Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0251-2005

for

Java Card Mokard Safe 2.2
V2.4.0

from

ST-Incard S.r.l.

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-0251-2005

Java Card Software

Java Card Mokard Safe 2.2 V2.4.0

from

ST-Incard S.r.l.

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 PP/0305, JavaCard System Standard 2.2 Configuration Protection Profile**
Functionality:	**PP conformant Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant EAL4 augmented by ADV_IMP.2 – Implementation of the TSF AVA_VLA.3 – Vulnerability Assessment - Moderately 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, 11. November 2005

The Vice President of the Federal Office
for Information Security

IT Security Certified
SOGIS - MRA

Hange L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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 22nd 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 ADV_IMP.2 (Implementation Representation - Implementation of the TSF) and AVA_VLA.3 (Vulnerability Assessment - Moderately 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 Java Card Mokard Safe 2.2 V2.4.0 has undergone the certification procedure at BSI.

The evaluation of the product Java Card Mokard Safe 2.2 V2.4.0 was conducted by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

ST-Incard S.r.l.
ZI Marcianise Sud
81025 Marcianise (CE), ITALY

The certification is concluded with

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

This work was completed by the BSI on 11. November 2005.

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, where 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-22.

The product Java Card Mokard Safe 2.2 V2.4.0 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] ST-Incard S.r.l.
ZI Marcianise Sud
81025 Marcianise (CE), ITALY

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) and subject of the Security Target (ST) [6] is called Java Card Mokard Safe 2.2 V2.4.0. It is a java card platform which consists of an installer and a Java Card Runtime Environment.

The installer is responsible for the installation of applets on the card and for the deletion of applets and packages and its associated data on the card.

The Java Card Runtime Environment (JCRE) is the central component of a Java Card System. It consists of the following parts:

- Java Card Virtual Machine (JCVM) interprets the Java Card bytecode and implements a applets firewall.
- Java Card API and its associated native methods. These are are methods and services for interaction with the platform resources.
- Remote Method Invocation (RMI) facilities that provide the ability to invoke a method on a remote object on the card.
- Logical Channels that enable the opening of up to four simultaneous sessions with the card.
- Object deletion facilities that are responsible for the deletion of unreferenced object owned by the current context and that the associated space is recovered for reuse prior to the next card reset.

The TOE is a software product. The following components (see also PP [9], chapter 2.1) do not belong to the TOE but to the IT environment:

- Smart Card Platform. It is comprised of the integrated circuit (Samsung S3CJ9QD 32-bit risk CPU based on the core ARMv5TEJ providing 256Kbytes of user ROM, 8Kbytes of RAM and 128K bytes of EEPROM), the operating system and the dedicated software of the smart card. See also PP [9], chapter 2.1.4,
- Card manager, see also PP [9], chapter 2.1.3,
- Bytecode verifier, see also PP [9], chapter 2.1.1,
- any applets.

The following figure gives a graphical overview of the TOE, where the red dashed line delimits its perimeter.

