Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0442-2008

for

## BAROC/FISC Terminal Security Access Module Version 1.0

from

## Financial Information Service Co., Ltd. (FISC)

sponsored by

## The Bankers Association of the Republic of China (BAROC)

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-0442-2008**

Smartcard Composition

**BAROC/FISC Terminal Security Access Module**
Version 1.0

| | |
|---|---|
| from | Financial Information Service Co., Ltd. (FISC) |
| sponsored by | The Bankers Association of the Republic of China (BAROC) |
| PP Conformance: | Java Card System Protection Profile Collection - Minimal Configuration, DCSSI PP/0303 |
| Functionality: | PP conformant<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by<br>ADV_IMP.2 and AVA_VLA.4 |

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 15 September 2008
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

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.

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....7

1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC - Certificates....8
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....9
5 Publication....9

B Certification Results....11

1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....14
4 Assumptions and Clarification of Scope....15
5 Architectural Information....15
6 Documentation....16
7 IT Product Testing....16
8 Evaluated Configuration....17
9 Results of the Evaluation....17
9.1 CC specific results....17
9.2 Results of cryptographic assessment....18
10 Obligations and notes for the usage of the TOE....19
11 Security Target....19
12 Definitions....19
12.1 Acronyms....19
12.2 Glossary....20
13 Bibliography....22

C Excerpts from the Criteria....25

D Annexes....33

# 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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

## 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 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

## 2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for 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 Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

## 2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including 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 Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ADV_IMP.2 and AVA_VLA.4 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 BAROC/FISC Terminal Security Access Module Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product BAROC/FISC Terminal Security Access Module Version 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 05 August 2008. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: Financial Information Service Co., Ltd. (FISC).

[6] Information Technology Security Evaluation Facility

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

# 4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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

# 5 Publication

The product BAROC/FISC Terminal Security Access Module Version 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de) and [5]. 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 product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Financial Information Service Co., Ltd. (FISC)
No. 81
Kang-Ning Rd., Sec. 3
Nei-Hu District
Taipei
Taiwan R. o. C.

This page is intentionally left blank.

# 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.

# 1 Executive Summary

The Target of Evaluation (TOE) is a Terminal Security Access Module (TSAM) and supports secure transactions in-between POS terminal and the remote host application in a way that it assures integrity, authenticity and confidentiality of POS transactions by encryption, decryption and MAC generation.

The functions of TSAM are:

- TSAM is provisioned with a management key, an encryption key, a decryption key and a MAC generation key.
- The POS terminal is equipped with a TSAM in one of its slots. The terminal asks for data encryption from TSAM when it is submitting a transaction to the remote host. The terminal performs encryption of the sensitive part of the transaction message by sending it to TSAM via "Data Encryption by Working Key" command and TSAM responds with the encrypted datagram. The terminal can also perform decryption of the encrypted part of the received transaction message by sending it to TSAM and TSAM responds with the decrypted result.
- By using TSAM, the terminal calculates the MAC for each transaction. The terminal prepares the transaction representation from the transaction message and sends the transaction representation to TSAM. TSAM responds with a MAC over the data it receives from its interface.
- TSAM is managed by the remote host, which means the management key and working keys (encryption, decryption and MAC) are subject to be changed over time via online transaction. The key management must be secure, and therefore, there is a unique management key for each TSAM so that the remote host can assure the integrity, confidentiality, and authenticity of the key management process.

The TOE is composed of a JavaCard applet and the NXP P541G072V0P (JCOP 41, v2.3.1) smart card platform and embedded software and native application [10]. While the JCP (JavaCard Platform) resides in ROM, the TSAM Applet resides in EEPROM of NXP P541G072V0P (JCOP 41, v2.3.1). NXP P541G072V0P (JCOP 41, v2.3.1) was evaluated separately, the respective certification report is BSI-DSZ-CC-0426 [11]. The TSAM applet is loaded and installed into NXP P541G072V0P (JCOP 41, v2.3.1), therefore, the TOE is a composition of the TSAM applet and NXP P541G072V0P (JCOP 41, v2.3.1). The GlobalPlatform keys necessary for applet management are not delivered together with the TOE, therefore it will not be possible to delete the TSAM applet from or install additional applets into the smart card controller after delivery.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Java Card System Protection Profile Collection - Minimal Configuration [9].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 4 augmented by ADV_IMP.2 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.5.

