

# eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA, embedded in the Infineon SLC52GDA Integrated Circuit

Common Criteria / ISO 15408  
Security Target – Public version  
EAL4+

# Table of content

|  |           |
|--|-----------|
| <b>1. REFERENCE DOCUMENTS</b>  | <b>4</b>  |
| 1.1 EXTERNAL REFERENCES [ER]   | 4         |
| 1.2 INTERNAL REFERENCES [IR]   | 4         |
| <b>2. ACRONYMS &amp; GLOSSARY</b>  | <b>5</b>  |
| 2.1 ACRONYMS   | 5         |
| 2.2 GLOSSARY   | 5         |
| <b>3. SECURITY TARGET INTRODUCTION</b>   | <b>7</b>  |
| 3.1 SECURITY TARGET IDENTIFICATION   | 7         |
| 3.2 TOE IDENTIFICATION   | 7         |
| 3.3 TOE OVERVIEW   | 7         |
| 3.4 TOE DESCRIPTION  | 8         |
| 3.4.1 TOE boundaries   | 8         |
| 3.4.2 TOE usage and security features for operational use                        | 8         |
| 3.4.3 TOE lifecycle  | 9         |
| 3.4.4 Non-TOE hardware/software/firmware required by the TOE                     | 12        |
| <b>4. CONFORMANCE CLAIMS</b>   | <b>13</b> |
| <b>5. SECURITY PROBLEM DEFINITION</b>  | <b>14</b> |
| 5.1 THREATS  | 14        |
| 5.2 ORGANIZATIONAL SECURITY POLICIES   | 14        |
| 5.3 ASSUMPTIONS  | 16        |
| 5.4 COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART                         | 16        |
| 5.4.1 Statement of Compatibility – Threats part                                  | 16        |
| 5.4.2 Statement of compatibility – OSPs part                                     | 19        |
| 5.4.3 Statement of compatibility – Assumptions part                              | 19        |
| <b>6. SECURITY OBJECTIVES</b>  | <b>21</b> |
| 6.1 SECURITY OBJECTIVES FOR THE TOE  | 21        |
| 6.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT                          | 22        |
| 6.3 SECURITY OBJECTIVES RATIONALES   | 22        |
| 6.3.1 Correspondence between Security Problem Definition and Security Objectives | 22        |
| 6.3.2 Security Objectives Rationale  | 23        |
| 6.4 COMPOSITION TASKS – OBJECTIVES PART  | 24        |
| 6.4.1 Statement of compatibility – TOE Objectives part                           | 24        |
| 6.4.2 Statement of compatibility – ENV Objectives part                           | 28        |
| <b>7. EXTENDED COMPONENTS DEFINITION</b>   | <b>29</b> |
| <b>8. SECURITY REQUIREMENTS</b>  | <b>30</b> |
| 8.1 SECURITY FUNCTIONAL REQUIREMENTS   | 30        |
| 8.1.1 Class FCS: Cryptographic support   | 30        |
| 8.1.2 Class FDP: User Data Protection  | 34        |
| 8.1.3 Class FIA: Identification and Authentication                               | 37        |
| 8.1.4 Class FMT: Security management   | 39        |
| 8.1.5 Class FPT: Protection of the TSF   | 39        |
| 8.1.6 Class FTP: Trusted paths / Channels  | 40        |
| 8.2 SECURITY ASSURANCE REQUIREMENTS  | 40        |
| 8.3 SECURITY REQUIREMENTS RATIONALE  | 41        |
| 8.3.1 SFR rationale – Coverage with the TOE security objectives                  | 41        |
| 8.3.2 SFR rationale sufficiency  | 42        |
| 8.3.3 SFR dependency rationale   | 44        |
| 8.3.4 Security Assurance Requirements Rationale                                  | 45        |
| 8.4 COMPOSITION TASKS – SFR PART   | 46        |
| <b>9. TOE SUMMARY SPECIFICATION</b>  | <b>53</b> |