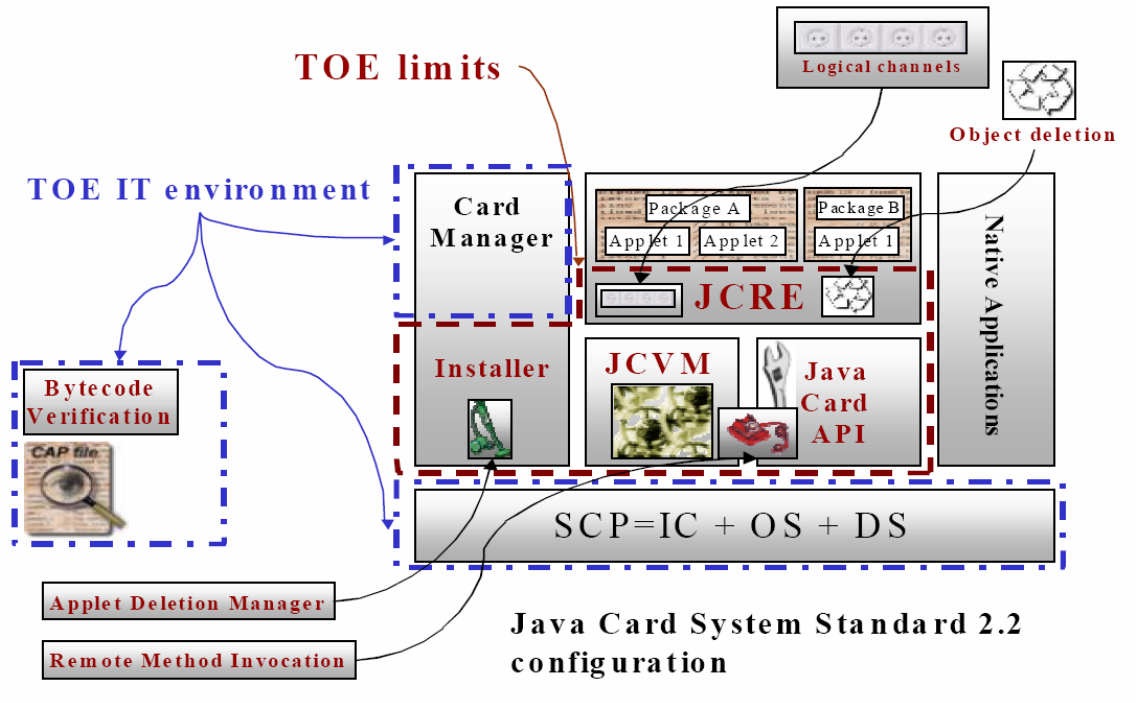

Figure 1: TOE Structure and Components

The IT product Java Card Mokard Safe 2.2 V2.4.0 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 09.11.2005. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and vendor and distributor is

ST-Incard S.r.l.
ZI Marcianise Sud
81025 Marcianise (CE), ITALY

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 part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented by ADV_IMP.2 - Implementation Representation - Implementation of the TSF) and AVA_VLA.3 - Vulnerability Assessment - Moderately resistant).

[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 conformant as shown in the following table.

The following SFRs are taken from CC Part 2:

SFR	Name
CoreG Security Functional Requirements	
Firewall Policy	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attributes based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_SEP.1	TSF domain separation
Application Programming Interface	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic destruction
FCS_COP.1	Cryptographic operation
FDP_RIP.1	Subset residual information protection
FDP_ROL.1	Basic rollback
Card Security Management	
FAU_ARP.1	Security alarms
FDP_SDI.2	Stored data integrity monitoring and action
FPT_RVM.1	Non-bypassability of the TSP
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_FLS.1	Failure with preservation of secure state
FPR_UNO.1	Unobservability
FPT_TST.1	TSF testing
AID Management	
FMT_MTD.1	Management of TSF data
FMT_MTD.3	Secure TSF data
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding

SFR	Name
InstG Security Functional Requirements	
FDP_ITC.2	Import of user data with security attributes
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_RCV.3	Automated recovery without undue loss
FRU_RSA.1	Maximum quotas
ADELG Security Functional Requirements	
Applet Deletion Manager Policy	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attributes based access control
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of management functions
FMT_MSA.3	Static attribute initialization
FMT_SMR.1	Security roles
Additional Deletion Requirements	
FDP_RIP.1	Subset residual information protection
FPT_FLS.1	Failure with preservation of secure state
RMIG Security Functional Requirements	
JCRMI Policy	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attributes based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_REV.1	Revocation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
LCG Security Functional Requirements	
The requirements are stated under CoreG.	
ODELG Security Functional Requirements	
FDP_RIP.1	Subset residual information protection
FPT_FLS.1	Failure with preservation of secure state
CarG Security Functional Requirements	
FCO_NRO.2	Enforced proof of origin
FIA_UID.1	Timing of identification
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_UIT.1	Data exchange integrity
FMT_MSA.1	Management of security attributes

SFR	Name
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FTP_ITC.1	Inter-TSF trusted channel

Table 1: TOE Security Functional Requirements

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

Security function
SF_CARD_MNGT: Card Management
SF_CRYPTO_KEY: Cryptographic Key Management
SF_PIN: PIN management
SF_CRYPTO_OP: Cryptographic Computation
SF_FIREWALL: Object access controller (firewall)
SF_OBJ_MNGT: Object Management
SF_RMI: Remote method invocation
SF_POST: Power on Self test
SF_TRANSACTION: Transaction Management

Table 2: TOE security functions

Note: Only the titles of the Security Functional Requirements and of the TOE Security Functions are provided. For more details please refer to the Security Target [6], chapter 6 and 7.

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-High) for specific functions as indicated in the Security Target [6] [chapter 2.2, detailed in chapter 7.1].

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 following list of considered threats for the TOE is defined in the Security Target [6], chapter 4.5:

Threat	Description
T.PHYSICAL	The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DP analysis. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques.
CONFIDENTIALITY	
T.CONFID-JCS-CODE	The attacker executes an application without authorization to disclose the Java Card System code.
T.CONFID-APPLI-DATA	The attacker executes an application without authorization to disclose data belonging to another application.
T.CONFID-JCS-DATA	The attacker executes an application without authorization to disclose data belonging to the Java Card System.
INTEGRITY	
T.INTEG-APPLI-CODE	The attacker executes an application to alter (part of) its own or another application's code.
T.INTEG-JCS-CODE	The attacker executes an application to alter (part of) the Java Card System code.
T.INTEG-APPLI-DATA	The attacker executes an application to alter (part of) another application's data.
T.INTEG-JCS-DATA	The attacker executes an application to alter (part of) Java Card System or API data.
T.INTEG-APPLI-CODE.2	The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation
T.INTEG-APPLI-DATA.2	The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation.
IDENTITY USURPATION	
T.SID.1	An applet impersonates another application, or even the JCRE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal.

Threat	Description
T.SID.2	The attacker modifies the identity of the privileged roles.
UNAUTHORIZED EXECUTION	
T.EXE-CODE.1	An applet performs an unauthorized execution of a method.
T.EXE-CODE.2	An applet performs an unauthorized execution of a method fragment or arbitrary data.
T.NATIVE	An applet executes a native method to bypass a security function such as the firewall.
DENIAL OF SERVICE	
T.RESOURCES	An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.
MODIFICATIONS OF THE SET OF APPLICATIONS	
T.INSTALL	The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process.
UNAUTHORIZED EXECUTIONS	
T.EXE-CODE-REMOTE	The attacker performs an unauthorized remote execution of a method from the CAD.
CARD MANAGEMENT	
T.DELETION	The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to pave the way for further attacks (putting the TOE in an insecure state).
SERVICES	
T.OBJ-DELETION	The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application.

Table 3: Threats

These threats against the TOE from the Security Target [6] are compliant with the related threats defined in the Protection Profile [9].

There is one Security policy to be fulfilled by the TOE, please refer to the Security Target [6], chapter 4.6:

Organisational security policy	Description
OSP.VERIFICATION	This policy shall ensure the adequacy between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority.

Table 4: Organisational security policy

1.5 Special configuration requirements

After its delivery, the TOE is embedded in the final product of a smartcard. It only features one fixed configuration (user mode), which cannot be altered by the user. The TOE was tested in this configuration, however, the TOE is only the software product according to the PP [9] and ST [6] and therefore no composition aspects were considered during the evaluation.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [6], chapter 4.4:

Assumption	Description
A.NATIVE	Those parts of the APIs written in native code as well as any pre-issuance native application on the card are assumed to be conformant with the TOE so as to ensure that security policies and objectives described herein are not violated.
A.VERIFICATION	All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.
A.APPLET	Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly “does not include support for native methods” outside the API.

Table 5: Secure usage assumptions of ST and PP

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 Java Card Mokard Safe 2.2 V2.4.0.

The following table summarises the TOE components and defines the evaluated configuration of the TOE:

Typ	Deliverables	Version / Date
SW	Mokard Safe 2.2 consisting of	2.4.0
SW	Code stored in ROM	2.3.3
SW	Code stored in EEPROM	2.4.0
DOC	Mokard Safe 2.2 The User and Administrator Guidance AGD_USR.1 – AGD_ADM.1	A-0 Draft 8 02.11.2005

Table 6: Identification of the TOE

For TOE identification the command APDU GET DATA for TOE ID is sent to the card. The card answers with the response APDU:

- ROM mask ID: 00 00 00 29.
- ROM code version: 00 02 03 03.
- EEPROM code version: 00 02 04 00.

The TOE version is equal to the EEPROM code version 2.4.0.

3 Security Policy

The security policy of the TOE is to provide card management functions for the card content management, applet selection and applet lifetime. It also provides functions for management of application key operations such as key distribution, access to keys, key generation and key destruction. It also assures the integrity of stored keys. Furthermore, cryptographic support is provided by the TOE. Another security policy of the TOE is to enforce the security model of the Java Card and manage the inter application resource sharing in a secure and controlled way. The object management of the TOE provides tasks for secure object management and the PIN verification procedure provides means to perform PIN verification, to update a PIN and to manage PIN counters. Other security policies of the TOE are to provide a self test function and to control all operations concerning the Java Card Remote Method Invocation as well as to control all operations concerning “persistent memory” modification.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

The Security Target does not contain usage assumptions.

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 4.4):

- Those parts of the APIs written in native code as well as any pre-issuance native application on the card are assumed to be conformant with the TOE so as to ensure that security policies and objectives described herein are not violated. (A.NATIVE)
- All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. (A.VERIFICATION)
- Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly “does not include support for native methods” outside the API. (A.APPLET)

Furthermore, the Security Target [6], chapter 4.6 defines an Organisational Security Policy (OSP.VERIFICATION) that ensures the adequacy between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority.

4.3 Clarification of scope

The TOE is a software product. The underlying chip hardware, the OS, the DS, the card manager, the bytecode verifier and any applets are not part of the TOE and have not been considered within the evaluation nor has a composite evaluation been performed. They are considered to be part of the IT environment.

Smartcards may be subject to TOE emanation attacks including power analysis and side channel emission measurements. Since the Smartcard platform is not part of the TOE but it is considered to be part of the IT-environment, no penetration tests related to power analysis or fault injection attacks via the hardware have been performed. The cryptolibrary provided by the chip manufacturer uses a hardware random number generator in order to generate prime numbers and the keys. Both cryptolibrary and the hardware random number generator are not part of the TOE. The underlying Smartcard chip S3CJ9QD as part of the IT environment is currently in the process of evaluation.

5 Architectural Information

The TOE (Java Card Mokard Safe 2.2 V2.4.0) is a software product. An overview of the architecture is given in section 3.1 of the Security Target [6] and in figure 1 of this report.

The TOE life-cycle as a part of a smartcard life-cycle is described in the protection profile [9] and consists of 3 main phases reproduced in the following:

Phase 1: TOE Development

- TOE specification, design, development & generation
- Mask software development and Mask IC production and test
- Testing, integration & validation
- Mask acceptance and Mask software maintenance and test

Phase 2: Production & Initialisation/Personalisation

- Platform initialisation
- Platform testing & production
- Golden sample (EEPROM binary image) generation and test, test and personalisation engineering, personalization sample card testing, sample card customer approval and mass production and test
- Initialisation/Personalisation (embedding of OS, Java Card System and applications in the card)

Phase 3: Usage

- Administration
- Configuration
- End-usage
- Loading & installation

At the end of phase 1 the TOE is delivered to the chip manufacturer in the form of ROM code. At the end of phase 2 the TOE is delivered to the end users embedded in the final product which is a smart card that is personalized and working, ready to provide services to end users.

Furthermore an administrator and user guidance (one document) is delivered to the application developer, the card embedder and the card issuer.

6 Documentation

The following documentation is provided by the developer to the application developer, the card embedder and the card issuer.

Document Name	Version / Date
Mokard Safe 2.2 The User and Administrator Guidance AGD_USR.1 – AGD_ADM.1	A-0 Draft 8 / 02.11.2005

Table 7: Documentation of the TOE

7 IT Product Testing

Developer Tests

Test Configuration

The TOE in the version 2.4.0 (ROM version 2.3.3 and EEPROM version 2.4.0) was tested in the TOE development environment using automated test tools. The TOE was also tested on a smart card as a java card, on a chip simulator with a virtual card reader, on a chip emulator and a card reader.

Test Approach

The test goal is to demonstrate that the TOE behaves as specified in the functional specification of the TOE. The developer's test strategy was to test all security functions together with the related interfaces as described in the functional specification.

Test Results

The developer's testing results demonstrate that the TOE performs as expected. All TSF behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

Independent Evaluator Tests

Test Configuration

The TOE was tested in form of the final product as smartcards as well as on an emulator.

