



# Certification Report

**BSI-DSZ-CC-0498-2009**

for

**SOMA\_80IFX  
Version 1.1.0**

from

**Gep S.p.A.**

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



# Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

## BSI-DSZ-CC-0498-2009

Security IC chip with ePassport Application

**SOMA\_80IFX**

Version 1.1.0

from Gep S.p.A.

PP Conformance: Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control Version 1.0, BSI-PP-0017-2005

Functionality: PP conformant; Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant  
EAL 4 augmented by  
ADV\_IMP.2 and ALC\_DVS.2



Common Criteria  
Recognition  
Arrangement  
for components up to  
EAL 4



The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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

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

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

Bonn, 16 November 2009

For the Federal Office for Information Security



SOGIS - MRA

Bernd Kowalski  
Head of Department/ Division

L.S.

This page is intentionally left blank.

## Preliminary Remarks

Under the BSIG<sup>1</sup> 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.

---

<sup>1</sup> Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

# Contents

- A Certification.....7
  - 1 Specifications of the Certification Procedure.....7
  - 2 Recognition Agreements.....7
    - 2.1 European Recognition of ITSEC/CC - Certificates.....8
    - 2.2 International Recognition of CC - Certificates.....8
  - 3 Performance of Evaluation and Certification.....8
  - 4 Validity of the certification result.....9
  - 5 Publication.....9
- B Certification Results.....11
  - 1 Executive Summary.....12
  - 2 Identification of the TOE.....13
  - 3 Security Policy.....14
  - 4 Assumptions and Clarification of Scope.....14
  - 5 Architectural Information.....15
  - 6 Documentation.....15
  - 7 IT Product Testing.....15
    - 7.1 Developer's Test according to ATE\_FUN .....15
    - 7.2 Evaluator Tests according to ATE\_IND .....16
    - 7.3 Penetration Testing according to AVA\_VLA .....17
  - 8 Evaluated Configuration.....18
  - 9 Results of the Evaluation.....18
    - 9.1 CC specific results.....18
    - 9.2 Results of cryptographic assessment.....19
  - 10 Obligations and notes for the usage of the TOE.....19
  - 11 Security Target.....19
  - 12 Definitions.....20
    - 12.1 Acronyms.....20
    - 12.2 Glossary.....20
  - 13 Bibliography.....22
- C Excerpts from the Criteria.....25
- D Annexes.....33

## A Certification

### 1 Specifications of the Certification Procedure

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

- BSIG<sup>2</sup>
- BSI Certification Ordinance<sup>3</sup>
- BSI Schedule of Costs<sup>4</sup>
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)<sup>5</sup> [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

### 2 Recognition Agreements

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

---

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

<sup>3</sup> 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

<sup>4</sup> 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

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

## 2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

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

## 2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 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 web site: <http://www.commoncriteriaportal.org>

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

This evaluation contains the components ADV\_IMP.2 and ALC\_DVS.2 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

## 3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SOMA\_80IFX Version 1.1.0 has undergone the certification procedure at BSI.

The evaluation of the product SOMA\_80IFX Version 1.1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21. July 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)<sup>6</sup> recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Gep S.p.A.

The product was developed by: Gep S.p.A.

---

<sup>6</sup> Information Technology Security Evaluation Facility



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

## 4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

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

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

## 5 Publication

The product SOMA\_80IFX, Version 1.1.0 has been included in the BSI list of the 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<sup>7</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

<sup>7</sup> Gep S.p.A.  
Corso S. D'Amato n° 90  
Edificio "U"  
80022 Arzano (NA)  
Italy

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 SOMA\_80IFX e-Passport version 1.1.0. The SOMA\_80IFX is utilized by Machine Readable Travel Documents (MRTD) based on the requirements and recommendations of the international Civil Aviation Organisation (ICAO). The TOE provides the Basic Access Control according to the Technical Report: PKI for MRTD offering ICC-Read only Access [11] and is supplied with a file system that contains all the data that are used in the context of the ICAO application as described in the Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control [10].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control Version 1.0, BSI-PP-0017-2005 [10].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 7.3.

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

TOE Security Function	Addressed issue
SF1	Agents Identification and Authentication
SF2	Data exchange with Secure Messaging
SF3	Access Control of stored Data Objects
SF4	Life cycle management
SF5	Software integrity check of TOE's assets
SF6	Security functions provided by the hardware

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 8.2.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 8.2 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 4.

