Federal Office
for Information Security

Certification Report

BSI-CC-PP-0038-2007

for

BAROC CC 3.1 Smart Card Protection Profile
Version 1.0

from

The Bankers Association of the Republic of China (BAROC)

Deutsches IT-Sicherheitszertifikat
erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0038-2007

Common Criteria Protection Profile

BAROC CC 3.1 Smart Card Protection Profile
Version 1.0

developed by The Bankers Association of the Republic of China (BAROC)

Assurance Package claimed in the Protection Profile:
   Common Criteria Part 3 conformant
   EAL 4 augmented by
   AVA_VAN.5 – Advanced methodical vulnerability analysis

Common Criteria
Arrangement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM), Version 3.1* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 3.1.*

This certificate applies only to the specific version and release of the Protection Profile 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.

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

Bonn, 11. December 2007
The President of the Federal Office for Information Security

Dr. Helmbrecht   L.S.

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

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.

---

[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) [3]

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5]

- Common Methodology for IT Security Evaluation, Version 3.1

- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

- Procedure for the Issuance of a PP certificate by the BSI

2   Recognition Agreements

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

2.1   International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including

---

[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 07 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 12 February 2007 in the Bundesanzeiger dated 23 February 2007

EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org.

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 PP BAROC CC 3.1 Smart Card Protection Profile, Version 1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-PP-0021-2006.

The evaluation of the PP BAROC CC 3.1 Smart Card Protection Profile, Version 1.0 was conducted by the ITSEF Evaluation Body for IT Security of TÜV Informationstechnik GmbH. The evaluation was completed on 6. December 2007. The ITSEF Evaluation Body for IT Security of TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: The Bankers Association of the Republic of China (BAROC).

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI on 11. December 2007.

4   Validity of the certification result

This Certification Report only applies to the version of the Protection Profile as indicated.

In case of changes to the certified version of the Protection Profile, the validity can be extended to the new versions and releases, provided the applicant applies for assurance continuity (i.e. re-certification or maintenance) of the modified Protection Profile, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

---

[6]   Information Technology Security Evaluation Facility

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

5   Publication

The following Certification Results contain pages B-1 to B-8.

The PP BAROC CC 3.1 Smart Card Protection Profile, Version 1.0 has been included in the BSI list of the certified Protection Profiles, 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 developer[7] of the Protection Profile. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

[7]   The Bankers Association of the Republic of China (BAROC)
3F, No. 9, De-Muei St.
Taipei 10461, Taiwan, R.O.C.

This page is intentionally left blank.

B   Certification Results

The following results represent a summary of

- the certified Protection Profile,

- the relevant evaluation results from the evaluation facility, and

- complementary notes and stipulations of the certification body.

Contents of the certification results

1   Protection Profile Overview

This Protection Profile BAROC CC 3.1 Smart Card Protection Profile, Version 1.0 [7] is established by The Bankers Association of the Republic of China (BAROC) as a basis for the development of Security Targets in order to perform a certification of an IT-product (TOE).

The PP is developed to serve as a baseline for the security requirements of smart cards developed by different vendors. These smart cards will be used for the financial transactions within the FISC inter-bank system which is a general-purpose platform for switching financial transactions between banks.

The PP focuses on a financial smart card which consists of embedded software and a secure IC Controller. The TOE is used as a security token for inter-bank financial transactions, such as cash withdrawal, fund transfer, tax payment and online sale.

The TOE security functionality consists of:

TAC (Transaction Authentication Code) generation

> The TOE calculates a TAC on transaction data. The TAC ensures authenticity and integrity of the transaction data. In addition to the TAC, the TOE also generates a transaction S/N (serial number) which participates in the calculation of the TAC. In order to generate a TAC, the user has to enter a PIN for confirmation.

Secure key update

> The TOE is providing a secure means to update cryptographic keys (especially the key which is used for TAC generation) that will be stored in the TOE.

Protection of TSF and user data

> The TOE protects its TSF and user data from unauthorized modification and disclosure.

For the private key used for generating „TACs", a secure cryptographic key creation device generating keys with sufficient quality is required in the TOE operational environment. Furthermore, a secure CAD (Card Accepted Device) for the key update process providing an authentication and encryption mechanism is required in the TOE operational environment. Rather, the functions of the TOE are to generate „TACs" and to maintain the secrecy of the private key used for generating these „TACs".

It should be noted that it is considered by the PP authors to be impossible for the user to maintain confidentiality of their PIN, thus the disclosure of the PIN during entry by the CAD is not considered as a threat to the TOE in this PP.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [7], chapter 3.1. Based on these assets the

security environment is defined in terms of assumptions, threats and policies. This is outlined in the Protection Profile [7], chapters 3.2, 3.3 and 3.4.

These assumptions, threats and policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the IT-Environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [7], chapters 4.1 and 4.2.