|       |   |    |
|-------|---|----|
| 9.1   | CRYPTOGRAPHY  | 53 |
| 9.1.1 | <i>Cryptographic key generation</i>                                 | 53 |
| 9.1.2 | <i>Cryptographic key destruction</i>                                | 53 |
| 9.1.3 | <i>Cryptographic operations</i>                                     | 53 |
| 9.1.4 | <i>Generation of random numbers</i>                                 | 54 |
| 9.2   | IDENTIFICATION AND AUTHENTICATION                                   | 54 |
| 9.2.1 | <i>Supported authentication mechanisms</i>                          | 54 |
| 9.2.2 | <i>Authentication failure handling</i>                              | 54 |
| 9.2.3 | <i>Timing of identification and authentication</i>                  | 54 |
| 9.2.4 | <i>Single-use authentication mechanisms</i>                         | 55 |
| 9.3   | ACCESS CONTROL  | 55 |
| 9.3.1 | <i>Access control during the issuance procedure</i>                 | 55 |
| 9.3.2 | <i>Access control during the operational phase (BAC procedure)</i>  | 56 |
| 9.3.3 | <i>Access control during the operational phase (PACE procedure)</i> | 56 |
| 9.4   | SECURE COMMUNICATION  | 56 |
| 9.4.1 | <i>Confidentiality and integrity protection for BAC</i>             | 56 |
| 9.4.2 | <i>Confidentiality and integrity protection for PACE</i>            | 56 |
| 9.4.3 | <i>Trusted channel between the terminal and the TOE</i>             | 56 |
| 9.5   | SECURITY MANAGEMENT   | 56 |
| 9.5.1 | <i>Privileged role in pre-issuance phase</i>                        | 56 |
| 9.5.2 | <i>Import of user data in pre-issuance phase</i>                    | 57 |
| 9.6   | RESISTANCE TO PHYSICAL ATTACK                                       | 57 |
| 9.7   | MAPPING OF SFRS TO TSS  | 57 |

## LIST OF FIGURES

|  |    |
|--|----|
| Figure 1: TOE boundaries                                 | 8  |
| Figure 2: TOE life-cycle 'Init on module at Thales site' | 11 |
| Figure 3: TOE life-cycle 'Wafer Init process'            | 12 |

## LIST OF TABLES

|  |    |
|--|----|
| Table 1: Internal data of the TOE access control by passport issuing authorities | 16 |
| Table 2: Cryptographic mechanisms in Mutual authentication (BAC)                 | 32 |
| Table 3: Cryptographic mechanisms in Secure Messaging (BAC)                      | 32 |
| Table 4: Cryptographic mechanisms in Secure Messaging (PACE)                     | 34 |
| Table 5: Multiple authentication mechanisms                                      | 38 |

## 1. REFERENCE DOCUMENTS

### 1.1 EXTERNAL REFERENCES [ER]

| [ISO]         | ISO references   |
|---------------|--|
| [ISO14443]    | Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Books 1 to 4  |
| [ICAO]        | ICAO references  |
| [ICAO-9303]   | ICAO Doc 9303, Machine Readable Travel Documents - Seventh Edition, 2015   |
| [ICAO-TR-SAC] | ICAO Technical Report, Supplemental Access Control for Machine Readable Travel Documents. Version 1.1, April 15 <sup>th</sup> 2014   |
| [CC]          | Common Criteria references   |
| [CC-1]        | Common Criteria for Information Technology Security Evaluation<br>Part 1: Introduction and general model<br>CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.  |
| [CC-2]        | Common Criteria for Information Technology Security Evaluation<br>Part 2: Security Functional Requirements<br>CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.  |
| [CC-3]        | Common Criteria for Information Technology Security Evaluation<br>Part 3: Security Assurance Components<br>CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.   |
| [CCDB]        | Common Criteria Supporting Document, Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices<br>Version 1.5.1, May 2018.   |
| [PP/0084]     | Security IC Platform Protection Profile with augmentation Packages<br>Ref: BSI-CC-PP-0084-2014   |
| [JISEC C0500] | Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication<br>Ref: JISEC C0500, Version 1.00, March 8 <sup>th</sup> 2016.   |
| [ST_IC]       | Common Criteria Public Security Target – IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h – Design step H13<br>Infineon Technologies AG, Version 1.8, April 22 <sup>nd</sup> 2020 |
| [CB]          | Certification Bodies references  |
| [TR-03111]    | Technical Guideline TR-03111: Elliptic Curve Cryptography. BSI, Version 2.0, 2012  |
| [SP800-90]    | Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST, Revision 1, June 2015   |
| [RGS-B1]      | Référentiel général de sécurité version 2.0 - Annexe B1 Mécanismes cryptographiques<br>ANSSI, Version 2.03, February 21 <sup>st</sup> 2014   |

### 1.2 INTERNAL REFERENCES [IR]

| [AGD]          | eTravel Essential for Japan 1.0 Embedded Software – Guidance documentation   |
|----------------|--|
| [REF-MAN]      | eTravel Essential for Japan 1.0 – Reference Manual<br>Ref: D1501060, revision B.5, July 10 <sup>th</sup> 2020      |
| [AGD-TopLevel] | eTravel Essential for Japan 1.0 – AGD top-level document<br>Ref: D1512963, version 1.4, July 16 <sup>th</sup> 2020 |

