# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0346-2006

for

## ACOS EMV-A03V1
## Configuration A

from

## Austria Card
## Plastikkarten und Ausweissysteme GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

**Deutsches IT-Sicherheitszertifikat**

erteilt vom

**Bundesamt für Sicherheit in der Informationstechnik**

BSI

Bundesamt für Sicherheit
in der Informationstechnik

## BSI-DSZ-CC-0346-2006

## ACOS EMV-A03V1
## Configuration A

from

## Austria Card
## Plastikkarten und Ausweissysteme GmbH

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0 extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

**Evaluation Results:**

| | |
|---|---|
| PP Conformance: | **Protection Profile BSI-PP-0006-2002** |
| Functionality: | **PP BSI-PP-0006-2002 conformant plus product specific extensions**<br>**Common Criteria Part 2 extended** |
| Assurance Package: | **Common Criteria Part 3 conformant**<br>**EAL4 augmented by**<br>AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states)<br>AVA_VLA.4 (Vulnerability assessment - Highly resistant) |

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 20. January 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht                L.S.

IT Security Certified

SOGIS - MRA

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

# Contents

# A Certification

## 1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 22 September 2000 in the Bundesanzeiger p. 19445

# 2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

## 2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

## 2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states) and AVA_VLA.4 (Vulnerability assessment - Highly resistant) that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

# 3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product ACOS EMV-A03V1, Configuration A has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0220-2004. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0220-2004 were re-used.

The evaluation of the product ACOS EMV-A03V1, Configuration A was conducted by T-Systems GEI GmbH. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

Austria Card
Plastikkarten und Ausweissysteme GmbH
Lamezanstraße 2-8
A-1232 Wien, Austria

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 20. January 2006.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described and specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

# 4 Publication

The following Certification Results contain pages B-1 to B-24.

The product ACOS EMV-A03V1, Configuration A has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Austria Card
Plastikkarten und Ausweissysteme GmbH
Lamezanstraße 2-8
A-1232 Wien, Austria

# B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# Contents of the certification results

# 1 Executive Summary

The Target of Evaluation (TOE) is Austria Card's ACOS EMV-A03V1, Configuration A. (For information about the two different configurations please read chapter 1.5 „Special configuration requirements“ of this report.)

The TOE is intended to be used as a secure signature creation device (SSCD) for the generation of signature creation data (SCD) and the creation of qualified electronic signatures according to Directive 1999/93/ec on a community framework for electronic signatures [14], the Austrian [15] and the German Signaturgesetz [16]. Note that a confirmation through the respective authorities is required for usage under the abovementioned laws for qualified electronic signatures.

The TOE comprises the following components:

- Integrated Circuit (IC) Philips SmartMX P5CC036V1D (hardware)
- Smart card operating system (software)
- Application for digital signature (software)

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

- Generation of SCD and the correspondent signature-verification data (SVD)
- Creation of qualified electronic signatures
  (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function is provided by the signature creation application (SCA) as appropriate TOE environment,
  (b) using appropriate hash functions that are, according to [17] and [18], agreed as suitable for qualified electronic signatures,
  (c) after appropriate authentication of the signatory by the TOE,
  (d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable according to [17] and [18].

Figure 1 shows the TOE scope from the structural perspective. The SSCD, i.e. the TOE, comprises the underlying hardware, the operating system (OS), the secure SCD/SVD generation, secure SCD storage and use, and signature creation functionality. The CGA and the SCA are part of the immediate environment of the TOE. The CGA shall communicate with the TOE over a trusted channel to receive the SVD generated by the TOE and to include the SVD in the certificate generated by the CGA. The human interface device provided by the SCA is used for the input of VAD for authentication by knowledge. The TOE holds RAD to check the provided VAD. The SCA establishes a trusted path to the TOE to protect the confidentiality and integrity of the VAD. The SCA establishes a trusted channel to the TOE to protect the integrity of the DTBS. The TOE requires the SCA to use a trusted path for sending the VAD and to use a trusted channel for sending the DTBS.

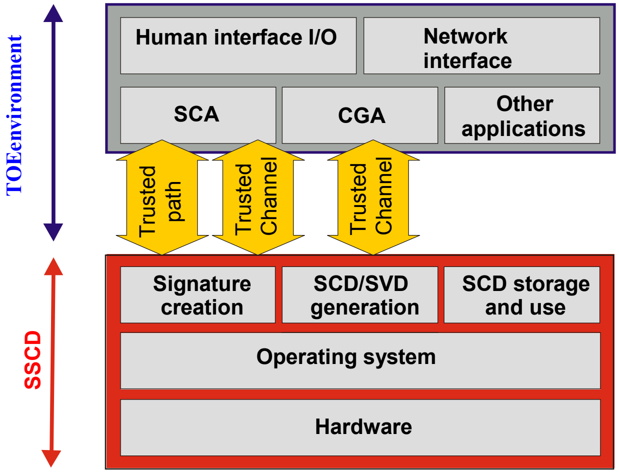

Figure 1: Scope of the SSCD, structural view

The TOE life cycle consists of the development phase and the operational phase. The operational phase starts after initialisation with personalisation for the signatory's use by

1. generating a SCD/SVD pair
2. creation of the signatory’s verification authentication data (SVAD).