The Protection Profile [7] requires a Security Target based on this PP or another PP claiming this PP, to be strict conformant.

2   Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of security functional requirements to be implemented by a TOE. It covers the following issues:

-    TAC (Transaction Authentication Code) generation

-    Secure key update

-    Protection of TSF and user data

For a detailed description of the TOE´s security functionality refer to section 1 in part B of this Certification Report.

These TOE security functional requirements (SFR) are outlined in the PP [7], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

<div align="center">Common Criteria Part 2 extended</div>

3   Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_VAN.5 – Advanced methodical vulnerability analysis

(for the definition and scope of assurance packages according to CC see part C or [1], part 3 for details).

4   Results of the PP-Evaluation

The Evaluation Technical Report (ETR), [6] 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.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE.

The following assurance components were used:

> APE_INT.1 PP introduction
> APE_CCL.1 Conformance claims
> APE_SPD.1 Security problem definition
> APE_OBJ.2 Security objectives
> APE_ECD.1 Extended components definition
> APE_REQ.2 Derived security requirements

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-PP-0021-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following aspects:

Regarding the content, this PP is identical to the PP already certified according to Common Criteria version 2.1 by BSI under the certification ID BSI-PP-0021-2006. Solely the structure and wording of this PP are adapted in order to be consistent with the new requirements of Common Criteria version 3.1 [1]. In addition, some editorial changes have been applied in order to improve the readability and comprehensibility of the PP. The augmentation of ADV_IMP.2 in the previous PP version is covered completely by ADV_IMP.1 in [1].

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5   Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

- The PP does not include any threats against the discovery of the PIN and, in particular, there is no functionality that enforces the privacy of the PIN in the environment, i.e. there is no secure path between the cardholder and the TOE. Hence, this PP is only appropriate for a TOE where the intended application does not require the confidentiality of the PIN.

- For the private key used for generating „TACs" (Transaction Authentication Code), a secure cryptographic key creation device generating keys with sufficient quality is required in the TOE operational environment.

- A secure CAD (Card Accepted Device) for the key update process providing an authentication and encryption mechanism is required in the TOE operational environment.

6   Protection Profile Document

The Protection Profile BAROC CC 3.1 Smart Card Protection Profile, Version 1.0 [7] is being provided within a separate document as Annex A of this report.

7   Definitions

7.1   Acronyms

ATM	Automated Teller Machine
BAROC	The Bankers Association of the Republic of China
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CAD	Card Accepted Device
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CD/ATM	Cash Dispenser/ Automated Teller Machine
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ES	Embedded Software
FISC	Financial Information Services Co., Ltd.
ICC	Integrated Circuit Controller
ID	Identification
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
PIN	Personal Identification Number
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SPA	Simple Power Analysis
ST	Security Target
TAC	Transaction Authentication Code
TOE	Target of Evaluation
TSF	TOE Security Functions / Functionality

7.2   Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

8   Bibliography

[1]   Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev. 2, September 2007

      Part 1: Introduction and general model, CCMB-2006-09-001,

      Part 2: Security functional components, CCMB-2007-09-002,

      Part 3: Security assurance components, CCMB-2007-09-003

[2]   Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007, CCMB-2007-09-004

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

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

          -    AIS 38, Version 2, 28. September 2007, Reuse of evaluation results

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

[6]   Evaluation Technical Report – Summary (ETR Summary), Version 2, BSI-CC-PP-0038-2007, 6. December 2007, TÜViT GmbH (confidential document)

[7]   BAROC CC 3.1 Smart Card Protection Profile, Version 1.0, 6. December 2007, The Bankers Association of the Republic of China (BAROC)

C   Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.

- describes the conformance to CC Part 2 (security functional requirements) as either:

  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or

  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.

- describes the conformance to CC Part 3 (security assurance requirements) as either:

  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or

  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:

  - the SFRs of that PP or ST are identical to the SFRs in the package, or

  - the SARs of that PP or ST are identical to the SARs in the package.

- Package name Augmented - A PP or ST is an augmentation of a predefined package if:

  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.

  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

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

- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

"Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP."

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition

Class ASE: Security Target evaluation (chapter 11)

" Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation."

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

" The following Sections describe the constructs used in representing the assurance classes, families, and components."
"Each assurance class contains at least one assurance family."
"Each assurance family contains one or more assurance components."

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

" 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 CC 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 8.1)

"Table 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 7 of this CC 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 standard 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS				1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VLA	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

"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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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."

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

"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 practise. 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 8.5)

"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 practises.

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 8.6)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

"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 8.9)

"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."

Class AVA: Vulnerability assessment (chapter 16)

"The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE."

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

This page is intentionally left blank

D   Annexes

List of annexes of this certification report

Annex A: Protection Profile BAROC CC 3.1 Smart Card Protection Profile,
              Version 1.0 [7] provided within a separate document.

This page is intentionally left blank.