Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0355-2006

for

Sharp passport booklet module
Version 1.1

from

Sharp Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0355-2006

Sharp passport booklet module Version 1.1

from

Sharp Corporation

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** **AVA_VLA.4 – Highly Resistant**

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

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

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

Bonn, September 29th, 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

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

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

Preliminary Remarks

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

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), 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 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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

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

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

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

2.2 CC - Certificates

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

This evaluation contains the components AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of this assurance family is 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 Sharp passport booklet module, Version 1.1 has undergone the certification procedure at BSI. Regarding the underlying hardware being part of this composite evaluation, specific results from the evaluation process based on BSI-DSZ-CC-0245-2005 were used.

The evaluation of the product Sharp passport booklet module, Version 1.1 was conducted by brightsight® BV[6]. brightsight® BV is an evaluation facility (ITSEF)[7] recognised by BSI.

The sponsor, vendor and distributor is:

Sharp Corporation
2613-1 Ichinomoto-cho
Tenri, Nara
Japan

The certification is concluded with

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

This work was completed by the BSI on 29 September 2006.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, 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 brightsight® BV was formerly known as TNO ITSEF BV.

7 Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18 and D1 to D-4.

The product Sharp passport booklet module, Version 1.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[8] of the product.

[8] Sharp Corporation
2613-1 Ichinomoto-cho
Tenri, Nara
Japan

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 the SHARP passport booklet module (called the passport booklet). This TOE comprises the application for the Passport Booklet „ePassJP“, a card operating system „eP-APE“ and the SM4128(V3) module (a packaged IC).

ePassJP is the application implementing e-passport functions according to the ICAO-document [10] for Machine Readable Travel Documents. The card operating system eP-APE supports that the ePassJP can run on the SM4128(V3) module. The module SM4128(V3) was certified under BSI-DSZ-CC-0245-2005 and is therefore described separately in the hardware Security Target [9].

The Security Target of the TOE [7] is based on the Protection Profile for IC for the passport booklet [13][9] that represents the official requirements of the Japanese Government. Concerning eavesdropping, an additional objective for the environment is added to the Security Target to be in line with international developments regarding Machine Readable Travel Documents with „ICAO Applications“ (e.g. [14]). The Protection Profile is referenced in the Security Target and contained in an appendix of [7].

The following figure taken from the ETR [8] shows the seven different phases of the TOE's lifecycle:

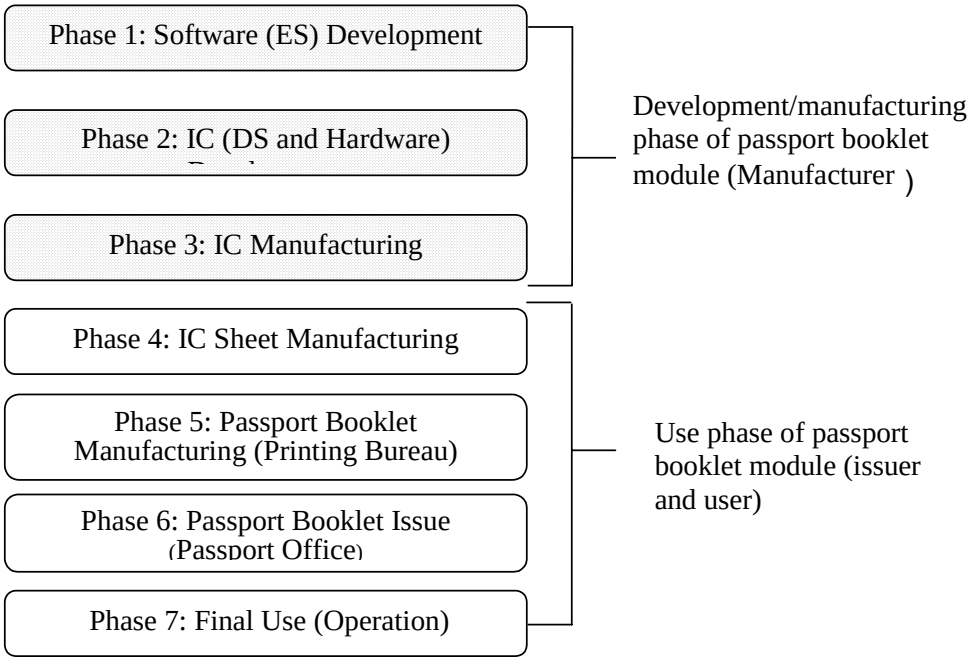

Figure 1: Lifecycle of the passport booklet

[9] This Protection Profile is not CC-certified.

