Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0171-2002

for

GemXplore'Xpresso V3 - Java Card Platform Embedded Software V3 (Core)

from

Gemplus S.A.

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

Deutsches
IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0171-2002

GemXplore’Xpresso V3 - Java Card Platform Embedded Software V3 (Core)

from

Gemplus S.A.

IT Security Certified

SOGIS-MRA

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, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/ IEC 15408)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria part 2 conformant**
Assurance Package:	**CC part 3 conformant** **EAL5 augmented by** **ALC_DVS.2 (Life cycle support - Sufficiency of security measures),** **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 Bundesamt für Sicherheit in der Informationstechnik 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, 15.02.2002

The President of the Bundesamt für
Sicherheit in der Informationstechnik

Dr. Henze L.S.

Common Criteria

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 Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by Bundesamt für Sicherheit in der Informationstechnik 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 Bundesamt für Sicherheit in der Informationstechnik (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 Bundesamt für Sicherheit in der Informationstechnik (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)
- The 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)

[2] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Bundesamtes für Sicherheit in der Informationstechnik (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 29th October 1992, Bundesgesetzblatt I p. 1838

[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. The agreement on the mutual recognition of IT security certificates based on the CC was extended up to and including the evaluation level EAL7.

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. As of November 2000, Israel joined the arrangement.

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 ‘GemXplore’Xpresso V3 - Java Card Platform Embedded Software V3 (Core)‘ has undergone the certification procedure at BSI.

The evaluation of the product ‘GemXplore’Xpresso V3 - Java Card Platform Embedded Software V3 (Core)’ was conducted by the Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH. The Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor, vendor and distributor is Gemplus S.A..

The certification is concluded with

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

This work was completed by the BSI on 15 February 2002.

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-13.

The product ‘GemXplore’Xpresso V3 - Java Card Platform Embedded Software V3 (Core)’ 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 0228/9582-111.

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] Gemplus S.A., Parc d’Activite de Gemenos – BP 100, 13881 Gemenos Cedex - France

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 *'GemXplore'Xpresso V3 - Java Card Platform Embedded Software V3 (Core)'*. The TOE provides an operating system for GSM applications written in Java. The TOE is based on:

- The Java Card specification (see [8], [9], [10]);
- The Open Platform specification (see [11]);
- The Visa Open Platform specification (see [11]) in compact configuration with PK (see [13]);

Figure 1 shows the scope of the TOE. The TOE includes the Java Card 2.1.1 support modules, the OP 2.0/ VOP 2.0.1 support modules and the native platform. The TOE does not include the micro-controller, the GSM layer and the application layer.