The main functionality in the usage phase is signature creation including all supporting functionality (e.g., secure SCD storage and SCD use). The TOE implements all IT security functionality, which are necessary to ensure the secrecy of the SCD. The SSCD protects the SCD during the whole life cycle as to be solely used in the signature creation process by the legitimate signatory. The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-serviceprovider (CSP). To prevent the unauthorised usage of the SCD, the TOE provides user authentication and access control. The TOE will destroy the SCD, if it is no longer used for signature generation. The life cycle of the device as SSCD ends with the destruction of all SCD within the device.

The TOE as a multi-application smart card implements additional functions and security features, but these are not subject of the ST [6].

The TOE provides a single physical interface over a serial connection according to [19] which is used to transmit command APDUs to the TOE and receive the corresponding response APDUs from the TOE as specified in [20] and in [21].

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluation of the underlying semiconductor. For this re-evaluation based on BSI-DSZ-CC-0220-2004 the underlying hardware platform of the TOEs is changed to the Philips P5CC036V1D Secure Smart Card Controller which was evaluated as BSI-DSZ-CC-0293-2005 ([8], [9]) and is fully compatible to the P5CC036V0M used in the baseline evaluation. The software of the TOE has not changed and the hardware changes are limited to changes that do not change the functional behaviour of the TOE.

"Philips P5CC036V1D Secure Smart Card Controller" provided by Philips Semiconductors GmbH (see [8]) was evaluated according to Common Criteria EAL 5 augmented with a minimum strength level for its security functions of SOF-high for specific functionality based on the Protection Profile BSI-PP-0002 [10] and as outlined in [9]. This platform evaluation was performed by T-Systems GEI GmbH.

The embedded Software of the ACOS EMV-A03V1, Configuration A and the overall composition were evaluated by T-Systems GEI GmbH, too. The evaluation was completed on 20. December 2005. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The concept for composition as outlined in CC Supporting Document [4, AIS 36] was used.

The sponsor, and vendor and distributor is

Austria Card
Plastikkarten und Ausweissysteme GmbH
Lamezanstraße 2-8
A-1232 Wien, Austria

## 1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [6], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

| Requirement | Identifier |
|---|---|
| EAL4 | TOE evaluation: Methodically designed, tested and reviewed |
| + AVA_MSU.3 | Vulnerability assessment - Analysis and testing for insecure states |
| + AVA_VLA.4 | Vulnerability assessment – Highly resistant |

Table 1: Assurance components and EAL-augmentation

[8] Information Technology Security Evaluation Facility

## 1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC Part 2:

| **Security Functional Requirement** | **Identifier** |
|---|---|
| **FCS** | **Cryptographic support** |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1 | Cryptographic operation |
| **FDP** | **User data protection** |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_ETC.1 | Export of user data without security attributes |
| FDP_ITC.1 | Import of user data without security attributes |
| FDP_RIP.1 | Subset residual information protection |
| FDP_SDI.2 | Stored data integrity monitoring and action |
| FDP_UIT.1 | Data exchange integrity |
| **FIA** | **Identification and Auzthentification** |
| FIA_AFL.1 | Authentication failure handling |
| FIA_ATD.1 | User attribute definition |
| FIA_UAU.1 | Timing of authentication |
| FIA_UID.1 | Timing of identification |
| **FMT** | **Security Management** |
| FMT_MOF.1 | Management of security functions behaviour |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.2 | Secure security attributes |
| FMT_MSA.3 | Static attribute initialisation |
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of management functions |
| FMT_SMR.1 | Security roles |
| **FPT** | **Protection of the TOE Security Functions** |
| FPT_AMT.1 | Abstract machine testing |
| FPT_FLS.1 | Failure with preservation of secure state |
| FPT_PHP.1 | Passive detection of physical attack |
| FPT_PHP.3 | Resistance to physical attack |

| Security Functional Requirement | Identifier |
|---|---|
| FPT_TST.1 | TSF testing |
| **FTP** | **Trusted Path/Channels** |
| FTP_ITC.1 | Inter-TSF trusted channel |
| FTP_TRP.1 | Trusted path |

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

| Security Functional Requirement | Identifier |
|---|---|
| **FPT** | **Protection of the TOE Security Functions** |
| FPT_EMSEC.1 | TOE Emanation |

Table 3: SFRs for the TOE, CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.