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

| TOE Security Function | Addressed issue |
|---|---|
| SF.AUT_GP | TSAM_GlobalPlatform authentication |
| SF.CP_GP | TSAM_GlobalPlatform communication protection |
| SF.CP_MK | Communication protection with MK |
| SF.AC | Access control |
| SF.LCM | Life cycle management |
| SF.SDP | Stored data protection |
| SF.USE_WK | Use of working keys |
| SF.Embedded_Software | Summary of embedded software security functions from [10] |
| SF.Hardware | Hardware security function from [10] |

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.2 is confirmed. 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). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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:

**BAROC/FISC Terminal Security Access Module (TSAM) Version 1.0**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/SW | The initialized TSAM product BAROC/FISC TSAM 1.0 (JCOP 41 v2.3.1, comprising of the smart card platform, the java card platform and BAROC/FISC TSAM 1.0 java card applet) and the corresponding initial management key are delivered to the TSAM issuer site. | 1.0<br>C.READ_VERSION response: '01 00 00'h<br>ATR JCOP41V231 platform with loaded TSAM applet: 3B FF 13 00 00 81 31 FE 45 42 41 52 4F 43 2F 46 49 53 43 20 54 53 41 4D A1<br>Application Identifier of TSAM applet (AID): A0 00 00 01 72 95 00 02. | Physical delivery of hardware containing firmware/software delivered via carrier company. |
| 2 | DOC | Administrator and User Guidance for BAROC/FISC TSAM 1.0 [13] | Version 1.0.0, date: 2008-05-21 BAROC/FISC<br>SHA-1 hash value of the PDF version: 94db00658c8790 2818433487eed8 2a88d8408114 | Delivered via email.<br>Verification of the authenticity/integrity of the guidance by comparing the calculated hash value of the electronically Guidance version with the published hash value. |
| 3 | OTHER | The seed IMK (SIMK), which is a 112-bit 3/DES key used to calculate the IMK contained in each individual copy of TSAM | N/A | Delivered via tamper-evident envelop by mail. In case tampering is detected or suspected, the issuer must not use the SIMK. |

Table 2: Deliverables of the TOE

The TOE undergoes the process of loading, installing and initializing the TSAM applet with GlobalPlatform keys. This is done at the production site. After loading and installation of the TSAM applet, the TOE is completed and its security functionality is operative. During subsequent initialization, the initial management key is written, which is necessary for personalization. The initialized TOE and the corresponding initial management key are delivered to the TSAM issuer site. For details please see [6] chapter 2.4.

The usage phase starts with the personalization process of TSAM by the issuer, which includes doing the mandatory first update of the management key and writing of terminal management data. The process is done at TSAM issuer site. For details please see [6] chapter 2.4.

# 3 Security Policy

The TOE is a composition of a JavaCard applet and the underlying smart card controller. The Security Policy is expressed by the set of Security Functional Requirements and

implemented by the TOE. It covers the issues Identification and Authentication, Key Access, TMD Access Policy, Life Cycle, and Stored Data Protection.

The Identification and Authentication policy associates a user of the TOE with one of several roles at a time. The Key Access Policy grants the access to several keys on specific rules. The Terminal Management Data (TMD) Access Policy grants access to TMD (Terminal Management Data) on the base of specific rules. The Life Cycle Policy controls the life cycle states of the TOE. The Stored Data Protection Policy monitors the integrity of TMD, LCS and RC data and takes some actions in case of the detection of an integrity error.

# 4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Issuer and the developer of the POS Terminal shall verify the hash values of their guidance documents as stated in the ST introduction to assure a secure delivery of it. The Issuer shall only issue the TOE after he could successfully verify the MAC returned by the TOE during first MK (management key) update with the delivered management key.
- The environment shall support and use secure communication protocols offered by the TOE.
- The management key and working keys which are stored and processed outside the TOE during personalization and usage phases shall be protected for confidentiality and integrity.
- Cryptographic keys created in the environment to be used within the TOE have to have sufficient quality by using a random number generator for key generation.
- No native codes shall be loaded into the hardware platform chip during development and production phases of the TOE. During development, byte code verification shall be performed on the TSAM applet. During production, only the TSAM applet shall be installed. GlobalPlatform keys shall not be delivered to Issuer and POS Terminal.
- TOE development and test information during TSAM.Phase_1 and TSAM.Phase_2 (see [6] chapter 2.4) shall be protected in a secure environment for its integrity and confidentiality. In case of delivery between different actors like applet developers and applet installers, this information shall be also protected in the same manner as aforementioned.