This certification covers the following configurations of the TOE:

SOMA\_80IFX 1.1.0 consisting of:

- IFX Chip SLE66CLX800PE,
- embedded software operation system SOMA\_80IFX 1.1.0,
- a file system in the context of the ICAO application.

After delivery the TOE only features one fixed configuration, which cannot be altered by the user/administrator.

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:

### **SOMA\_80IFX Version 1.1.0**

The TOE consists of an integrated circuit inserted between two paper sheets, which also embed an antenna for wireless communication. The resulting sandwich is called “inlay” and can be bound to the cover of a passport booklet.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW + SW	TOE: SOMA_80IFX, consisting of: <ul style="list-style-type: none"> <li>• SW: SOMA_80IFX OS</li> <li>• HW: SLE66CLX800PE</li> </ul>	1.1.0	Software contained in the chip, chip mounted into an inlay package and initialised.
2	DOC	SOMA_80IFX e-Passport User Guidance	1.1.1	Document in electronic form as PDF
3	DOC	SOMA_80IFX e-Passport Administrator Guide	1.1.1	Document in electronic form as PDF

Table 2: Deliverables of the TOE

The TOE is delivered after the initialisation. The following items are shipped to the Personalisation Agent:

- fully-functional and already initialized, but not operational SOMA\_80IFX inlays
- The master key required to derive the Personalization Keys at runtime.
- Secure Access Module (SAM, if used for the delivery of the master key)
- SAM activation codes (SAC, if a SAM is used to deliver the master key)
- The Administrator Guidance
- The User Guidance

The master key is delivered according to Customer’s requirements. The use of a Secure Access Module (SAM) is a possible solution. The SAM is a smart card and during

the delivery the Personalization Keys generation is disabled and a SAM Activation Code (SAC) must be used to enable that functionality.

Inlays, SAMs (if used) and CD-ROMs are shipped separately by means of a courier trusted by Gep. The SAM Activation Codes (if required) are delivered to the Personalisation Agent by means of PGP enciphered e-mail messages.

The TOE identification data (SOMA\_80IFX 1.1.0) is located in the non-volatile memory of the chip and can be read by means of the administrative command GET DATA. The TOE is uniquely identified by a string of bytes as follows:

- OS identifier: 53h 4Fh 4Dh 41h
- IC identifier: 38h 30h 49h 46h 58h
- OS version: 31h 2Eh 31h 2Eh 30h

### 3 Security Policy

The security policy of the TOE is defined according to the MRTD BAC PP [10] by the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). It addresses the advanced security methods Basic Access Control in the technical reports of the ICAO New Technology Working Group.

### 4 Assumptions and Clarification of Scope

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

Development and Manufacturing Environment

- Assurance Security Measures in Development and Manufacturing Environment
- Control over MRTD Material

Issuing State or Organization

- Personalization of logical MRTD
- Authentication of logical MRTD by Signature
- Administration of logical MRTD

Receiving State or Organization

- Examination of the MRTD passport book
- Verification by Passive Authentication
- Protection of data of the logical MRTD

MRTD Holder

- Secure Handling of the MRTD holder

Details can be found in the Security Target [6] and [9] chapter 5.2.

## 5 Architectural Information

The architecture of the Operating System embedded in the chip and the OS has been designed following a layered approach. In a bottom to top view, i.e. from the physical layer to the applicative layer, following layers are defined:

- Layer 1: HL - Hardware Layer  
The HL is the hardware chip. The interface to the HAL layer is constituted by the processor instructions set (ISA) and a specific library file supplied by the Infineon Technologies AG, i.e. the Resource Management System. It contains a set of subroutines for programming the integrated EEPROM along with others functions who offer a sophisticated interface to upper layer.
- Layer 2: HAL - Hardware Abstraction Layer  
The HAL is in charge to manage the functionality directly related with the chip-dependent hardware. Therefore it performs actions on the hardware and provides exposed services like APIs to the upper layer.
- Layer 3: DOL - Data Objects Layer  
The DOL attends to abstract the physical organization of the data structures (objects) stored in EEPROM memory area. It provides to the upper layer the services to manage the card objects and data stored within these.
- Layer 4: SSML - Security Services Management Layer  
This layer provides additional services necessary to support card applicative features which are the security status of the card, authentication objects (i.e. keys), the security environment and the secure messaging.
- Layer 5: CML - Command Management Layer  
The most external layer offers the externally visible interface by means of the APDU commands.

