Anhang Nr. 2 vom 30.09.2004

zum Zertifizierungsreport

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

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 keine Änderungen erfahren. Jedoch wurde folgende Einsatzumgebung hinzugefügt:

1. Als technische Einsatzumgebung wird nun neben der Hardware SLE66CX322P, Designstand b14 auch die Hardware SLE66CX322P, Designstand f18 zugrunde gelegt.
2. Die Designstände b14 und f18 sind identisch. Chips mit Designstand b14 werden in Dresden (Production Line Indicator „2“) produziert, Chips mit Designstand f18 in Corbeil Essonnes, Frankreich (Production Line Indicator „5“), genannt „Altis“.

[3] Die mit dem EVG ausgelieferte Dokumentation wurde bereits im Anhang Nr. 1 aufgeführt und bleibt unverändert.

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

[5] Die im Verfahren T-Systems-DSZ-ITSEC-04084-2002 eingereichte und für den Anhang Nr. 1 re-evaluierte Dokumentation zum EVG bleibt weiterhin gültig mit der

Maßgabe, dass für den Designstand f18 auf das Zertifikat BSI-DSZ-CC-0265-2004 verwiesen wird.

6 Die Auswirkungen der Einbeziehung des Designstandes f18 (Production Line Altis) auf die bei der Re-Evaluierung verwendete Dokumentation sind im Hersteller-Dokument „Re-Zertifizierung für den zusätzlichen Chip-Produktionsstandort Altis“, Version 1.0, August 2004 dargelegt.

3 Re-Evaluierung

7 Die im vorangehenden Abschnitt beschriebenen Änderungen machen keine Re-Evaluierung des EVG erforderlich, da sich der Umfang des EVG nicht geändert hat. Die Änderung der technischen Einsatzumgebung bezieht sich nicht auf Design, Layout oder Funktionalität des Chips, sondern auf den Produktionsstandort.

8 Es wurde eine Re-Evaluierung der Hardware SLE66CX322P mit den Designständen b14 und f18 durchgeführt, die insbesondere die Identität der Designstände b14 und f18 bestätigte und den Produktionsstandort Altis einbezog.

9 Für die geänderte technische Einsatzumgebung liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0265-2004 vom 13. September 2004 vor. Auf der Grundlage dieses Zertifikates können die im Zertifikat T-Systems-DSZ-ITSEC-04084-2002 ausgewiesenen und im Anhang Nr. 1 vom 30. April 2004 bestätigten Sicherheitseigenschaften auch für den Designstand f18 bestätigt werden.

10 Für die im Produktionsstandort Altis produzierten Chips SLE66CX322P, Designstand f18 ist daher nachweislich die gleiche Sicherheit ausgewiesen wie für den Designstand b14.

4 Auflagen und Hinweise

11 Die in dem Zertifizierungsreport T-Systems-DSZ-ITSEC-04084-2002 enthaltenen Auflagen und Hinweise gelten mit folgenden Änderungen / Ergänzungen (**fett**) gegenüber dem Anhang Nr. 1 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 f18**, deren **Chip Type Identifier ‘7B’ (hexadezimal)** ist und die in der Production **Line Number “5” (für Altis)** 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 veröf-

fentlicht. 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 Evaluationsergebnisse 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.

[12] 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 $n \neq 1$) 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

[13] Das mit Datum vom 24.09.2002 ausgestellte Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-ITSEC-04084-2002 bleibt auch für den Designstand f18 gültig.

[14] Der vorliegende Anhang Nr. 2 ergänzt den Zertifizierungsreport T-Systems-DSZ-ITSEC-04084-2002 vom 24.09.2002 und seinen Anhang Nr. 1 vom 30.04.2004.

[15] Dieser Anhang Nr. 2 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.

[16] Hiermit wird bestätigt, dass

- die am Verfahren beteiligten 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 30.09.2004

Dr. Heinrich Kersten

Leiter der Zertifizierungsstelle

Ende des Anhangs Nr. 2 zu T-Systems-DSZ-ITSEC-04084-2002.

Anhang Nr. 2 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