Details can be found in the Security Target [6] chapter 4.2.

For details addressed in the underlying platform please read the Security Target [6] chapter 4.2.2 or the Security Target of the underlying platform [10] chapter 3.3.

# 5 Architectural Information

The overall TOE architecture including the underlying hardware platform is displayed in figure 2-1 of the security target [6].

The TSAM applet is divided into 6 subsystems. The main purpose for each subsystem is described shortly in the following:

- One subsystem communicates with the external world. It performs the basic APDU command parameter checking and security checking. It utilizes the interface provided by other subsystems to perform the management of the assets (i.e. several keys). It is also in charge of the Life Cycle management.
- One subsystem manages the MK and functions used in utilizing the MK to assure the APDU command's authenticity, integrity and confidentiality.
- One subsystem includes the functions used in managing the WKs and functions used in utilizing the WKs to provide cryptographic services for transaction data.
- One subsystem is in charge of functions used in managing and reading the TMD for transaction.
- One subsystem is used as a Store Data Protector (SDP) by providing functions to help other subsystems to maintain and check the checksum of critical data. The checksum ensures the integrity of the critical data (i.e. LCS, RC and TMD) stored in other subsystems.
- One subsystem is used as a Data Manager (DM) to manage or check the data used by each subsystem and provides temporary buffers or objects which are needed by each subsystem during processing.

# 6 Documentation

The evaluated documentation [13] as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7 IT Product Testing

The TOE has been tested as a composite product on its hardware platform. According to the defined configuration only the contact interface and the corresponding protocol T=1 was available.

The developer has tested all nine TSF of the TOE (seven TSF of the TSAM applet and indirectly two security functions of the used hardware platform).

The testing strategies were executed in individual test scenarios so that all TSF have been successfully tested against the functional specification and the high level design of the TOE. The developer's testing results demonstrate that the TSF perform as specified. The developer's testing results demonstrate that the TOE performs as expected.

The evaluators have tested all nine TSF of the TOE (seven TSF of the TSAM applet and indirectly two security functions of the used hardware platform).

The evaluators have repeated developer tests and have performed own tests that cover all TSF. During the evaluator's TSF subset testing the TOE operated as specified. The evaluators have verified the developer's test results by executing a sample of tests of the developer's test documentation.

The evaluators have performed penetration testing based on the developer's and on the evaluator's vulnerability analysis. During the evaluator's penetration testing the TOE operated as specified. In the intended environment of use the TOE does not feature exploitable vulnerabilities for attackers possessing a high attack potential if all the measures required are taken into consideration.

# 8 Evaluated Configuration

This certification covers only one fixed configuration which cannot be altered by the user. The TOE is uniquely identifiable by the following data:

- C.READ_VERSION response: '01 00 00'h.
- ATR JCOP41V231 platform with loaded TSAM applet: 3B FF 13 00 00 81 31 FE 45 42 41 52 4F 43 2F 46 49 53 43 20 54 53 41 4D A1.
- Application Identifier of TSAM applet (AID): A0 00 00 01 72 95 00 02.

Delivery Protection of TSAM:

When TSAM copies are delivered to the issuer, they contain IMKs (initial management key). Different copies of TSAM have different values of its contained IMK, they are generated from its MKSN (MK Serial Number) with SIMK (Seed Initial Management Key, the seed key that is used to generate diversified IMKs).

To verify authenticity of the delivered TSAM, the issuer verifies the card cryptogram that is provided by TSAM in the response of the C.UPD_INIT_MK command (see also Guidance [13]). If the cryptogram can be verified successfully, the delivered TSAM contains the correct IMK.