The TOE is delivered in module form. This means that it is delivered at the end of phase 3, therefore the relevant phases of the lifecycle model for this TOE are Phases 1, 2, and 3. Phases 2, 3 were covered by the hardware evaluation with the certification-ID BSI-DSZ-CC-0245-2005.

The IT product Sharp passport booklet module, Version 1.1 was evaluated by brightsight® BV[6]. The evaluation was completed on 28 August 2006. brightsight® BV is an evaluation facility (ITSEF)[10] recognised by BSI.

The sponsor, vendor and distributor is

Sharp Corporation
2613-1 Ichinomoto-cho
Tenri, Nara
Japan

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented with AVA_VLA.4). The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: AVA_VLA.4	Highly Resistant

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic key generation
FDP	**User data protection**

[10] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_SDI.1	Stored data integrity monitoring
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT	**Security Management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security Functions**
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

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

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.2.

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

TOE Security Function	Addressed issue
SF.Sec_Messaging	Cryptographic operation by secure messaging The TOE protects the communication with end-users and controls access using secure messaging with Triple-DES cryptography according to the specifications in [10].
SF.Sec_Stat_Key	Data protection by cryptographic key

TOE Security Function	Addressed issue
	The TOE performs authentication by SF.Mutual_Auth and maintains the result of this authentication in the security status. This security status is used for access control. The TOE is constructed such that on startup the maintained security statuses express that no successful authentication (by SF.Verify) has been performed.
SF.Sec_Stat_PIN	Data protection by personal identification number The TOE performs authentication by SF.Verify and maintains the result of authentication in the security status. This security status is used for access control. The TOE is constructed such that on startup the maintained security statuses express that no successful authentication (by SF.Verify) has been performed.
SF.Access_Con	Access control The TOE permits access to the user data only when the present security status matches the access control conditions for the user data.
SF.Stores	Security attributes of data The TOE stores security attributes for each ISO7816 DF and EF that stores user data or authentication data. SF.Stores allows access (read-only due to pre-loaded initial data, see below) to these security attributes. The TOE has pre-loaded initial data that determines its access control.
SF.Construction	Security structure The TOE is securely constructed. This SF covers security functionality of the hardware platform that protects against tampering.
SF.Verify	Administrator identification and authentication The TOE identifies the administrator by use of the VERIFY command. The TOE authenticates the administrator by successful use of the VERIFY command. The number of consecutive failed authentication attempts is limited.
SF.Mutual_Auth	Mutual authentication The TOE identifies the end-user by use of the MUTUAL AUTHENTICATE command. The TOE authenticates the end-user by successful use of the MUTUAL AUTHENTICATE command (according the specifications in [10]).
SF.Integrity_Check	Safety check The TOE functionality that allows for reading stored user data includes integrity checking of the data.
SF.Protection	Prevention of bypassing including self protection The TOE mediates all requests from the administrator and end-user, and maintains a security domain for itself protected from logical and physical tampering.
SF.Key_Destruction	Invalidation of cryptographic keys

TOE Security Function	Addressed issue
	The TOE invalidates cryptographic session keys in the following situations: • When a subsequent MUTUAL AUTHENTICATE command is started by invalidating the session key validity flag. • When an abnormality is detected during processing of a secured message by invalidating the session key validity flag. • On power-up by overwriting all RAM.

Table 3: Security Functions of the TOE

For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed 'high' (SOF-high) for specific functions as indicated in the Security Target [6, chapter 6.2].

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.

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

The assets to be protected by the TOE are the user data as follows:

- Personal information like face image, name, etc.
- Passport information like passport number, hash values, digital signatures, etc.

