Annex No. 1 as of April 30, 2004

to the certification report

T-Systems-DSZ-ITSEC-04084-2002 as of September 24, 2002

1 Scope of this annex

[1] This annex describes

- all changes applied by the vendor to the previously certified TOE, its documentation, developmental environment, operational environment, the delivery procedure as well as
- the scope and the results of the re-evaluation,
- recommendations and stipulations to be observed,
- the re-certification.

2 Description of Changes

[2] The TOE „CardOS/M4.01A with Application for Digital Signature Creation“ has been modified as follows:

1. For the technical environment of the TOE, the hardware SLE66CX322P, design level b14, is now used.
2. The firmware RMS+ Super Slim, version 1.3, which is an integral part of the new hardware SLE66CX322P, design level b14, is included in the TOE. This firmware does not realise security enforcing functions, but is security relevant.

[3] The documentation delivered with the new TOE consists of (changes / modifications in **bold**):

No.	Type	Name	Version	Date	Delivery
1	Software (Operating System)	CardOS/M4.01A	C804	**Nov 25, 2003** (compilation date of the current HEX-file for the ROM-mask)	loaded in ROM / EEPROM

No.	Type	Name	Version	Date	Delivery
2	Software (Application / Data Structure)	SigG application	2.1	July 29, 2002	loaded in EEPROM
3	Documentation	CardOS/M4 User's Manual	1.0	Oct 2001	Paper form or PDF-File
4	Documentation	CardOS/M4 User's Manual – Correction Sheet	2.0	June 2002	Paper form or PDF-File
5	Documentation	CardOS/M4.01 Benutzerdokumentation für Kartenhalter	1.02	Feb 27, 2002	Paper form or PDF-File
6	Documentation	CardOS/M4.01A Benutzerdokumentation für Kartenhalter	2.1	July 08, 2002	Paper form or PDF-File
7	Documentation	CardOS/M4.01 Benutzerdokumentation für Terminalentwickler	1.12	Feb 27, 2002	Paper form or PDF-File
8	Documentation	CardOS/M4.01A Benutzerdokumentation für Terminalentwickler	2.0	June 17, 2002	Paper form or PDF-File
9	Documentation	CardOS/M4.01 Dokumentation für Trust Center	1.02	Feb 27, 2002	Paper form or PDF-File
10	Documentation	CardOS/M4.01A Dokumentation für Trust Center	2.0	June 17, 2002	Paper form or PDF-File
11	Documentation	CardOS/M4.01 Auslieferung, Generierung und Konfiguration	1.1	Dec 18, 2001	Paper form or PDF-File
12	Documentation	CardOS/M4.01A Auslieferung, Generierung und Konfiguration	2.0	June 17, 2002	Paper form or PDF-File

[4] The operating system CardOS/M4.01A, the „Application for Digital Signature Creation", the developmental environment and the delivery procedure for the TOE have **not** been changed.

[5] The security target for the new TOE is designated as version 3.0 (as of March 18, 2004); compared to the former security target, version 2.2, only the following modification have been applied: updated table of documentation, reference to new chip design level.

3 Re-Evaluation

[6] The changes described in the preceding sections require a re-evaluation of the TOE, because the scope of the TOE and its technical environment have been modified.

[7] The re-evaluation of the TOE by the Prüfstelle für IT-Sicherheit of T-Systems GEI GmbH, BU ITC Security, was sponsored by Siemens AG (ICN EN SEC, Charles-de-Gaulle Strasse 2, 81737 Munich, Germany).

[8] The evaluation facility accredited against ISO 17025 has a valid licence of the certification body and the BSI for the scope of the evaluation.

[9] The re-evaluation was carried out against the ITSEC level E4 / high under the terms of the certification scheme of T-Systems GEI GmbH .

[10] In compliance with the criteria, the re-evaluation was monitored by the certification body.

[11] The Evaluation Technical Report (ETR), version 3.01 and dated April 29, 2004, provided by the evaluation facility, contains the outcome of the re-evaluation.

[12] The re-evaluation was completed on April 29, 2004.

4 Stipulations and Recommendations

[13] For the stipulations and recommendations contained in the certification report T-Systems-DSZ-ITSEC-04084-2002, the following changes / modifications (in **bold**) have to be applied for the re-certified TOE with :

1. The certificate T-Systems-DSZ-ITSEC-04084-2002 and the corresponding certification report apply also to „CardOS/M4.01A with Application for Digital Signature Creation“ implemented on the hardware SLE66CX322P, **design level b14**, with Chip Type Identifier ‘6C’ (hexadecimal) produced in Production Line Number “2” (for Dresden). **Extending the results to other production lines is possible if there is sufficient assurance that the hardware SLE66CX322P produced in other production lines provides the same degree of security.**

2. The cryptographic mechanisms suitable for SigG compliant electronic signatures are published according to /SigV/, annex 1, section 2 “Algorithmen – Veröffentlichung und Neubestimmung der Eignung“ in the Federal Gazette. According to the current publication **("Übersicht über geeignete Algorithmen, 02.01.2004",**

Federal Gazette No. 30 pages 2537-2538 as of February 13, 2004) the following algorithms of the TOE are **approved: hash algorithm SHA-1 until end of 2009, RSA algorithm with 1024 bit key length until end of 2007**. The results of the evaluation as to the security objectives SO6 “Quality of Key Generation” and SO7 “Provide Secure Digital Signature” are, therefore, valid until end of **2007**. Then, they shall be re-examined.

3. It is necessary to re-evaluate the TOE as soon as there are new findings on potential successful attacks against the TOE’s cryptographic or other security mechanisms leading to the assumption that the minimum strength of mechanism “high” is in question.

4. The following procedure for delivery of the hardware SLE66CX322P must be used: The manufacturer Siemens AG, ICN EN TNA has to personally collect wafer and modul at the Infineon Warehouse in Regensburg.

5. Special care must be taken to deliver the complete user documentation (cf. Security Target).

14 The following additional stipulations for the secure usage of the TOE have to be met:

1. If „CardOS/M4.01A with Application for Digital Signature Creation“ implemented on SLE66CX322P hardware is to be used for creating qualified electronic signatures compliant to the (German) Signature Act /SigG/, the certification service provider has to specify in his security concept all measures required for secure personalisation.

2. The signature module configuration of the TOE ($n \neq 1$) designed for a specially secured environment must not be delivered to an individual as a personal configuration ($n = 1$) of the TOE. It is the responsibility of the card issuer (e. g. a certification service provider) to meet this requirement.

3. The procedures of completion, initialisation, and personalisation as described in *CardOS/M4.01A Auslieferung, Generierung und Konfiguration* and *CardOS/M4.01A Dokumentation für Trust Center* must strictly be followed, no deviation is allowed. These procedures avoid mistakes and shall be part of the security concept of the certification service provider. Changes to the personalisation scripts may be applied only at locations and in the sense indicated by comments.

4. Key pair generation shall take place within a secure environment only, e. g. at a certification service provider’s site.

5. In the following respect, the TOE is not compliant to the DIN V 66291-1 standard: The TOE always allows reading of the certificate of the card holder (C.CH.DS) located in the EF_C_CH_DS without any authentication by PIN.

5 Re-Certification

[15] The "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] T-Systems-DSZ-ITSEC-04084-2002 remains valid for the modified TOE.

[16] This annex no. 1 is to be added to the certification report T-Systems-DSZ-ITSEC-04084-2002 as of September 24, 2002.

[17] This annex no. 1 is posted on the web pages of the certification body (www.t-systems-zert.com) and referenced in the brochures BSI 7148 / 7149 of the Bundesamt für Sicherheit in der Informationstechnik (BSI).

[18] It is hereby certified that

- the evaluators and certifiers who have participated in this procedure, have not been involved in developing, selling or applying the TOE,
- all rules of the certification scheme, of the specific type of procedure and the relevant criteria have been met.

Bonn: April 30, 2004

Dr. Heinrich Kersten

Head of the Certification Body

End of Annex No. 1 to T-Systems-DSZ-ITSEC-04084-2002.

Annex No. 1 to T-Systems-DSZ-ITSEC-04084-2002

Editor:	T-Systems GEI GmbH
Address:	Rabinstr.8, D-53111 Bonn, Germany
Phone:	+49-228-9841-0
Fax:	+49-228-9841-60
Web:	www.t-systems-ict-security.com www.t-systems-zert.com