These Security Functional Requirements are implemented by the following TOE Security Functions:

| TOE Security Functions | Description |
|---|---|
| SF1 | Life cycle support |
| SF2 | Identification and authentication of user |
| SF3 | Access control |
| SF4 | SCD/SVD pair generation |
| SF5 | SVD export and correspondence proof |
| SF6 | Signature creation |
| SF7 | Secure messaging |
| SF8 | Self test |
| SF9 | Physical protection |
| SF10 | Object reuse |

Table 4: TOE Security Functions

## 1.3 Strength of Function

The TOE‘s strength of functions is rated ‘high’ (SOF-high) for those functions, identified in the Security Target [6], chapter 6.1.11, SOF Claim. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2) (see Chapter 9 of this report).

## 1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats and Organisational Security Policies (OSPs) which were assumed for the evaluation and averted by the TOE are specified in the BSI-PP-0006-2002 [11] and mentioned in the Security Target [6]:

| **Name** | **Definition** |
|---|---|
| T.Hack_Phys | Physical attacks through the TOE interfaces |
| T.SCD_Divulg | Storing, copying, and releasing of the signature creation data |
| T.SCD_Derive | Derive the signature creation data |
| T.Sig_Forgery | Forgery of the electronic signature |
| T.Sig_Repud | Repudiation of signatures |
| T.SVD_Forgery | Forgery of the signature-verification data |
| T.DTBS_Forgery | Forgery of the DTBS-representation |
| T.SigF_Misuse | Misuse of the signature creation function of the TOE |

Table 5: Threats for the TOE

| **Name** | **Definition** |
|---|---|
| P.CSP_Qcert | Qualified certificate |
| P.Qsign | Qualified electronic signatures |
| P.Sigy_SSCD | TOE as secure signature creation device |

Table 6: OSPs

Note: Only the titles of the threats and OSPs are provided. For more details please refer to the Security Target [6], chapter 3.

## 1.5 Special configuration requirements

The TOE is intended to be used as a secure signature creation device. It is defined uniquely by the name and version number ACOS EMV-A03V1, Configuration A. Its implementation representation and its configuration are specified by the Configuration List [27] in appendices of the document [26]. The evaluated version of the TOE has the label P5CC036_2004_EEP_RC8 according to the configuration list [27].

The product is available in two configurations, "configuration A" and "configuration B," whereby configuration A mandates the use of secure messaging between the SSCD and the IT-environment and configuration B supports secure messaging but also allows for operation without the use of secure messaging in a trusted IT-environment. The TOE is the product in configuration A but configuration B has also been evaluated, see [12], [13] and chapter 8 of this report.

In configuration A the SCA must authenticate itself to the TOE. The TOE in configuration A requires the SCA to use a trusted path for sending the VAD and to use a trusted channel for sending the DTBS. The TOE in configuration A is compliant with the Protection Profile SSCD Type 3 [11]. In configuration B the SCA uses a trusted environment for communication with the SSCD. The product in configuration B supports a trusted path and a trusted channel to the SCA but accepts VAD and DTBS not sent via trusted path or trusted channel and is not compliant with the Protection Profile SSCD Type 3 [11]. The configuration is irreversibly specified during the initialisation process.

The TOE mandates the use of secure messaging between the TOE and the IT-environment, i. e. it mandates the use of secure messaging between the TOE and the CGA entity of the IT-environment and mandates secure messaging between the TOE and the SCA entity of the IT-environment. It requires the SCA to use a trusted path for sending the VAD and to use a trusted channel for sending the DTBS. The TOE is compliant with the Protection Profile [11].

The configuration of the memory management unit (MMU) constitutes a central part of the TOE's security. The MMU implements memory separation of different applications using MMU tables. Changes to the MMU configuration for the signature application and the operating system are not allowed, changes to the MMU configuration for other applications have to be applied according to the rules described in the document Secure Patching, Version 1.1 [30]. The separation of applications without application-specific executable code is covered by this certification process but the functionality "application separation for executable code" is not covered.

Therefore both changes to the executable code of other applications as well as changes to the MMU tables of other applications are not covered by this evaluation. (The term “other applications” is used to denote applications located in a dedicated file (DF) which are different from the signature application located in the signature application's DF). The evaluation results are restricted to chip cards containing the TOE as well as other applications which have been inspected as part of this evaluation. These applications are listed in table 7 below. During the evaluation, tests have been performed to demonstrate that the applications listed do not have any negative influence on the signature application.

