Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0790-2013

for

MorphoSmart Optic 301, Version 1.0

from

Safran Morpho

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-0790-2013

Fingerprint Spoof Detection System

MorphoSmart Optic 301
Version 1.0

from	Safran Morpho
PP Conformance:	Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant Assurance package as defined in the PP: ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2

Common Criteria Recognition Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the 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, 31 January 2013

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

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 September 2011 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: 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 by the nations listed above.

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 MorphoSmart Optic 301, Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product MorphoSmart Optic 301, Version 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 31 January 2013. 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: Safran Morpho.

The product was developed by: Safran Morpho.

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

[6] Information Technology Security Evaluation Facility

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, as specified in the following report and in the Security Target.

For the meaning of the assurance levels 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5 Publication

The product MorphoSmart Optic 301, Version 1.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://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] Safran Morpho
11 boulevard Galliéni
92130 ISSY LES MOULINEAUX
France

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 the MorphoSmart Optic (MSO) 301, Version 1.0.

The MorphoSmart Optic (MSO) 301, Version 1.0 is a high end fingerprint optical scanner, offering a large capture surface. It covers a wide range of applications: enrollment, authentication and identification (using an internal database capable to store up to 5000 users) in industrial/commercial and governmental environments. It integrates a patented technology from Morpho which enables the detection of fake fingers.

The TOE is a system that provides fingerprint spoof detection as part of a biometric system for fingerprint recognition. The TOE has a hardware part which is the capture device and a software part which is the spoof detection module. The TOE determines whether a fingerprint presented to the biometric system is genuine or spoofed.

For this purpose the spoof detection system acquires spoofing evidences for a presented fingerprint using sensors. These sensors are part of the capture device that is used to capture the biometric sample of the fingerprint.

The fingerprint spoof detection forms the main security functionality covered by the certification. Beside the fingerprint spoof detection functionality, the TOE implements management functionality to modify security relevant parameters, audit functionality for security relevant events and protection of residual and security relevant data. Biometric verification is out of scope of the certification.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010 [7].

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 ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2 as defined in the claimed Protection Profile.

The TOE security functional requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [17], chapter 6.1 to 6.4. They are selected from Common Criteria Part 2 and one of them is newly defined. Thus the TOE is CC Part 2 extended.

The TOE security functional requirements are implemented by the following TOE security functions:

TOE security functions	Addressed issue
TSF_FFD - Fake Finger Detection	Detection of spoofed fingerprints and secure deletion of sensitive information
TSF_MANAGEMENT – Security Management	Sending an individual security level value to the TSF_FFD for each use of the TSF_FFD and checking if the value is in the accepted range
TSF_AUDIT – Security Audit Generation	Generation of audit records for every use of the security functions

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [17], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [17], chapter 3.2. Based on these assets the TOE security problem is defined in terms of assumptions and organisational security policies. This is outlined in the Security Target [6] and [17], chapter 3.3 and 3.5.

This certification covers the following configuration of the TOE:

The only valid version of the TOE is MorphoSmart Optic (MSO) 301, Version 1.0 and firmware version 11.00.m-c.

The administrator of the TOE has to pass a value for the parameter “Security Level” with each command (enrol, verify, identify, modify user data fields, enrole OTP user, generate OTP) where the spoof detection meachnism is used. The only valid value of the parameter “Security Level” in the certified configuration is “High”.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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:

MorphoSmart Optic 301, Version 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	MorphoSmart Optic (MSO) 301 (including firmware version 11.00.m-c)	Version 1.0	HW
2	DOC	MSO 301– GUIDES [13]	Version 12 2012-09-18	Printed document
3	DOC	MorphoSmart Programmer’s Guide [14]	for Version 6.3 of the MorphoSmart SDK 2012-02	Printed document
4	DOC	MorphoSmart Host System Interface [15]	Version 3.3 2011-09	Printed document
5	DOC	Morpho Biometric Terminals Finger Positioning Recommendations [16]	Version 1 2011-04	Printed document

Table 2: Deliverables of the TOE

The delivery content is described in a release sheet which is send to the customer with seperate post. If the delivery content is not exactly what is described in this sheet, the administrator must contact Safran Morpho (refer to [13] §7.3).

During the power on, the MSO 301 checks its firmware and hardware parts. If any error occurs, the MSO will switch to the ”End of life” mode (refer to paragraph [13] §6.2).

The command ILV_SECU_GET_CONFIG (refer to [13] §5.1.4.8) provides the MSO serial number. The administrator must check that the serial number of the received MSO 301 is the same than the serial number in the associated release sheet. If serial numbers are different, the administrator must contact Safran Morpho (refer to [13] 7.3).

To get the TOE version, the administrator has to send the command ILV_GET_DESCRIPTOR with the following input parameter: ID_FORMAT_BIN_VERSION. This command is described in [15], chapter ILV Commands Description.

The firmware version must be 11.00.m-c.

The TOE identifier associated to this firmware version is: MorphoSmart Optic 301, Version 1.0.

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

- Spoof detection: The TOE shall be able to detect whether a presented fingerprint is spoofed or genuine.
- Residual Information Protection: The TOE shall ensure that no residual or unprotected security relevant data remain in memory after operations are completed.
- Security management: The TOE shall provide the necessary management functionality for the modification of security relevant parameters for TOE administrators. Only secure values shall be used for such parameters.
- Security audit: The TOE shall record security-relevant events.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of 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: Well trained and non hostile administrators, physical protection against unauthorized access or modification, secure TOE platform providing necessary services (i.e. administrator identification and authentication, access control, secure communication, secure storage and review of audit information, reliable time stamps and protection against malware) and the biometric verification mechanism that is protected by the security functionality of the TOE. Details can be found in the Security Target [6] and [17], chapter 4.2.

5 Architectural Information

The TOE consists of the following subsystems:
Camera and APIs, Electrodes and APIs, Audit, Security, Acquisition, Fake Finger Detection, MSO Services and Biometric System.

The Camera and APIs subsystem comprises the camera used to capture the finger image and its associated APIs to use it.

The Electrodes and APIs subsystem comprises the electrodes used to check the finger impedance and their associated APIs to use them.

The Audit subsystem is responsible for managing the audit functionality of the TOE, i.e. the creation of the log.

The Security subsystem ensures that there is no residual information in the TOE.

The Acquisition subsystem retrieves the image from the Camera and API subsystem. Furthermore, it is responsible for checking that something is present on the sensor and is stable.

The Fake Finger Detection subsystem analyzes the finger impedance captured by the Electrodes and APIs subsystem. It decides whether the presented pingerprint is spoofed or genuine.

The MSO Services subsystem represents a software layer to use the USB service protocol of the MSO 301 device.

The Biometric System subsystem accomplishes the matching process which is not part of the certified functionality.

All subsystems have been declared as SFR-enforcing subsystems, except MSO Services which is declared as SFR-supporting and Biometric System which is declared as SFR-non-interfering.

6 Documentation

The evaluated documentation 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

7.1 TOE Test Configuration

All developer’s and evaluator's tests in the context of the evaluation have been conducted using the final version of the TOE (version 1.0). Regardless of whether manual or automatic tests were performed, the following software configuration in the TOE environment was in place:

- Operating System: Windows 7, 32 Bit
- SDK: SDK MSO 6.3.1.0

The developer used the following hardware for automated and manual testing :

- Intel® Core 2 Duo CPU 2.93 GHz 3.50 GB of RAM with USB port

The hardware satisfies the requirements made by the ST and the guidance documentation.

7.2 Functional Developer Testing

Testing Approach

The developer used the following test tools and materials for different aspects of the testing activities. The following list gives an overview about the used tools and their purpose or field of application:

- MSO_Demo: Tool for the testing of SDK functionality / implicit testing of TOE functionality
- ILV_Scripter: Tool for testing the interface E.API
- Fake materials (Playdoh, latex, Window Color, white silicon, transparent silicon, candle wax, white glue, gelatine, foil, photocopy, wood glue, Micro Krystal Klear, potato): The materials were used to create fake fingers to test the spoof detection functionality of the TOE.

A test case conducted with the first two test tools thereby consists of several test steps which are executed sequentially and which results are compared to the expected results. Only if all checks of all test steps are successful, the corresponding test case passes.

The testing of the spoof detection functionality (according to FPT_SPOD.1) was conducted by creating fake fingers from different materials (see list above). In total, the developer created 142 fakes and applied each fake 10 times to the TOE.

All in all, the developer tested the TOE systematically at the level of TSFI as given in the functional specification. The developer thereby followed the strategy to cover all TSFI.

Test results

The developer's testing effort has been proven sufficient to demonstrate that the TOE security functions perform as specified.

The spoof detection test results showed that no fake finger was detected as a real finger in each attempt.

Overall the TSF have been tested systematically against the Security Target and the functional specification. The tests results demonstrate that no discrepancy between the TOE behaviour and the TOE specification has been found.

7.3 Independant Evaluator Testing

Testing approach

The evaluator repeated 2 manual and 8 automatic developer tests in order to verify the adequateness of the tests using the different test tools MSO_DEMO and ILV_SCRIPTER used by the developer.

The evaluator further developed a set of own manual test cases for functional testing. Thereby he had chosen the approach to cover TSF from all the functional areas of the TOE (spoof detection, audit and management). This approach extends the one used for the developer tests. Full TSFI coverage is provided in both approaches since all TSFI are relevant for all test cases. The evaluator devised and performed 2 functional tests and 2 other tests.

For fake testing the evaluator created 51 fakes of various materials. The evaluator carried out 535 attempts to spoof the TOE with these fakes.

All TSFI (E.CAMERA, E.ELECTRODES, E.API) were used for testing of SFR-relevant behavior during evaluation body testing.

Test results

The spoof detection test results showed that no fake finger was detected as a real finger in each attempt.

The overall judgment on the results of independent testing consisting of developer test repetition (sampling), TSF subset and TSFI testing and other testing is that the TOE security functionality and TSFI are successfully tested and actually have the effects as specified.

8 Evaluated Configuration

This certification covers the following configuration of the TOE:

The only valid version of the TOE is MorphoSmart Optic (MSO) 301 in Version 1.0 and the firmware version 11.00.m-c.

The administrator of the TOE has to pass a value for the parameter "Security Level" with each command (enrol, verify, identify, modify user data fields, enrole OTP user, generate OTP) where the spoof detection meachnism is used. The only valid value of the parameter "Security Level" in the certified configuration is "High".

9 Results of the Evaluation

9.1 CC specific results

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.

The following guidance specific for the technology was used:

(i) Fingerprint Spoof Detection Evaluation Guidance (FSDEG) [9]

(ii) Finger Fake Toolbox for Common Criteria evaluations – Developer Overview [10]

(iii) TÜViT Toolbox documentation [11]

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

- The components ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2
  as defined in the claimed Protection Profile for this TOE certification and defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance:
  Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010 [10]
- for the Functionality:
  PP conformant
  Common Criteria Part 2 extended
- for the Assurance:
  Common Criteria Part 3 conformant
  Assurance package as defined in the PP:
  ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2

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 TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The 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 all aspects of assumptions and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

11 Security Target

For the purpose of publishing, the Security Target [17] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSDEG	Fingerprint Spoof Detection Evaluation Guidance
FSDPP_OSP	Fingerprint Spoof Detection Protection Profile based on OSPs
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MSO	MorphoSmart Optic
OTP	One Time Password
PP	Protection Profile
SAR	Security Assurance Requirement
SDK	Software Development Kid
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

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

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

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

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

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

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

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

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[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), periodically updated list published also in the BSI Website

[6] Security Target, Version 8, 12 September 2012, MorphoSmart Optic 301 Security Target, Safran Morpho (confidential document)

[7] Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010

[8] Evaluation Technical Report, Version 6, 21 January 2013, TÜV Informationstechnik GmbH, (confidential document)

[9] Fingerprint Spoof Detection Evaluation Guidance (FSDEG), Version 2.1, 18 December 2009, Federal Office for Information Security

[10] Finger Fake Toolbox for Common Criteria evaluations – Developer Overview, Version 1.0, 14 September 2011, Federal Office for Information Security

[11] TÜViT Toolbox documentation, Version 0.7, May 2012, TÜV Informationstechnik GmbH

[12] Configuration list for the TOE, Version 10, 19 September 2012, MorphoSmart Optic 301 – Life Cycle Support (ALC) (chapter 2.1), Safran Morpho (confidential document)

[13] MSO 301– GUIDES, Version 12, 18 September 2012, Safran Morpho

[14] MorphoSmart Programmer's Guide for Version 6.3 of the MorphoSmart SDK, February 2012, Safran Morpho

[15] MorphoSmart Host System Interface, Version 3.3, September 2011, Safran Morpho

[16] Morpho Biometric Terminals Finger Positioning Recommendations, Version 1, April 2011, Safran Morpho

[17] Security Target, Version 1, 18 January 2013, MorphoSmart Optic 301 Public Security Target, Safran Morpho (sanitised public document)

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

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

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

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

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

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

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

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

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

Table 1: Evaluation assurance level summary”

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

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

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

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.