The independent evaluator tests have been performed at the ITSEF facility in Essen while the repeated manufacturer tests have been performed by the evaluator within the test environment of the developer.

Test Approach:

For the sampling of repeated manufacturer tests the evaluator has performed a chosen subset of developer tests, so each TSF was covered by the tests. For independent testing the evaluator applied a test strategy that covered all TSF. The evaluator used the automated test tools of the developer to perform parts of the independent tests.

To verify and reject possible vulnerabilities, the ITSEF performed penetration tests. Some of these tests were performed in the TOE development environment using script based developer test tools. The majority of the penetration tests were performed in the test laboratory of the ITSEF.

Test Results

The independent tests as well as the repeated manufacturer tests confirmed that the TOE's security functions behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

During the evaluator's penetration testing the TOE operated as specified. The TOE withstood the penetration efforts of attackers with moderate attack potential in the intended environment for the TOE.

8 Evaluated Configuration

The Target of Evaluation (TOE) is a java card platform which consists of an installer and a Java Card Runtime Environment.

The TOE is a software product, therefore, the following do not belong to the TOE but to the IT environment (see also PP [9], chapter 2.1):

- Smart Card Platform which is comprised of the integrated circuit, the operating system and the dedicated software of the smart card. See also PP [9], chapter 2.1.4,
- Card manager, see also PP [9], chapter 2.1.3,
- Bytecode verifier, see also PP [9], chapter 2.1.1,
- any applets.

For evaluation, the tests of the TOE have been performed by the ITSEF using the Samsung S3CJ9QD, Firmware version: 13, Crypto Library version: S3CJ9QD RSA v3.2s, OS: 2.4.0.

The TOE is delivered to the end users embedded in the final product which is a smart card that is personalized and working, ready to provide services to end users.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] 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]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by ADV_IMP.2 and AVA_VLA.3 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
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
Installation, generation, and start-up procedures	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.2	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

Assurance classes and components		Verdict
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-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.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Moderately resistant	AVA_VLA.3	PASS

Table 8: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conformant to the Protection Profile PP/0305, JavaCard System Standard 2.2 Configuration Protection Profile [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant EAL4 augmented by ADV_IMP.2 and AVA_VLA.3.
- the following TOE Security Function fulfils the claimed Strength of Function: SF_CARD_MNGT for the mutual authentication procedure as a permutational mechanism.

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 holds for the algorithms listed in the security functions SF_CARD_MNGT, SF_CRYPTO_KEY, SF_CRYPTO_OP, as described in the Security Target [6], chapter 7.1.

The results of the evaluation are only applicable to the software product called Java Card Mokard Safe 2.2 V2.4.0 as identified in chapter 2 above.

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

Due to the nature of the TOE as a software product that is composed of the mask identifier, the ROM version, and the EEPROM version and that is a part of a smartcard product, there exist a number of requirements that are specified in the User and Administrator Guidance of the TOE [7].

The User and Administrator Guidance of the TOE [7] contains necessary information about the secure usage of the TOE and is delivered to the application developer, the card embedder and the card issuer who have to follow the requirements.

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.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [10] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CPU	Central Processin Unit
DS	Dedicated Software
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
OS	Operating System
PIN	Personal Identification Number
PP	Protection Profile

RAM	Random Access Memory
RMI	Remote Method Invocation
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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] Mokard Safe 2.2, ASE-Security Target, BSI-DSZ-0251-2005, Version B-0, Draft-11, Date 14.10.2005, (confidential document)

[7] Mokard Safe 2.2, The User and Administrator Guidance AGD_USR.1 – AGD_ADM.1, Version A-0, Draft-8, Date: 02.11.2005

[8] Evaluation Technical Report, BSI-DSZ-CC-0251-2005, Version 2, Date: 09.11.2005, (confidential document)

[9] Protection Profile PP/0305, JavaCard System Standard 2.2 Configuration Protection Profile

[10] Mokard Safe 2.2, ASE-Security Target Lite, BSI-DSZ-0251-2005, Version A-0, Date 10.11.2005

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 2.1 -Assurance family breakdown and mapping“

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 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 6.1 - 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.“

This page is intentionally left blank.