| Application Name | AID (Application Identifier) | Short Description |
|---|---|---|
| EMV Maestro | A0000000043060 | International EMV application, Version 2.1 |
| EMV MasterCard | A0000000041010 | International EMV application, Version 2.1 |
| EMV ATM Maestro | D0400000190001 | Domestic EMV application, Version 2.1 |
| EMV POS Maestro | D0400000190002 | Domestic EMV application, Version 2.1 |
| EMV ATM MasterCard | D0400000190003 | Domestic EMV application, Version 2.1 |

| Application Name | AID (Application Identifier) | Short Description |
|---|---|---|
| EMV POS MasterCard | D0400000190004 | Domestic EMV application, Version 2.1 |
| Quick (IEP) | D040000001000002 | Domestic Paymentsystem, Version 2.1 |
| ATM | D040000004000002 | Domestic Paymentsystem, Version 2.1 |
| POS | D040000003000002 | Domestic Paymentsystem, Version 2.1 |
| RFU | D040000002000002 | Domestic Paymentsystem, Version 2.1 |
| Retail | D04000000B000002 | Domestic Loyalty, Version 2.1 |
| Bank_Data | D04000000C000002 | Domestic Loyalty, Version 2.1 |
| Shopping | D04000000D000002 | Domestic Loyalty, Version 2.1 |
| Digital ID | D0400000190010 | Domestic Paymentsystem, Version 2.1 |
| Digital Signature (SSCA) | A0000001184543 | Signature Application |
| Encryption Application | A000000118454E | Encryption Application, Version 1.10 |
| DF_UNI_Ausweis | D040000015000001 | Domestic Loyalty, Version 2.0 |
| DF_UNI_Kepler1 | D040000013000001 | Domestic Loyalty, Version 2.0 |
| DF_UNI_Kepler2 | D040000013000002 | Domestic Loyalty, Version 2.0 |
| DF_Mensa | D040000014000001 | Domestic Loyalty, Version 2.0 |
| DF_KEP_SIG | A000000118040000 | Domestic Loyalty, Version 1.32 |
| DF_Ausweis | D040000015000001 | Domestic Loyalty, Version 1.3 |
| DF_Schüler1 | D040000013000001 | Domestic Loyalty, Version 1.3 |
| DF_Schüler2 | D040000013000002 | Domestic Loyalty, Version 1.3 |
| DF_Verkehr | A000000118010000 | Domestic Loyalty, Version 1.3 |
| DF_Partner | A000000118020000 | Domestic Loyalty, Version 1.3 |
| DF_Schülerdaten | A000000118030000 | Domestic Loyalty, Version 1.3 |
| DF_Schul_SIG | A000000118040000 | Domestic Loyalty, Version 1.32 |

Table 7: Optional applications on ACOS EMV-A03

## 1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [11], the assumptions defined in section 3.1 of the Protection Profile are valid for the Security Target of this TOE. The following constraints concerning the operating environment are made in the Protection Profile and are repeated in the Security Target, please refer to the Security Target [6], chapter 3.1:

A.CGA Trustworthy certification-generation application

The CGA protects the authenticity of the signatory’s name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA Trustworthy signature creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

## 1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# 2 Identification of the TOE

The Target of Evaluation (TOE) is called:

ACOS EMV-A03V1, Configuration A

The following table outlines the TOE deliverables:

| No | Type | Name | Form of Delivery |
|---|---|---|---|
| 1 | HW/SW | Philips SmartMX P5CC036V1D with Austria Card ROM Mask AC000004.hex dated 19.12.2003 | Smart card with ROM code |
| 2 | SW | Digital Signature Application according to Specification of the generic Secure Signature Application for ACOS EMVA03, Version 1.7 [24].<br>The application is configuration A. There is another configuration possible (Configuration B, see [12]). The configuration of the application (and thus the TOE's configuration) is determined during production and cannot be changed afterwards. The user is informed of the type of TOE delivered. | EEPROM |
| 3 | Doc | Administrator Guidance - Evaluation of ACOS EMVA03V0, Version 1.20 [23] | Copy or pdf |
| 4 | Doc | User Guidance - Evaluation of ACOS EMV-A03V0, Version 1.10 [22] | Copy or pdf |
| 5 | Doc | Specification of the generic Secure Signature Application for ACOS EMV-A03, Version 1.7 [24] | Copy or pdf |
| 6 | Doc | Delivery & Operation, Version 1.20, Austria Card GmbH, 23.06.2004 [25] | Copy or pdf |
| 7 | Doc | Commands for ACOS EMV-A03, Version 1.2 [28] | Copy or pdf |
| 8 | Doc | ACOS EMV-A Init-Pers-Concept, Version 3.04 [29] | Copy or pdf |

Table 8: Deliverables of the TOE

The TOE's evaluated configuration contains other applications which have been listed in table 7, see chapter 1.5. According to the configuration list [27] the label of the evaluated version of the TOE is P5CC036_2004_EEP_RC8.

# 3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and will be used as a secure signature creation device (SSCD) for the generation of signature creation data (SCD) and the creation of qualified electronic signatures. The security policy is to provide protection against

- physical attacks through the TOE interfaces,
- storing, copying, releasing and deriving the signature creation data by an attacker,
- forgery of the electronic signature, of the signature-verification data, or of the DTBS-representation,
- repudiation of signatures,
- misuse of the signature creation function of the TOE.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage assumptions

Specific usage assumptions were not addressed by this product evaluation.