# 9 Results of the Evaluation

## 9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

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

*(ii) The ETR [7] builds up on the ETR-lite for Composition documents of the evaluation of the underlying product "NXP P541G072V0P (JCOP 41, v2.3.1)". The ETR-lite for Composition is in this case identical to the ETR of the underlying product [12] and was provided by the ITSEF TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]).*

*(iii) For smart card specific methodology the scheme interpretations AIS 25 and AIS 26 (see [4]) were used.*

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components ADV_IMP.2 and AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Java Card System Protection Profile Collection - Minimal Configuration [9]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ADV_IMP.2 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function High:
  - SF.AUT_GP, TSAM_GlobalPlatform authentication
  - SF.CP_GP TSAM_GlobalPlatform communication protection
  - SF.CP_MK, Communication protection with MK
  - SF.SDP, Stored data protection
  - SF.Embedded_Software, Summary of embedded software security functions from [10]
  - SF.Hardware, Hardware security function from [10]

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

## 9.2 Results of cryptographic assessment

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:

- SF.AUT_GP: 3/DES-key (16 byte) is effective 112 bit long.
- SF.USE_WK: 3/DES encryption/ decryption in ECB mode with key size of 112 bits. 3/DES MAC generation in CBC mode with key size 112 bits.
- SF.Embedded_Software: 3DES (112 and 168 bit keys) for en-/decryption (CBC and ECB) and signature (MAC) generation and verification, AES (Advanced Encryption Standard) with key length of 128, 192, and 256 Bit for en-/decryption (CBC and ECB), RSA (1024 up to 2368 bits keys) for en-/decryption and signature generation and verification.

# 10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, the following aspects need to be fulfilled when using the TOE:

In case of tampered PIN-mailer Delivery the issuer is required to stop using the delivered TSAM TOE immediately. The event happens when any of the recipients of SIMK (in the form of A-part and B-part in two distinct PIN-mailers) detect that the tamper-resistant envelop of A-part or B-part has been opened during delivery. The tamper-resistant envelop is to protect the delivery of SIMK. Therefore, the event alerts TSAM issuer that the delivery is no longer secure.

In case of non-trusted TSAM Delivery the delivered copy of TSAM must not be used. Furthermore, TSAM issuer should stop the personalization process and contact FISC to clarify the integrity/authenticity problem. The event happens when the verification of the card cryptogram in the response APDU of the C.UPD_INIT_MK command during TSAM personalization fails. The card cryptogram is to ensure the integrity/authenticity of the delivered copy of TSAM. Therefore, the event alerts TSAM issuer that the delivered TSAM is non-trusted.

For the expiry of the cryptographic algorithms please refer to the relevant and applicable national directives. The usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms.

# 11 Security Target

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

# 12 Definitions

## 12.1 Acronyms

| | |
|---|---|
| **3/DES** | Triple Data Encryption Standard |
| **APDU** | Application Protocol Data Unit |
| **BAROC** | The Bankers Association of the Republic of China |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **CBC** | Cipher Block Chaining |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **DES** | Data Encryption Standard |
| **DM** | Data Manager |
| **EAL** | Evaluation Assurance Level |
| **ECB** | Electronic Code Book |
| **EEPROM** | Electrically Erasable Programmable Read Only Memory |

| | |
|---|---|
| **FISC** | Financial Information Service Co., Ltd. |
| **JCP** | Java Card Platform |
| **IMK** | Initial Management Key |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **LCS** | Life Cycle State |
| **MAC** | Message Authentication Code |
| **MK** | Management Key |
| **MKSN** | MK Serial Number |
| **PIN** | Personal Identification Number |
| **POS** | Point of Sales |
| **PP** | Protection Profile |
| **RC** | Retry Counter |
| **ROM** | Read Only Memory |
| **SAR** | Security Assurance Requirement |
| **SDP** | Store Data Protector |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SIMK** | Seed Initial Management Key |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **TMD** | Terminal Management Data |
| **TOE** | Target of Evaluation |
| **TSAM** | Terminal Security Access Module |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |
| **WK** | Working Key |

## 12.2 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.

# 13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

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

[6] Security Target BSI-DSZ-442-2008, Version 1.0.0, Date 2008-05-21, Document Title: Security Target for BAROC/FISC TSAM 1.0, BAROC & FISC

[7] Evaluation Technical Report, BSI-DSZ-CC-0442, Version 3, Date 2008-07-30, Product:BAROC/FISC TSAM 1.0, ITSEF: TÜVIT (confidential document)

