.01A Dokumentation für Trust Center* darf nicht abgewichen werden. Diese Abläufe schließen Bedienfehler aus und müssen Bestandteil des Sicherheitskonzepts der Zertifizierungsdiensteanbieter sein. Ebenso dürfen die Personalisierungsscripte nur an den durch Kommentare kenntlich gemachten Stellen im Sinne der Kommentare angepasst werden.

4. Die Generierung von Signaturschlüsselpaaren darf nur in sicherer Umgebung (innerhalb eines Trust Centers) erfolgen.

5. Der EVG ist in folgendem Punkt nicht konform zur DIN V 66291-1: Der EVG lässt lesenden Zugriff auf das Kartenhalter-Zertifikat C.CH.DS (gespeichert im EF_C_CH_DS) stets zu und sichert diesen nicht durch die PIN.

5 Re-Zertifizierung

15 Das mit Datum vom 24.09.2002 ausgestellte Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-ITSEC-04084-2002 bleibt auch für den geänderten EVG gültig.

16 Der vorliegende Anhang Nr. 1 ergänzt den Zertifizierungsreport T-Systems-DSZ-ITSEC-04084-2002 vom 24.09.2002.

17 Dieser Anhang Nr. 1 ist auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle veröffentlicht und wird in den Broschüren BSI 7148 / 7149 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) referenziert.

18 Hiermit wird bestätigt, dass

- die am Verfahren beteiligten Evaluatoren und Zertifizierer weder an der Entwicklung, dem Vertrieb noch an einer Anwendung des EVG beteiligt waren,
- alle Regeln des Zertifizierungsschemas, des speziellen Verfahrenstyps und der maßgebenden Kriterien eingehalten wurden.

Bonn, den 30.04.2004

Dr. Heinrich Kersten

Leiter der Zertifizierungsstelle

Ende des Anhangs Nr. 1 zu T-Systems-DSZ-ITSEC-04084-2002.

Anhang Nr. 1 zu T-Systems-DSZ-ITSEC-04084-2002

Hrsg.: T-Systems GEI GmbH
Adresse: Rabinstr.8, 53111 Bonn
Telefon: 0228/9841-0
Fax: 0228/9841-60
Web: www.t-systems-ict-security.com
www.t-systems-zert.com