## 4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.1):

- The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP(A.CGA).
- The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE (A.SCA).

Furthermore, the Security Target [6], chapter 3.3 defines three Organisational Security Policies that state that the CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD (P.CSP_Qcert), that the signatory uses a signature creation system to sign data with a qualified electronic signature that is based on a qualified certificate and that is created by an SSCD (P.Qsign), and that the TOE implements the SCD used for signature creation under sole control of the signatory (P.Sigy_SSCD). Please refer to the Security Target [6], chapter 3.3 for more detail.

### 4.3 Clarification of scope

Additional threats that are not countered by the TOE and its evaluated security functions were not addressed by this product evaluation.

## 5 Architectural Information

The TOE (ACOS EMV-A03V1, Configuration A) is intended to be used as a secure signature creation device comprising an integrated circuit (IC) with an operating system (OS) and a signature application. An overview of the architecture is given in section 2 of the Security Target [6]. A top level block diagram can be found in figure 1 of this report and in chapter 2 of the Security Target [6]. The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software. A top level block diagram of the hardware IC including an overview of subsystems can be found within the TOE description of the Security Target of the chip [8].

## 6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 8 of this report):

- Administrator Guidance - Evaluation of ACOS EMV-A03V0, Version 1.20, Austria Card GmbH, 28.07.2004, [23]
- User Guidance - Evaluation of ACOS EMV-A03V0, Version 1.10, Austria Card GmbH, 26.07.2004, [22]
- Specification of the generic Secure Signature Application for ACOS EMV-A03, Version 1.7, Austria Card GmbH, 16.09.2004, [24]
- ADO_DEL.2, ADO_IG.1, BSI-DSZ-CC-0220 and BSI-DSZ-CC-0221, Version 1.20, Austria Card GmbH, 23.06.2004, [25]
- Commands for ACOS EMV-A03, Version 1.2-Release, Austria Card GmbH, 31.03.2004, [28]
- ACOS EMV-A Init-Pers-Concept, Version 3.04, Austria Card GmbH, Revised on 27.07.2004, [29]

## 7 IT Product Testing

The developer tested all TOE-relevant interactions with both RSA and ECC key pairs. The test team defined all necessary test cases with respect to standards the implementation has to adhere to and with respect to the Common Criteria evaluation. Testing was divided in two parts: Every single command was tested with all possible valid and invalid test cases first. Then test scenarios were created where all commands were tested in different combinations. The test cases are implemented by scripts and run against the TOE.

In all, the developer tests covered all security functions. Where possible, the tests were performed at the APDU level, ensuring a coverage of at least all FSP interfaces. Since there is a direct mapping between APDUs and subsystems, the testing depth is on HLD level. In addition there are module tests. Usually they are performed by the programmers.

Evaluator testing consisted of both tests at the APDU interface and of tests using a simulator (or emulator), where necessary. The APDU tests have been carried out with the emulator, SO28 and test cards (modules). All tests that made use of the signature key pair have been executed with both an RSA key pair and an ECC key pair.

All tests have been carried out on the emulator first. Characteristic parts of the final test suite have been executed against test cards. Following test cards have been used for these tests:

- configuration A with an RSA signature key pair,
- configuration A with an ECC signature key pair.

The security functions tested included every security function but SF9 (Physical protection). SF9 has not been tested explicitly, since SF9 requires no direct interaction between chip and operating system software: If the chip identifies an attack, the chip provides its security functionality without any further requirements.

Every APDU of the operating system has been tested. To cover the security aspects not already tested by the operating system focused tests, additional tests have been prepared. The evaluators also performed tests that verified that the additional applications do not have an negative influence on the signature application. The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The tests have been carried out on a PC with card reader equipped with special test software capable of performing cryptographic calculations, a digital oscilloscope and special analysis tools and covered the resistance of the RSA-CRT and ECC Implementation against Side Channel Analysis.

For the re-evaluation, tests have been performed that proof the correct integration of the software with the new hardware platform, the continuing resistance against side channel attacks, and the functional correctness of the cryptographic function’s implementations.

# 8 Evaluated Configuration

The TOE is delivered in state initialised and is of configuration A. It is defined uniquely by the name and version number ACOS EMV-A03V1, Configuration A and is referenced by a label according to the configuration list [27] which is P5CC036_2004_EEP_RC8. There is also a configuration B of the product available that has been evaluated in a different evaluation. See also [12] and [13]. The configuration of the application (and thus the TOE’s configuration) is determined during production and cannot be changed afterwards. The user is informed of the type of TOE delivered. The evaluation results are restricted to chip cards containing the TOE with applications that have been inspected during the evaluation process and that are listed in table 7 of this report. See also chapter 1.5 of this report.