## 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 Developer's Test according to ATE\_FUN

The developer's testing effort is summarized in the following 4 aspects:

TOE configurations tested:

- The tests were performed with the composite smartcard product SOMA\_80IFX 1.1.0 consisting of the Infineon Chip SLE66CLX800PE, operational system SOMA\_80IFX and a file system in the context of the ICAO application.

Developer's testing approach:

- The 5 testable TSF's and related sub-functions and subsystems are tested (if applicable) in Pre\_Personalisation, Personalisation, Operational and Terminated life cycle states.
- Test suites are implemented in accordance with the functional specification and the guidance documentation in order to verify the TOE's compliance with its expected behaviour.
- All test cases in each test suite were run successfully on this TOE version.

#### Amount of developer testing performed:

- The developer has tested all 5 testable TSF of the TOE within 67 test scenarios.
- As demonstrated by the test coverage analysis the developer has tested the TOE systematically at the level of TSF functionalities as given in the functional specification.
- As demonstrated by test depth analysis the developer has tested the TOE systematically at the level of the subsystems as given in the high level design.

#### Overall developer testing results:

- All testing strategies of the TSF passed all tests of each individual test scenario so that all testable TSF have been successfully tested against the functional specification and the high level design.
- The developer's testing results demonstrate that the TSF perform as specified.
- The developer's testing results demonstrate that the TOE performs as expected.

## **7.2 Evaluator Tests according to ATE\_IND**

#### TOE configurations tested:

- The tests were performed with the composite smartcard product SOMA\_80IFX 1.1.0 consisting of the Infineon Chip SLE66CLX800PE, operational system SOMA\_80IFX, and a file system in the context of the ICAO application.

#### Subset size chosen:

- The evaluators have tested all 5 testable TSF.

#### TSF subset selection criteria:

- The evaluators have chosen a subset of developer tests so that all testable TSF could be covered by at least one test case in order to confirm that the TOE operates as specified. Valid cases as well as invalid cases were considered.

#### Security functions tested:

- The evaluators have covered all 5 testable TSF: SF1, SF2, SF3, SF4, and SF5 within the independent testing.

#### Developer tests performed:

- The evaluators have selected and tested a sample of 12 test cases from the developer TSF tests.

#### Verdict for the activity:

- During the evaluator's TSF subset testing the TOE operated as specified.



- The evaluators have verified the developer's test results by executing a sample of tests in the developer's test documentation.

### 7.3 Penetration Testing according to AVA\_VLA

#### Developer VLA:

In the following the evaluator's penetration testing effort based on developer vulnerability analysis is summarised:

##### Testing approach:

- Examination of developer's vulnerability analysis in the intended environment of the TOE.

##### TOE test configurations:

- The tests were performed with the composite smartcard product SOMA\_80IFX 1.1.0 consisting of the Infineon Chip SLE66CLX800PE, operational system SOMA\_80IFX OS and a file system in the context of the ICAO application.

##### Amount of penetration testing performed:

- (2T)DES
- Vulnerability of Access Control
- TOE reliability
- Life Cycle Model

##### Security functions penetration tested:

- SF1, SF2, SF3, SF4, SF5

##### Verdict for the sub-activity:

- The evaluator has performed penetration testing based on the developer's vulnerability analysis.
- During the evaluator's penetration testing the TOE operated still as specified.
- All potential vulnerabilities are not exploitable with a low attack potential in the intended environment for the TOE.
- The TOE is resistant to attackers with low attack potential.

#### Evaluator VLA:

In the following the evaluator's penetration testing effort based on his independent vulnerability analysis is summarised:

##### Testing approach:

- Examination of evaluator's vulnerability analysis in the intended environment of the TOE.

##### TOE test configurations:

- The tests were performed with the composite smartcard product SOMA\_80IFX 1.1.0 consisting of the Infineon Chip SLE66CLX800PE, operational system SOMA\_80IFX 1.1.0 and a file system in the context of the ICAO application.