[8] Configuration list for the TOE: Configuration Management for 1 BAROC/FISC TSAM 1.0, Version: 1.0.0, Date: 2008-05-21, Authors: BAROC & FISC (confidential document)

[9] Java Card System Protection Profile Collection, Version: 1.0b, August 2003. This Document contains 4 protection profile, whereas "Java Card System - Minimal Configuration Protection Profile" (registered at DCSSI under Registration number PP/0303) is relevant for this ST

[10] Security Target Lite, NXP P541G072V0P (JCOP 41 v2.3.1), Secure Smart Card Controller, Version 1.0, 2007-07-23, IBM Deutschland Entwicklung GmbH

[11] Bundesamt für Sicherheit in der Informationstechnik, Certification Report BSI-DSZ-CC-0426-2007 for NXP P541G072V0P (JCOP 41 v2.3.1) from IBM Deutschland Entwicklung GmbH and
Assurance Continuity Maintenance Report BSI-DSZ-CC-0426-2007-MA-01,

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

Smartcard with Java Card Platform NXP P521G072V0P (JCOP 21 v2.3.1), NXP P531G072V0P (JCOP 31 v2.3.1) and NXP P531G072V0Q (JCOP 31 v2.3.1) from IBM Deutschland Entwicklung GmbH

[12] Evaluation technical report (ETR), BSI-DSZ-CC-0426, Product: NXP P541G072V0P (JCOP 41, v2.3.1), Version 1.0, Date 2007-07-27, ITSEF: TÜVIT (confidential document)

[13] Administrator and User Guidance for BAROC/FISC TSAM 1.0, Version 1.0.0, date: 2008-05-21, BAROC/FISC

This page is intentionally left blank.

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC 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:

**Protection Profile criteria overview** (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

| Assurance Class | Assurance Family |
|---|---|
| Class APE: Protection Profile evaluation | TOE description (APE_DES) |
| | Security environment (APE_ENV) |
| | PP introduction (APE_INT) |
| | Security objectives (APE_OBJ) |
| | IT security requirements (APE_REQ) |
| | Explicitly stated IT security requirements (APE_SRE) |

Table 3 - Protection Profile families - CC extended requirements”

**Security Target criteria overview** (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

| Assurance Class | Assurance Family |
|---|---|
| Class ASE: Security Target evaluation | TOE description (ASE_DES) |
| | Security environment (ASE_ENV) |
| | ST introduction (ASE_INT) |
| | Security objectives (ASE_OBJ) |
| | PP claims (ASE_PPC) |
| | IT security requirements (ASE_REQ) |
| | Explicitly stated IT security requirements (ASE_SRE) |
| | TOE summary specification (ASE_TSS) |

Table 5 - Security Target families - CC extended requirements ”

**Assurance categorisation** (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

| Assurance Class | Assurance Family |
|---|---|
| ACM: Configuration management | CM automation (ACM_AUT) |
| | CM capabilities (ACM_CAP) |
| | CM scope (ACM_SCP) |
| ADO: Delivery and operation | Delivery (ADO_DEL) |
| | Installation, generation and start-up (ADO_IGS) |
| 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) |
| AGD: Guidance documents | Administrator guidance (AGD_ADM) |
| | User guidance (AGD_USR) |
| ALC: Life cycle support | Development security (ALC_DVS) |
| | Flaw remediation (ALC_FLR) |
| | Life cycle definition (ALC_LCD) |
| | Tools and techniques (ALC_TAT) |
| ATE: Tests | Coverage (ATE_COV) |
| | Depth (ATE_DPT) |
| | Functional tests (ATE_FUN) |
| | Independent testing (ATE_IND) |
| AVA: Vulnerability assessment | Covert channel analysis (AVA_CCA) |
| | Misuse (AVA_MSU) |
| | Strength of TOE security functions (AVA_SOF) |
| | Vulnerability analysis (AVA_VLA) |

Table 1: Assurance family breakdown and mapping”

**Evaluation assurance levels** (chapter 11)

“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 11.1)

“Table 6 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 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 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: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 11.3)

“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 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 11.4)

“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 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 11.5)

“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 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 11.6)

“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 11.7)

“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 11.8)

“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 11.9)

“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.“

**Strength of TOE security functions (AVA_SOF)** (chapter 19.3)

“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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

# D Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.