# 9 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [7] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36].

The ETR [7] builds up on the ETR-lite for Composition documents of the evaluations of the underlying hardware "Philips P5CC036V1D Secure Smart Card Controller" ([9]). These ETR-lite for Composition documents were provided by the ITSEF T-Systems GEI GmbH according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]).

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body. For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used. For specific methodology on random number generator evaluation the scheme interpretations AIS 20 and AIS 31 (see [4]) were used.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

| **Assurance classes and components** | | **Verdict** |
|---|---|---|
| Security Target evaluation | CC Class ASE | PASS |
| TOE description | ASE_DES.1 | PASS |
| Security environment | ASE_ENV.1 | PASS |
| ST introduction | ASE_INT.1 | PASS |
| Security objectives | ASE_OBJ.1 | PASS |
| PP claims | ASE_PPC.1 | PASS |
| IT security requirements | ASE_REQ.1 | PASS |
| Explicitly stated IT security requirements | ASE_SRE.1 | PASS |

| Assurance classes and components | | Verdict |
|---|---|---|
| TOE summary specification | ASE_TSS.1 | PASS |
| Configuration management | CC Class ACM | PASS |
| Partial CM automation | ACM_AUT.1 | PASS |
| Generation support and acceptance procedures | ACM_CAP.4 | PASS |
| Problem tracking CM coverage | ACM_SCP.2 | PASS |
| Delivery and operation | CC Class ADO | PASS |
| Detection of modification | ADO_DEL.2 | PASS |
| Generation log | ADO_IGS.1 | PASS |
| Development | CC Class ADV | PASS |
| Fully defined external interfaces | ADV_FSP.2 | PASS |
| Security enforcing high-level design | ADV_HLD.2 | PASS |
| Implementation of the TSF | ADV_IMP.1 | PASS |
| Descriptive low-level design | ADV_LLD.1 | PASS |
| Informal correspondence demonstration | ADV_RCR.1 | PASS |
| Informal TOE security policy model | ADV_SPM.1 | PASS |
| Guidance documents | CC Class AGD | PASS |
| Administrator guidance | AGD_ADM.1 | PASS |
| User guidance | AGD_USR.1 | PASS |
| Life cycle support | CC Class ALC | PASS |
| Identification of security measures | ALC_DVS.1 | PASS |
| Developer defined life-cycle model | ALC_LCD.1 | PASS |
| Well-defined development tools | ALC_TAT.1 | PASS |
| Tests | CC Class ATE | PASS |
| Analysis of coverage | ATE_COV.2 | PASS |
| Testing: low-level design | ATE_DPT.1 | PASS |
| Functional testing | ATE_FUN.1 | PASS |
| Independent testing - sample | ATE_IND.2 | PASS |
| Vulnerability assessment | CC Class AVA | PASS |
| Validation of analysis | **AVA_MSU.3** | PASS |
| Strength of TOE security function evaluation | AVA_SOF.1 | PASS |
| Highly resistant | **AVA_VLA.4** | PASS |

Table 9: Verdicts for the assurance components

For this re-evaluation based on BSI-DSZ-CC-0220-2004 the underlying hardware platform of the TOEs is changed to the Philips P5CC036V1D Secure Smart Card Controller which was evaluated as BSI-DSZ-CC-0293-2005 ([9], [8]) and is fully compatible to the P5CC036V0M used in the baseline evaluation. The software of the TOE has not changed and the hardware changes are limited to changes that do not change the functional behaviour of the TOE.

The evaluation has shown that:

- the TOE is conformant to Protection Profile BSI-PP-0006-2002 [11]
- the Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_MSU.3 and AVA_VLA.4
- the TOE fulfils the claimed strength of function SOF-high for the functions as outlined in chapter 1.3.

The underlying hardware had been successfully assessed by T-Systems GEI GmbH.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The results of the evaluation are only applicable to ACOS EMV-A03V1, Configuration A as outlined in chapter 8 of this report and that is produced and initialised in an environment that was subject to an audit in the cause of the evaluation.

The documentation (see chapter 6 of this report) has not changed from the baseline evaluation.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

# 10 Comments/Recommendations

The operational documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

The user of the TOE has to be aware of the existence of two configurations. The name and version number of this TOE ACOS EMV-A03V1, Configuration A but there is another configuration available, see [12], [13] and chapter 1.5 of this report. The configuration of the application (and thus the TOE’s configuration) is determined during production and cannot be changed afterwards. The user is informed of the type of TOE delivered, see User Guidance [22], chapter 4.1.