##### Amount of penetration testing performed:

- (2T)DES
- Vulnerability of Access Control
- TOE reliability
- Life Cycle Model
- Vulnerability of Secure Messaging und Access Control
- TOE reliability behaviour after interruptions

#### Security functions penetration tested:

- SF1, SF2, SF3, SF4, SF5

#### Verdict for the sub-activity:

- The evaluator has performed penetration testing based on the evaluator's vulnerability analysis.
- During the evaluator's penetration testing the TOE operated as specified.
- In the intended environment of use the TOE does not feature any exploitable vulnerabilities in the meaning of the security targets [ST] for typical attackers possessing a low attack potential, if all the measures required are taken into consideration.
- The TOE is resistant to attackers with low attack potential.

## **8 Evaluated Configuration**

The evaluated TOE is the SOMA\_80IFX 1.1.0 consisting of:

- IFX Chip SLE66CLX800PE,
- embedded software operation system SOMA\_80IFX 1.1.0,
- a file system in the context of the ICAO application. The TOE was tested in the evaluated configuration as described above.

## **9 Results of the Evaluation**

### **9.1 CC specific results**

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

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

The following guidance specific for the technology were used:

- Application Notes and Interpretation of the Scheme (AIS), AIS 25, Anwendung der CC auf integrierte Schaltungen, Version 5, 2009-05-07, Bundesamt für Sicherheit in der Informationstechnik [4],

- Application Notes and Interpretation of the Scheme (AIS), AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 6, 2009-05-07, Bundesamt für Sicherheit in der Informationstechnik [4].

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

- All components of the class ASE
- All components of the EAL4 package as defined in the CC (see also part C of this report)
- The components ADV\_IMP.2 and ALC\_DVS.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control Version 1.0, BSI-PP-0017-2005 [10]
- for the Functionality: PP conformant; Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant  
EAL 4 augmented by  
ADV\_IMP.2  
ALC\_DVS.2

The following TOE Security Functions fulfil the claimed Strength of Function : high

- SF1: Agents Identification and Authentication
- SF2: Data exchange with Secure Messaging
- SF6: Security functions provided by the hardware

In order to assess the Strength of Function the scheme interpretation AIS 31 (see [4]) was used.

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

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

## 9.2 Results of cryptographic assessment

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- SF2: Data exchange with Secure Messaging (Triple-DES, Retail MAC)

## 10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

## 11 Security Target

For the purpose of publishing, the Security Target [9] 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

<b>(2T)DES</b>	2-key Triple DES
<b>APDU</b>	Application Protocol Data Unit
<b>BAC</b>	Basic Access Control
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Errichtungsgesetz
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>DES</b>	Data Encryption Standard; symmetric block cipher algorithm
<b>EAL</b>	Evaluation Assurance Level
<b>EEPROM</b>	Electrically Erasable Programmable Read Only Memory
<b>ETR</b>	Evaluation Technical Report
<b>IC</b>	Integrated Circuit
<b>ICAO</b>	International Civil Aviation Organisation
<b>IT</b>	Information Technology
<b>ITSEF</b>	Information Technology Security Evaluation Facility
<b>MAC</b>	Message Authentication Code
<b>MRTD</b>	Machine Readable Travel Document
<b>PP</b>	Protection Profile
<b>ROM</b>	Read Only Memory
<b>SAC</b>	SAM activation codes
<b>SAM</b>	Secure Access Module
<b>SAR</b>	Security Assurance Requirement
<b>SF</b>	Security Function
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SOF</b>	Strength of Function
<b>ST</b>	Security Target

<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	TOE Security Policy

## 12.2 Glossary

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

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

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

**Informal** - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 13 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.<sup>8</sup>
- [5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website
- [6] Security Target BSI-DSZ-CC-0498, Version 1.6.2, dated 02/10/2008, Common Criteria Security Target for SOMA\_80IFX, Gep S.p.A. (confidential document)
- [7] Evaluation Technical Report BSI-DSZ-CC-0498 for SOMA\_80IFX 1.1.0, Version 1, Date: 2009-07-17, TÜV Informationstechnik GmbH (confidential document)
- [8] Configuration list for the TOE, Version 1.2, Date: 16.04.2009, Configuration Item List for SOMA\_80IFX (confidential document)
- [9] Security Target BSI-DSZ-CC-0498, Version 1.0.0, Date: 07/12/2009, Security Target SOMA\_80IFX Electronic Passport, Gep S.p.A. (sanitised public document)
- [10] Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.0, BSI-PP-0017, 18 August 2005, Bundesamt für Sicherheit in der Informationstechnik
- [11] Machine Readable Travel Documents – Technical Report: PKI for MRTD offering ICC-Read only Access, Version 1.1
- [12] ETR for composite evaluation according to AIS 36 for the Product SLE66CLXxxxPEx/m158x-e12 from Infineon Technologies AG, Version 2, Date 2008-08-21, TÜV Informationstechnik GmbH (confidential document)
- [13] Certification report BSI-DSZ-CC-0399-2009, for Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12,