Though the user data stored in the TOE is not secret, unauthorized access to it should not be possible. Thus, the assets are exposed to the following the threats of the user environment:

- Reading the user data without permission via the contactless interface
- Tampering physical parts of the TOE to forge a passport booklet

Apart from countering the threats, the security functionality of the TOE comply with the following organisational security policies:

- Maintenance of the integrity of the IC serial number
- Performance of mutual authentication with a terminal device
- Invalidation of transport keys if an error counter exceeds a defined threshold.

1.5 Special configuration requirements

The TOE can only be operated in a one dedicated configuration that is described in the user guidance and set by the passport booklet issuer. Thus, no special configuration requirements exist for the TOE.

1.6 Assumptions about the operating environment

To provide the security features being part of this evaluation, the following assumptions must be taken in account:

- The Printing Bureau and passport offices issue the passport in a secure manner. Furthermore, physical attacks are not possible in these sites.
- The delivery process from the developer to the user site is protected against physical attacks.
- The end user will prevent eavesdropping to the communication with the TOE before Secure Messaging is successfully established based on the authentication protocol supported by the module.

1.7 Disclaimers

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Sharp passport booklet module, Version 1.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SM4128(V3) module (see the report of the certification procedure BSI-CC-0245-2006)	A5 step or A7 step	packaged module
2	SW	BootROM (including DRNG function)	1.1.0	Software incorporated in the IC
3	SW	APE (the Operating System)	1.100	Software incorporated in the IC

No	Type	Identifier	Release	Form of Delivery
4	SW	ePassJP (the application implementing the E-passport functions)	1.0	Software incorporated in the IC
5	DOC	Outline of the manufacture process command of eP-APE	1.2.0	Printed Version or PDF
6	DOC	SHARP e-Passport Module Users Manual	1.01	Printed Version or PDF
7	DOC	Sharp Passport Booklet User guidance	1.0	Printed Version or PDF

Table 4: Deliverables of the TOE

Regarding the delivery process, the handling of the PINs required by the different authorities for the initialisation and personalisation is crucial for a secure operation. The evaluation examined the procedures applied and confirms that the confidentiality and integrity of this data is adequately protected. The physical delivery of the TOE is conducted by trusted courier services with prior information of the receiving authority.

The version of the TOE and the manufactured year/month information is included in the serial number. Thus, the user can identify the TOE by checking the serial number printed on the passport booklet module.

3 Security Policy

According to the security policy model that is contained in the Security Target [6] and supports the directives specified in [10], the TOE complies with the following security policies:

- ePassPort Policy:

  This policy requires the TOE to grant access to specific data objects only after a successful authentication with the corresponding keys. These keys are generated externally and an appropriate handling in the environment of the TOE is assumed.

- Secure Communication Policy:

  This policy arranges the security measures that are applied to assure the confidentiality of the user data during the communication. The algorithm for the session keys, requirements for the establishment of a session and the behaviour of the TOE after the end of a session are subject of the corresponding rule set.

- User Policy:

  The user policy defines the various users of the TOE and how they identify. Especially the commands that are allowed without prior identification and

authentication and the error counter are part of this policy and thus supported by the TOE.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

It is assumed that physical attacks in the Printing Bureau and the passport offices are not possible. Thus, sites where access to the user data is a legal obligation are assumed to constitute a secure environment.

To guarantee a secure distribution of the TOE the Security Targets contains the assumption that the Printing Bureau and the passport offices issue the passport booklets in a secure manner.

Furthermore, it is assumed that the TOE will be delivered to the user in a secure manner. This includes all delivery procedures from the personalisation instance to the end user, and especially the delivery to the National Printing Bureau.

4.2 Environmental assumptions

The end user will prevent eavesdropping to the communication with the TOE before Secure Messaging is successfully established based on the authentication protocol supported by the module.

5 Architectural Information

The following figure provides an overview of the TOE architecture as provided by the evaluator in the evaluation technical report [8]:

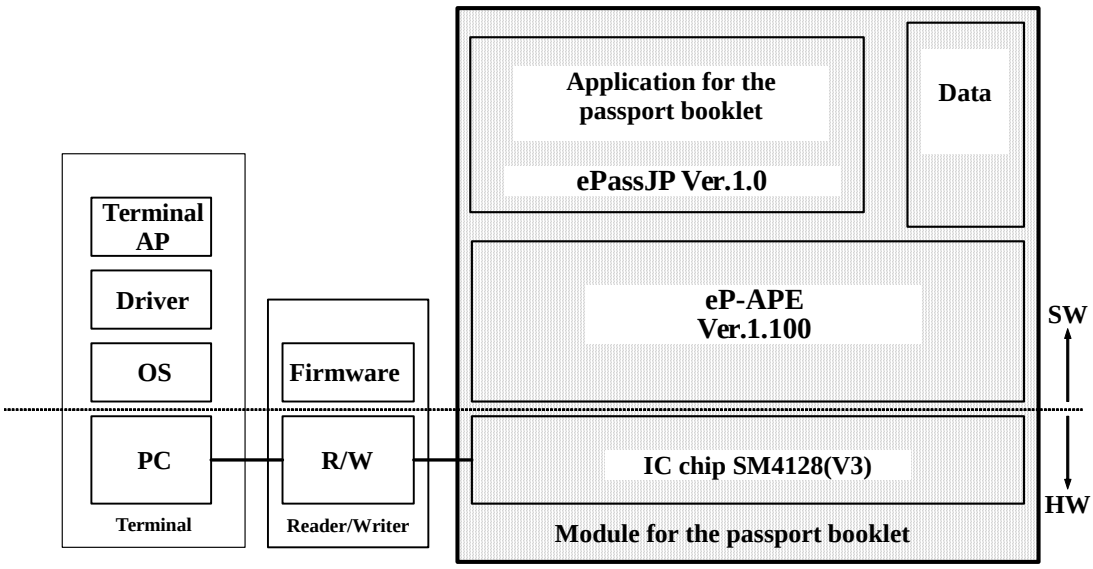

Figure 2: The TOE in its environment

Figure 2 (right side) shows the TOE composition of hardware (SM4128(V3) module), operating system (eP-APE) and e-passport application (ePassJP). On the left side of Figure 2 the context of the TOE is indicated by a card reader. This reader is typically at a border control station.

The basic function of the TOE is as follows:

- Function of selecting file which stores data
- Function of reading data
- Function of writing data
- Enforcing access control rules on the access to data, including use of secure messaging

The hardware supports the software by providing separation between applications, and between applications and operating system. The hardware also provides protection against physical attacks. Note that the software does not require the hardware to provide protection of the Triple-DES keys used in the secure messaging, as these keys are derived from data printed on the passport booklet itself, and therefore do not need to be protected against side channel attacks that require physical access to the booklet module.

6 Documentation

The developer provides the following documentation for secure usage of the TOE in accordance with the Security Target:

- Sharp Corporation, SHARP e-Passport Module Users Manual, version 1.01, December 15, 2005
- Sharp Corporation, Sharp Passport Booklet User guidance, version 1.0, February 20, 2006

7 IT Product Testing

7.1 Developer Testing

The procedure manual for the ePassport application describes two types of tests; the module tests that use a simulator and functional testing using a test rig and scripts. The test specification for the APE (Operation System) describes the tests for the TOE ePassport Operation System.

The developer test effort is designed to show the correct operation of the Japanese e-Passport security functionality. Every security function that is defined in the functional specification and every subsystem that is defined in the high level design has at least one test attributed to it. Thus, testing is performed in sufficient depths and coverage to meet the requirements of the chosen evaluation assurance level EAL4+.

The overall developer results show that the obtained results are consistant with the expected results.

7.2 Independent Testing

The following test configuration of the TOE was used for all independent tests:

- E-Passport Booklet module version 1.1 (TOE)
- Application for the Passport Booklet ePassJ version 1.1 (the application implementing the E-passport functions)
- Operating System version 2.506
- Hardware platform: SM4128 (V3)

Furthermore, the TOE is tested in the following modes:

- Issuer mode, i.e. the mode in which the TOE is after delivery of the factory.
- Personalised, i.e. the mode in which the TOE is after issue to the user.

According to the requirements of the Common Criteria, the evaluator performed different tests independently for the subsystems that were defined in the high level design and thus for the security function that were listed in the functional specification.

The overall conclusion is that the evaluator testing showed that the security functions perform as expected.

7.3 Penetration Testing

The evaluator assessed the developer vulnerability analysis and examined all other evaluation evidence to determine whether there are vulnerabilities not addressed in the developer vulnerability analysis.

The evaluators devised a test plan and conducted additional independent perantration tests. All test results were as expected. Thus, no security functional requirement was violated.

The conclusion is that the TOE is resistant against attackers with a high attack potential.

8 Evaluated Configuration

The TOE is identified by Sharp passport booklet module, Version 1.1. There is only one evaluated configuration of the TOE. All information of how to use the TOE and its security functions by the software is provided within the user documentation.

The TOE has two different operating modes, the issuer mode and the personalized mode. In the issuer mode all commands can be executed, whereas the personalized mode only allows a read-only access to the TOE data. Both modes and the irreversible transition between them were subject to the evaluation.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

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

For smart card IC specific methodology the CC supporting documents

(i) Functionality classes and evaluation methodology for deterministic random number generators

(ii) Application of CC to ICs

(iii) Application of Attack Potential to ICs

(iv) Functionality classes and evaluation methodology for true (physical) random number generators

(v) Guidance for Smartcard Evaluation

(see [4, AIS 20, AIS 25, AIS 26, AIS 31, AIS 37]) were used.

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

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented with AVA_VLA.4 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
I Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS

Assurance classes and components		Verdict
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented with AVA_VLA.4.
- The following TOE Security Functions fulfil the claimed Strength of Function: SF.Verify, SF.Mutual_Auth

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

(i) for the TOE Security Function SF.Sec_Messaging and

(ii) for other usage of encryption and decryption within the TOE.

For specific evaluation results regarding the development and production environment see annex A in part D of this report.

The results of the evaluation are only applicable to the Sharp passport booklet module, Version 1.1.

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

10 Comments/Recommendations

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

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CPLD	Complex Programmable Logic Device
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

[6] Security Target BSI-DSZ-CC-0355-2006, Version 1.13, August 25, 2006, SHARP Passport Booklet Module Security Target, Sharp Corporation (confidential document)

[7] Security Target BSI-DSZ-CC-0355-2006, Version 1.13, August 25, 2006, SHARP Passport Booklet Module Security Target, Sharp Corporation (public document)

[8] Evaluation Technical Report, Version 3.0, 30 August, 2006, Evaluation Technical Report SHARP Passport Booklet module Ver. 1.1 – EAL4+ (confidential document)

[9] Sharp Corporation, LSI for the SM4128(V3) IC card Security Target, SHARP Corporation - Integrated Circuits Group, version 1.8.5, 29 March 2005 - IC Group

[10] ICAO, PKI for Machine Readable Travel Documents offering ICC read-only access, ICAO-NTWG, version V1.1, October 01, 2004

[11] SHARP e-Passport Module Users Manual, Sharp Corporation, Version 1.01, December 15, 2005

[12] Sharp Passport Booklet User guidance, Sharp Corporation, Version 1.0, February 20, 2006

[13] Passport booklet IC Protection Profile, Japanese government, Version 1.0, 24 September, 2004

[14] Common Criteria Protection Profile, Machine Readable Travel Documents with “ICAO Application”, Extended Access Control (BSI-PP-0026) .

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0355-2006

Evaluation results regarding development and production environment

The IT product Sharp passport booklet module, Version 1.1 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005), extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 29. September 2006, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

(a) Sharp Makuhari, 1-9-2, NAKASE, MIHAMA-KU, CHIBA-SHI, CHIBA 261-8520, Japan

(b) Sharp Tenri, 2631-1, ICHINOMOTO-CHO, TENRI-SHI, NARA 632-8567, Japan

(c) Toppan Printing Co. Ltd., 1101-20, MYOHOJI-CHO, YOHKAICHI-SHI, SHIGA 527-8566, Japan

(d) Sharp Fukuyama, 1, ASAHI, DAIMON-CHO, FUKUYAMA-SHI, HIROSHIMA 721-8522, Japan

(e) Sharp Takaya Electronic Industry Co. Ltd., 3121-1, SATOMI, SATOSHO-CHO, ASAKUCHI-GUN, OKAYAMA 719-0301, Japan

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target (Security Target BSI-DSZ-CC-0355-2006, Version 1.13, August 25, 2006, SHARP Passport Booklet Module Security Target).

The evaluators verified, that the requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.