If a new application is not only restricted to a new data structure in a separate DF but also introduces new executable code, the MMU tables will probably have to be changed. The functionality “application separation for executable code” is not covered by this certification process. Therefore the evaluation results are restricted to chip cards containing the TOE as well as the applications which have been inspected during the evaluation process. Therefore both changes to the executable code of other applications as well as changes to the MMU tables of other applications imply a re-certification. The other applications which have been inspected as part of this evaluation are listed in table 7 of this report.

# 11 Annexes

None.

# 12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

# 13 Definitions

## 13.1 Acronyms

| | |
|---|---|
| **AID** | Application identifier |
| **AIS** | Application Notes and Interpretation of the Scheme |
| **APDU** | Application Protocol Data Unit, interface standard for smart cards, see ISO/IEC 7816 part 3 |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security |
| **CA** | Certification authority (part of a CSP) |
| **CEM** | Common Methodology for IT Security Evaluation |
| **CGA** | Certification generation application |
| **CC** | Common Criteria for IT Security Evaluation |
| **CSP** | Certification-service-provider |
| **DPA** | Differential Power Analysis, an attack, which may compromise cryptographic keys by analysing the power consumption of the smart card chip |
| **DF** | Dedicated file, directory on a smart card file system according to ISO/IEC 7816 |

| | |
|---|---|
| **DRNG** | Deterministic Random Number Generator (a term used and introduced in AIS20) |
| **DTBS** | Data to be signed |
| **EAL** | Evaluation Assurance Level |
| **ECC** | Elliptic Curve Cryptographic |
| **EEPROM** | Electrically erasable programmable read-only memory; EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge |
| **ETR** | Evaluation Technical Report |
| **FSP** | Functional Specification |
| **HLD** | High-level design |
| **IC** | Integrated Circuit |
| **IT** | Information Technology |
| **MF** | Master file, top level directory (root) on a smart card file system according to ISO/IEC 7816 |
| **MMU** | Memory Management Unit |
| **OS** | Operating System |
| **OSP** | Organisational Security Policy |
| **PC** | Personal Computer |
| **PIN** | Personal identification number |
| **PP** | Protection Profile |
| **PROM** | Programmable read-only memory, a memory chip on which data can be written only once |
| **PUK** | Personal unblock key |
| **RA** | Registration authority (part of a CSP) |
| **RAD** | Reference authentication data |
| **RNG** | Random Number Generator |
| **RSA** | Asymmetric crypto algorithm by R. L. Rivest, A. Shamir, L. Adleman |
| **SCA** | Signature creation application |
| **SCD** | Signature creation data |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SigG** | (Austrian or German) Signaturgesetz |

| | |
|---|---|
| **SigV** | (Austrian or German) Signaturverordnung |
| **SM** | Secure Messaging |
| **SO28** | a packaging technology; small outline package, 28 leads |
| **SOF** | Strength of Function |
| **SSCD** | Secure signature creation device |
| **ST** | Security Target |
| **SVAD** | Signatory’s verification authentication data |
| **SVD** | Signature verification data |
| **SW** | Software |
| **TOE** | Target of Evaluation |
| **TRNG** | True Random Number Generator (a term used and introduced in AIS31) |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSFI** | TOE security functions interface |
| **TSP** | TOE Security Policy |
| **VAD** | Verification authentication data |

## 13.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

**Extension** - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Object** - An entity within the TSC that contains or receives information and upon which subjects perform operations.

**Protection Profile** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

**Security Function** - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Strength of Function** - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

**SOF-basic** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

**SOF-medium** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

**SOF-high** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**Subject** - An entity within the TSC that causes operations to be performed.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**TSF Scope of Control** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

# 14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0346; Version 1.1; 17.10.2005; Evaluation of the ACOS EMV-A03V1, Configuration A; Austria Card GmbH

[7] Evaluation Technical Report; BSI-DSZ-CC-0346 and BSI-DSZ-CC-0347; Version 2.2; December 16th, 2005; Product ACOS EMV-A03V1 (confidential document)

[8] Security Target Lite BSI-DSZ-CC-0293, Evaluation of the Philips P5CC036V1D Secure Smart Card Controller, Version 1.0, 13.03.2005, Philips Semiconductors GmbH

[9] Certificate of the Philips P5CC036V1D with specific IC Dedicated Software Secure Smart Card Controller from Philips Semiconductors GmbH, Business Line Identification; Deutsches IT-Sicherheitszertifikat, BSI-DSZ-CC-0293-2005, Bundesamt für Sicherheit in der Informationstechnik, 19.08.2004

[10] Smartcard IC Platform Protection Profile (SSVG-PP), Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[11] Protection Profile - Secure Signature Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002T, 03.04.2002

[12] Certification Report; BSI-DSZ-CC-0347-2006 for ACOS EMV-A03V1 Configuration B from Austria Card GmbH; Bundesamt für Sicherheit in der Informationstechnik

[13] Security Target BSI-DSZ-CC-0347; Version 1.1; 17.10.2005; Evaluation of the ACOS EMV-A03V1, Configuration B; Austria Card GmbH

[14] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[15] (Austrian) Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG) (inkl. Einarbeitung der Novelle lt. Ministerrat 10/2000), 19. August 1999, BGBl. I Nr. 190/1999

[16] (German) Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. I S.876 ff)

[17] Algorithms and Parameters for Secure Electronic Signatures, V.2.1 Oct 19th 2001, Algorithms group working under the umbrella of European Electronic Signature Standardisation Initiative Steering Group

[18] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen); Vom 2. Januar 2005, Bundesnetzagentur (BNetzA); Veröffentlicht am 30.