<sup>8</sup> specifically

- AIS 25, Version 6, 07.09.2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 07.05.2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24.10.2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2, 12.11.2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document

SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12 and SLE66CLX360PES / m1589-e12 with specific IC Dedicated Software, Date: 29.01.2007, Bundesamt für Sicherheit in der Informationstechnik

- [14] SOMA\_80IFX e-Passport Administrator Guidance, Version 1.1.1, Date: 7.11.2008, Gep S.p.A.
- [15] SOMA\_80IFX e-Passport User Guidance, Version 1.1.1, Date: 7.11.2008, Gep S.p.A.



## C Excerpts from the Criteria

CC Part1:

### Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

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

plus one of the following:

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

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

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

CC Part 3:

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

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

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

Table 3 - Protection Profile families - CC extended requirements”

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

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

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

Table 5 - Security Target families - CC extended requirements ”

**Assurance categorisation** (chapter 7.5)

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

<b>Assurance Class</b>	<b>Assurance Family</b>
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 Evaluation Assurance Level Components							by
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	
Configuration management	ACM_AUT				1	1	2	2	
	ACM_CAP	1	2	3	4	4	5	5	
	ACM_SCP			1	2	3	3	3	
Delivery and operation	ADO_DEL		1	1	2	2	2	3	
	ADO_IGS	1	1	1	1	1	1	1	
Development	ADV_FSP	1	1	1	2	3	3	4	
	ADV_HLD		1	2	2	3	4	5	
	ADV_IMP				1	2	3	3	
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	
	ADV_RCR	1	1	1	1	2	2	3	
	ADV_SPM				1	3	3	3	
Guidance documents	AGD_ADM	1	1	1	1	1	1	1	
	AGD_USR	1	1	1	1	1	1	1	
Life cycle support	ALC_DVS			1	1	1	2	2	
	ALC_FLR								
	ALC_LCD				1	2	2	3	
	ALC_TAT				1	2	3	3	
Tests	ATE_COV		1	2	2	2	3	3	
	ATE_DPT			1	1	2	2	3	
	ATE_FUN		1	1	1	1	2	2	
	ATE_IND	1	2	2	2	2	2	3	
Vulnerability assessment	AVA_CCA					1	2	2	
	AVA_MSU			1	2	2	3	3	
	AVA_SOF		1	1	1	1	1	1	
	AVA_VLA		1	1	2	3	4	4	

Table 6: Evaluation assurance level summary”

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

## “Objectives

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

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

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 11.4)

## “Objectives

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

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

**Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 11.5)

## “Objectives

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

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

**Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed**  
(chapter 11.6)**“Objectives**

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

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

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested**  
(chapter 11.7)**“Objectives**

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

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

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested**  
(chapter 11.8)**“Objectives**

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

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

**Evaluation assurance level 7 (EAL7) - formally verified design and tested**  
(chapter 11.9)

## "Objectives

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

**Strength of TOE security functions (AVA\_SOF)** (chapter 19.3)

## "Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

**Vulnerability analysis (AVA\_VLA)** (chapter 19.4)

## "Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

## "Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA\_VLA.2 Independent vulnerability analysis), moderate (for AVA\_VLA.3 Moderately resistant) or high (for AVA\_VLA.4 Highly resistant) attack potential."



## **D Annexes**

### **List of annexes of this certification report**

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development  
and production environment

35

This page is intentionally left blank.

## Annex B of Certification Report BSI-DSZ-CC-0498-2009

### Evaluation results regarding development and production environment



The IT product SOMA\_80IFX, Version 1.1.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 16 November 2009, the following results regarding the development and production environment apply. The Common Criteria Security 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.2, ALC\_LCD.1, ALC\_TAT.1),

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

- (a) Gep S.p.A., Corso Salvatore D'Amato 90, 80022 Arzano (Naples), Italy (Gep Arzano, Development site and production site)
- (b) For development and productions sites regarding the Infineon chip SLE66CLX800PE refer to the certification report BSI-DSZ-CC-0399-2007 [13]

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.