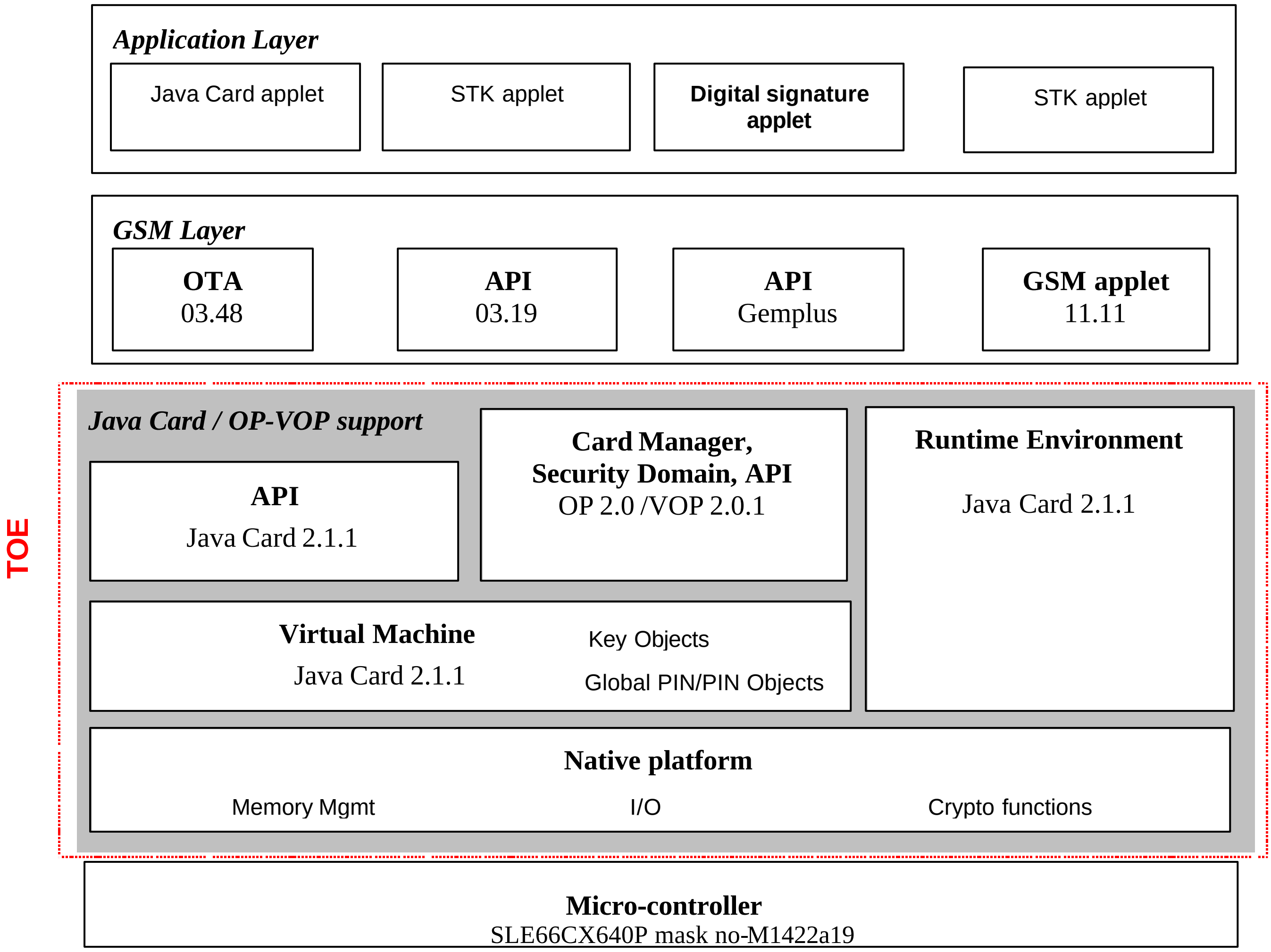

Figure 1 – TOE Architecture

The TOE was evaluated against the claims of the Security Target (see [5]) by the Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH. The evaluation was completed on 14 February 2002. The Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH is an evaluation facility recognised by BSI (ITSEF)[8].

The sponsor, vendor and distributor is Gemplus S.A..

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see Annex C of [1], Part 3 for details). The TOE meets the assurance requirements of assurance level EAL5+ (Evaluation Assurance Level 5 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL5	TOE evaluation: Semiformally designed and tested
+: ALC_DVS.2	Life cycle support - Sufficiency of security measures
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Assurance components and EAL-augmentation

1.2 Functionality

The TOE security functions are listed in the following table:

TOE Security Function	Description
SF_ACCESS_CONTROL	TOE access control enforcement
SF_AUDIT	Security Audit
SF_CARD_TERMINATING	Card Life Cycle Management
SF_CRYPTO_KEY	Cryptographic Key Management
SF_CRYPTO_OPERATION	Cryptographic Computation
SF_IDENTIFICATION_AUTHENTICATION	End user and administrator Identification and Authentication
SF_INTEGRITY	Data Integrity
SF_PIN	PIN Management
SF_SECURE_MESSAGING	Secure channel Management
SF_TRANSACTION	Transaction Management

TOE security functions

[8] Information Technology Security Evaluation Facility

1.3 Strength of Function

The strength of function for the security function SF_IDENTIFICATION_AUTHENTICATION is rated 'high' (SOF-high).

For the security functions SF_CRYPTO_KEY and SF_SECURE_MESSAGING the strength was not evaluated as it is a crypto algorithm suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

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

It is assumed that the attacker is a human being or a process acting on behalf of him.

The threats which were assumed for the evaluation and averted by the TOE are specified in the Security Target [5] and can be summarized as follows.

- Confidential data disclosure: Disclosure of confidential data, i.e. application code, cryptographic keys, Global PIN, PIN,
- Identity usurpation: Management (i.e. load, personalization) of Java Card Platform Embedded Software and application by unauthorized administrator, i.e. other than *Card manufacturer*, *Personalizer*, and *Card issuer*. Use of Application by unauthorized user, i.e. other than *End user*, and *Card issuer*.
- Data integrity loss: Use of a non-valid asset data.