März 2005 im Bundesanzeiger Nr. 59, S. 4695-4696; Regulierungsbehörde für Telekommunikation und Post

[19] ISO/IEC 7816-3: 1997 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols, International Standard

[20] ISO/IEC 7816-4: 1995 Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry command for interchange

[21] ISO/IEC FDIS 7816-8:1998 Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands

[22] User Guidance - Evaluation of ACOS EMV-A03V0, Version 1.10, Austria Card GmbH, 26.07.2004

[23] Administrator Guidance - Evaluation of ACOS EMV-A03V0, Version 1.20, Austria Card GmbH, 28.07.2004

[24] Specification of the generic Secure Signature Application for ACOS EMV-A03, Version 1.7, Austria Card GmbH, 16.09.2004

[25] ADO_DEL.2, ADO_IG.1, BSI-DSZ-CC-0220 and BSI-DSZ-CC-0221, Version 1.20, Austria Card GmbH, 23.06.2004

[26] Configuration Management & Life cycle support, BSI-DSZ-CC-0220 and BSI-DSZ-CC-0221, Evaluation of the ACOS EMV-A03V0, Version 1.10, Austria Card GmbH, 18.05.2004

[27] Configuration list as addendum for Configuration Management & Life cycle support, Austria Card GmbH, 14.10.2004

[28] Commands for ACOS EMV-A03, Version 1.2-Release, Austria Card GmbH, 31.03.2004

[29] ACOS EMV-A Init-Pers-Concept, Version 3.04, Austria Card GmbH, Revised on 27.07.2004

[30] Secure Patching, Version 1.1, Austria Card GmbH, 27.08.2004

This page is intentionally left blank

# C Excerpts from the Criteria

CC Part 1:

**Caveats on evaluation results** (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

**Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

**Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

**Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

**Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

**Assurance categorisation** (chapter 2.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 2.1."

| Assurance Class | Assurance Family | Abbreviated Name |
|---|---|---|
| Class ACM: Configuration management | CM automation | ACM_AUT |
| | CM capabilities | ACM_CAP |
| | CM scope | ACM_SCP |
| Class ADO: Delivery and operation | Delivery | ADO_DEL |
| | Installation, generation and start-up | ADO_IGS |
| Class ADV: Development | Functional specification | ADV_FSP |
| | High-level design | ADV_HLD |
| | Implementation representation | ADV_IMP |
| | TSF internals | ADV_INT |
| | Low-level design | ADV_LLD |
| | Representation correspondence | ADV_RCR |
| | Security policy modeling | ADV_SPM |
| Class AGD: Guidance documents | Administrator guidance | AGD_ADM |
| | User guidance | AGD_USR |
| Class ALC: Life cycle support | Development security | ALC_DVS |
| | Flaw remediation | ALC_FLR |
| | Life cycle definition | ALC_LCD |
| | Tools and techniques | ALC_TAT |
| Class ATE: Tests | Coverage | ATE_COV |
| | Depth | ATE_DPT |
| | Functional tests | ATE_FUN |
| | Independent testing | ATE_IND |
| Class AVA: Vulnerability assessment | Covert channel analysis | AVA_CCA |
| | Misuse | AVA_MSU |
| | Strength of TOE security functions | AVA_SOF |
| | Vulnerability analysis | AVA_VLA |

**Table 1: Assurance family breakdown and map**

**Evaluation assurance levels** (chapter 6)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

**Evaluation assurance level (EAL) overview** (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

| Assurance Class | Assurance Family | Assurance Components by<br>Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

**Table 2: Evaluation assurance level summary**

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 6.2.1)

"Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats."

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 6.2.2)

"Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

**Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 6.2.3)

"Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

**Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed** (chapter 6.2.4)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested** (chapter 6.2.5)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested** (chapter 6.2.6)

"Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

**Evaluation assurance level 7 (EAL7) - formally verified design and tested** (chapter 6.2.7)

"Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

### **Strength of TOE security functions (AVA_SOF)** (chapter 14.3)

**AVA_SOF** Strength of TOE security functions

"Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

### **Vulnerability analysis (AVA_VLA)** (chapter 14.4)

**AVA_VLA** Vulnerability analysis

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential."