Annex No. 2 as of September 30, 2004

to the certification report

T-Systems-DSZ-ITSEC-04084-2002 as of September 24, 2002 and to Annex No. 1 as of April 4, 2004

1 Scope of this annex

1 This annex describes

- all changes applied by the vendor to the 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 **not** been modified; the following technical environment was added:

1. For the technical environment of the TOE, the hardware SLE66CX322P, design level b14, as well as the hardware SLE66CX322P, design level **f18** can be used.
2. The design levels b14 and f18 are identical. Chips with design level b14 are produced in Dresden (Production Line Indicator „2“), Chips with design level f18 in Corbeil Essonnes, France (Production Line Indicator „5“), called „Altis“.

3 The documentation delivered with the TOE was specified in annex no. 1 to the certification report and remains unchanged.

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 documentation of the TOE previously submitted for certification under T-Systems-DSZ-ITSEC-04084-2002 and for re-evaluation (cf. annex no. 1) remains valid except for the fact that for the design level f18 the certificate BSI-DSZ-CC-0265-2004 is referenced.

6 For the transition to the design level f18 (Production Line Altis), the impact on the documentation submitted for the previous re-evaluation (cf. annex no. 1) is described in the document „Re-Zertifizierung für den zusätzlichen Chip-Produktionsstandort Altis“, version 1.0, August 2004, supplied by the vendor .

3 Re-Evaluation

7 The changes described in the preceding sections do not require a re-evaluation of the TOE, because the scope of the TOE has not been modified: The changes to the technical environment refer to the location of the chip production; design, layout and functionality of the chip have not been modified.

8 A re-evaluation of the hardware SLE66CX322P with the design levels b14 und f18 TOE has been performed to include the production facility "Altis" and to confirm that the design levels b14 and f18 are identical.

9 The "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] BSI-DSZ-CC-0265-2004 as of September 13, 2004 references the added technical environment for the TOE (design level f18). Based on this certificate, the security features of the TOE indicated in the certificate T-Systems-DSZ-ITSEC-04084-2002 and its annex no. 1 as of April 30, 2004, can be confirmed for the design level f18 as well.

10 Thus, there is sufficient assurance that the chips SLE66CX322P, design level f18, produced at the production facility Altis, and SLE66CX322P, design level b14, have the same degree of security.

4 Stipulations and Recommendations

11 For the stipulations and recommendations contained in the certification report T-Systems-DSZ-ITSEC-04084-2002, the following modifications (in **bold**: changes to annex no. 1) have to be applied for the re-certified TOE:

1. The certificate T-Systems-DSZ-ITSEC-04084-2002 and the corresponding certification report apply to „CardOS/M4.01A with Application for Digital Signature Creation“ implemented on the hardware SLE66CX322P, **design level f18**, with **Chip Type Identifier ‘7B’ (hexadecimal)** produced in **Production Line Number “5” (for Altis)**. 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).

12 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 ≠ 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

13 The "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] T-Systems-DSZ-ITSEC-04084-2002 issued on September 29, 2002 remains valid for the design level f18 as well.

14 This annex no. 2 is to be added to the certification report T-Systems-DSZ-ITSEC-04084-2002 as of September 24, 2002 and its annex no. 1 as of April 30, 2004.

15 This annex no. 2 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).

16 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: September 30, 2004

Dr. Heinrich Kersten

Head of the Certification Body

End of Annex No. 2 to T-Systems-DSZ-ITSEC-04084-2002.

Annex No. 2 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