1.5 Special configuration requirements

There is only one fixed configuration of the TOE.

1.6 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 Bundesamt für Sicherheit in der Informationstechnik (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 following TOE deliverables are provided for a customer who purchases the TOE:

- GemXplore'Xpresso V3 - Java Card Platform Embedded Software V3 (Core)

- User Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102593, Version_08, Release: 08.11.2001
- Administrator Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102592, Version_09, Release: 13.01.2002

3 Security Policy

The security policy of the TOE is to provide basic security functions to be used by Java applications. The TOE implements the following mechanisms:

- Logical separation or sharing of user data between applications.
- Authentication of the TOE administrators.
- Confidentiality of the platform's cryptographic keys, PIN, embedded software.
- Integrity of the platform's cryptographic keys, PIN, embedded software.

It also contributes by providing basic mechanisms that are listed below. It is the responsibility of the *application developers* to use these basic mechanisms properly in their applications:

- Authentication of the *end user*.
- Confidentiality of the application's cryptographic keys, PIN, and code.
- Integrity of the application's cryptographic keys, PIN, and code.
- External bi-directional communication protection against disclosure and corruption (secure messaging).

In the applet developed by the *application developer*, Global PIN and/or PIN could be used.

The *end user* has to know the Global PIN to use the TOE and after that there are one or more application specific PINs to:

- Build an authentication for two or more *end users.*
- Make an extra (second) authentication for some high sensitive applications.

The TOE can only have one Global PIN but many (one or more) application specific PINs.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

- Only the *end user* shall know the GLOBAL_PIN/PIN code in a deciphered way. The GLOBAL_PIN/PIN code mailing shall be separate from the card mailing. A card shall never be close to any document giving GLOBAL_PIN/PIN contents. A third party like a GSM operator or an applet provider generates the GLOBAL_PIN/PIN code.
- The *Card issuer* and administrator servers shall keep the cryptographic keys of the Card Manager and of the applications with a high level of confidentiality.

4.2 Environmental assumptions

- The TOE is used on the chip SLE66CX640P mask no-M142a19, which is currently under re-certification based on certificate TÜVIT-DSZ-ITSEC-9130-2001. The main security features of the certified chip are the following:
  - operating state checking,
  - data encryption with on-chip key management and random number generation,
  - phase management and test mode lock-out,
  - protection against snooping.
- With respect to the life cycle defined in the Security Target (see [5]) the *application developer* develops in phase 1 the applet to be loaded in the card during phase 5 and uses Java Compiler and Converter Virtual Machine in order to produce CAP and EXPORT files. Before loading these files in the card, the *Card manufacturer* verifies them by using the SUN verifier off-card according to the "Java Card 2.1.2 off-card verifier" document (see [14]). The role of this verifier is to check if CAP and EXPORT files are in conformance with the Java Card 2.1.1 specifications.

5 Architectural Information

The TOE can be divided in the Native Platform that consists of the Memory Manager, the Communication Manager and the Cryptographic Computation Subsystem. The next layer is composed of the Java Kernel, the Open Platform Loader and the SUN Javacard API (see Figure 1).

The TOE consists of the following subsystems as defined in the High-Level-Design.

Subsystem	Description
SS_JAVACARD	SUN Javacard API implementation
SS_KERNEL	Java Kernel

SS_OP_LOADER	Open Platform Loader implementation
SS_MEMORY	Memory Manager
SS_INPUT_OUTPUT	Communication Manager
SS_CRYPTOGRAPHY	Cryptographic Computation

Subsystems of the TOE

The following briefly describes the functionality of the subsystems:

1. SS_CRYPTOGRAPHY, in charge of

- all cryptographic algorithms
- key generation
- random data generation
- checksum computation
- secure comparisons and affectation

2. SS_INPUT_OUTPUT, in charge of

- communications management from/to outside the card
- GSM protocol handling

3. SS_JAVACARD, Java-Card API and herewith entry point for Java Applets to the following services

- ciphering
- signature
- random data generation
- key generation and implementation
- exception mechanism
- PIN management
- transaction management
- transient memory management

4. SS_KERNEL, in charge of

- execution of Java Card byte code
- management of exceptions
- control of the checksumed objects integrity
- applet isolation

5. SS_MEMORY, in charge of

- low level memory allocation
- low level backup management

6. SS_OP_LOADER, in charge of

- global PIN management
- key management
- applet loading, installation and deletion
- card life cycle management
- secure messaging management

6 Documentation

- User Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102593, Version_08, Release: 08.11.2001
- Administrator Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102592, Version_09, Release: 13.01.2002

7 IT Product Testing

The developer tests cover all security functions and all security mechanisms as identified in the functional specification, the high level design and the low level design.

