Technical Annex No. 2
as of May 18, 2009 to the certification report

T-Systems-DSZ-CC-04164/04165-2008 as of July 11, 2008 for
ACOS EMV-A04V1 Configuration A and Configuration B

1   Scope of this annex

[1] This annex describes

- all changes applied by the developer to the certified TOE and its documentation 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 has been modified as follows:

- The TOE was re-named to *ACOS EMV-A04V1 (r018) Configuration A* resp. *ACOS EMV-A041 (r018) Configuration B* to clearly reflect the modified TOE.

- The following bug fixes have been applied:

  - bug fix for the "get processing options" (GPO) command of the common payment application (CPA)

  - bug fix in start-up code to correct 16 bit vs. 24 bit addressing mode

  - three bug fixes for T=1 protocol issues – the TOE's implementation returned wrong error codes.
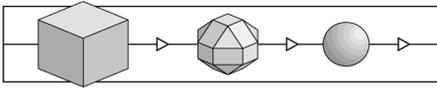
- The delivered TOE consists of following parts (changes / additions in **bold face**):

No.	Type[1]	Name	Version	Delivery
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 r018**	-	EEPROM
3	SW	Digital Signature Application[2]	1.1	EEPROM
4	Doc	Administrator Guidance	1.2	Paper or pdf
5	Doc	**User Guidance**	**1.2**	Paper or pdf
6	Doc	Specification of the generic Secure Signature Application for ACOS EMV-A04	1.1	Paper or pdf
7	Doc	Delivery & Operation Documentation	1.2	Paper or pdf
8	Doc	**ACOS EMV-A04 Commands (Command specification)**	**2.2**	Paper or pdf
9	Doc	ACOS EMV-A04 Init-Pers-Concept	1.3	Paper or pdf

- The security targets[3] identified by final version 2.1 as of Apr 30, 2009, have been modified to reflect all changes relevant on this level. A remark concerning the usage of SHA-1 in national signature schemes was added.
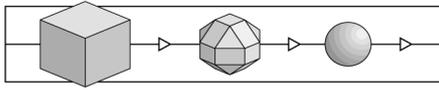
3 Re-Evaluation

3 The changes described in the preceding sections required a re-evaluation of the TOE.

4 The re-evaluation was performed by the Prüfstelle für IT-Sicherheit of T-Systems GEI GmbH and sponsored by Austria Card Plastikkarten und Ausweissysteme GmbH.

---

1   HW = Hardware, SW = Software, Doc = Documentation

2   according to *Specification of the generic Secure Signature Application for ACOS EMV-A04;* the application is in one of the two configurations (configuration A or configuration B) and determines the TOE's configuration. The configuration of the application / the TOE is determined during production and cannot be changed afterwards. The user is informed of the type of TOE delivered.

3   separate for configuration A and B

5   The evaluation facility accredited against ISO 17025 has a valid licence of the certification body for the scope of the evaluation.

5   The evaluation was carried out under the terms of the certification scheme of T-Systems against the Common Criteria level EAL4 with augmentations AVA_MSU.3 and AVA_VLA.4 (EAL4+).

6   The minimum strength of the TOE security functions (SOF) is claimed as SOF-high.

7   Only for Configuration A: The TOE is compliant with the protection profile *Secure Signature-Creation Device (SSCD-PP) Type 3, Version 1.05, BSI-PP-0006-2002T, 03.04.2002*.

8   In compliance with the criteria, the evaluation was monitored by the certification body.

9   The Evaluation Technical Report (ETR), version 1.0 as of May 05, 2009, provided by the evaluation facility, contains the outcome of the evaluation.

10 The evaluation was completed on May 05, 2009.

4   Stipulations and Recommendations

11 The stipulations for the *sponsor* as well as stipulations and recommendations *for the secure usage* of the TOE contained in the certification report T-Systems-DSZ-CC-04164/04165-2008 remain valid for the modified TOE.

5   Re-Certification

12 The certification of ACOS EMV-A04V1 Configuration A and Configuration B can be maintained for the modified TOE as described in section 1.

Bonn: May 18, 2009

Dr. Heinrich Kersten

(Head of the Certification Body)

End of Technical Annex No. 2 to T-Systems-DSZ-CC-04164/04165-2008