The evaluators could repeat all tests of the developer either using the library of programs and tools delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer.

The penetration testing conducted confirmed that the TOE in the intended environment does not feature any exploitable vulnerabilities.

8 Evaluated Configuration

The TOE is 'GemXplore'Xpresso V3 - Java Card Platform Embedded Software V3 (Core)'. There is only one configuration of the TOE (all TSF are active and usable).

9 Results of the Evaluation

The Evaluation Technical Report (ETR) 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) 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 coordination with the Certification Body. 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 classes and components (according to EAL5 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

Assurance classes and components		Verdict
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	n.a.
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
Development tools CM coverage	ACM_SCP.3	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
Semiformal functional specification	ADV_FSP.3	PASS
Semiformal high-level design	ADV_HLD.3	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Semiformal low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.2	PASS
Formal TOE security policy model	ADV_SPM.3	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
Sufficiency of security measures	ALC_DVS.2	PASS
Standardised life-cycle model	ALC_LCD.2	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-low design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Covert chanel analysis	AVA_CCA.1	PASS
Analysis and testing for insecure states	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Verdicts for the assurance components (n.a.= not applicable)

The evaluation has shown that the TOE will fulfil the claimed strength of function for the security function SF_IDENTIFICATION_AUTHENTICATION.

For the security functions SF_CRYPTO_KEY and SF_SECURE_MESSAGING the strength was not evaluated as it is a crypto algorithm suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

10 Evaluator Comments/Recommendations

For the administrator it is mandatory to set the minimal PIN length to 6 and the ratification counter value equal or less then 3 to have the strength of the end user identification and authentication mechanism equal to SOF-high (see [7]).

11 Annexes

none

12 Security Target

For the purpose of publishing, the security target [5] of the target of evaluation (TOE) is provided as a separate document.

13 Definitions

13.1 Acronyms

CC	Common Criteria for IT Security Evaluation (see [1])
DES	Data Encryption Standard; symmetric block cipher algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GSM	Global System for Mobile communication
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
RNG	Random Number Generator
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

VOP	Visa Open Platform

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from 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 (ISO/IEC 15408)

[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, Version 5.1, January 1998)

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

[5] ASE - Security Target - Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102590, Version_20, Release: 25.01.2002

[6] User Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102593, Version_08, Release: 08.11.2001

[7] Administrator Guidance – Java Card Platform Embedded Software V3 (Core) – GemXplore'Xpresso V3, Ref.: DPC102592, Version_09, Release: 13.01.2002

[8] Java Card 2.1.1 API Specification, SUN Microsystems Inc.

[9] Java Card 2.1.1 Virtual Machine Specification, SUN Microsystems Inc.

[10] Java Card 2.1.1 Runtime Environment (JCRE) Specification, SUN Microsystems Inc.

[11] Open Platform Card Specification V2.0.1, Visa International

[12] Visa Open Platform Card Implementation, Visa International

[13] OP 2.0.1 Visa Card Implementaion Guide – Configuration 2, Compact with PK, Visa International

[14] Java Card 2.1.2 Off-card verifier, SUN Microsystems

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (Kapitel 5.4)

The pass result of evaluation shall be a statement that describes the extent to which the PP or TOE can be trusted to conform to the requirements. The results shall be caveated with respect to Part 2 (functional requirements), Part 3 (assurance requirements) or directly to a PP, as listed below.

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

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

c) **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an **EAL** or **assurance package** that is based only upon assurance components in Part 3.

d) **Part 3 augmented** - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an **EAL** or **assurance package**, plus other assurance components in Part 3.

e) **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an **EAL** associated with additional assurance requirements not in Part 3 or an **assurance package** that includes (or is entirely made up from) assurance requirements not in Part 3.

f) **Conformant to PP** - A TOE is conformant to a PP only if it is compliant with all parts of the PP.

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 in as much 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.