## 2. ACRONYMS & GLOSSARY

### 2.1 ACRONYMS

|          |  |
|----------|--|
| AA       | Active Authentication                                      |
| BAC      | Basic Access Control                                       |
| BIS-BAC  | Basic Inspection System with Basic Access Control protocol |
| BIS-PACE | Basic Inspection System with PACE protocol                 |
| CAN      | Card Access Number   |
| CC       | Common Criteria  |
| EAL      | Evaluation Assurance Level                                 |
| ES       | Embedded Software  |
| IC       | Integrated Circuit   |
| IS       | Inspection system  |
| IT       | Information Technology                                     |
| LDS      | Logical Data Structure                                     |
| MRTD     | Machine readable travel document                           |
| MRZ      | Machine Readable Zone                                      |
| NVM      | Non Volatile Memory  |
| PACE     | Password Authenticated Connection Establishment            |
| PCT      | PACE Terminal  |
| PP       | Protection Profile   |
| SAC      | Supplemental Access Control                                |
| ST       | Security Target  |
| TOE      | Target of Evaluation                                       |

### 2.2 GLOSSARY

|   |  |
|---|--|
| <b>Active Authentication</b>                                      | Security mechanism by which means the MTRD's chip proves its identity and authenticity to the inspection system as part of a genuine MRTD issued by a known State or Organization.   |
| <b>Basic Access Control</b>                                       | Security mechanism by which means the MTRD's chip and the inspection system protect their communication by means of secure messaging with Basic Access Keys.   |
| <b>Basic Inspection System with Basic Access Control protocol</b> | Technical system being used by an official organisation and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn from printed MRZ data for reading the less-sensitive data (travel document details data and biographical data) stored on the travel document.      |
| <b>Basic Inspection System with PACE protocol</b>                 | A technical system being used by an inspecting authority and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. |

|  |   |
|--|---|
| <b>Card Access Number</b>                              | A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies).   |
| <b>Inspection system</b>                               | Technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.   |
| <b>Integrated circuit</b>                              | Electronic component(s) designed to perform processing and memory functions. The MRTD's chip is an integrated circuit.  |
| <b>Logical Data Structure</b>                          | The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.   |
| <b>Machine readable travel document</b>                | Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. See [ICAO-9303]   |
| <b>Machine Readable Zone</b>                           | Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. See [ICAO-9303]  |
| <b>Password Authenticated Connection Establishment</b> | A communication establishment protocol defined in [ICAO-TR-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password $\pi$ ). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained. |
| <b>PACE Terminal</b>                                   | A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the MRTD using a shared password (CAN or MRZ).   |
| <b>Supplemental Access Control</b>                     | A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.   |

### 3. SECURITY TARGET INTRODUCTION

#### 3.1 SECURITY TARGET IDENTIFICATION

|                          |   |
|--------------------------|---|
| <b>Title:</b>            | eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA, embedded in the Infineon SLC52GDA Integrated Circuit - Security Target, public version |
| <b>Version:</b>          | 1.4p  |
| <b>Author:</b>           | Thales  |
| <b>Reference:</b>        | D1510690  |
| <b>Publication date:</b> | 16/07/2020  |

#### 3.2 TOE IDENTIFICATION

|                           |  |
|---------------------------|--|
| <b>Product:</b>           | eTravel Essential for Japan 1.0  |
| <b>TOE name:</b>          | eTravel Essential for Japan Embedded Software  |
| <b>TOE version:</b>       | 0101h (Operating System release level)   |
| <b>TOE documentation:</b> | Guidance [AGD]   |
| <b>TOE hardware part:</b> | Infineon SLC52GDA <sup>1</sup> security controller (Common Criteria Certification Identifier IFX_CCI_000005h in [ST_IC]) |
| <b>Developer:</b>         | Thales   |

#### 3.3 TOE OVERVIEW

The eTravel Essential for Japan 1.0 product is a machine readable travel document (MRTD) addressing the Japan e-passport market. Based on the requirements and recommendations of the International Civil Aviation Organization [ICAO-9303], it implements the following security features:

- Basic Access Control (BAC)
- Password Authenticated Connection Establishment (PACE)
- Active Authentication mechanism (AA).

eTravel Essential for Japan 1.0 is a contactless product based on [ISO14443], type B.

For the present ST, the Target of Evaluation (TOE) is the eTravel Essential for Japan 1.0 embedded software. The TOE boundaries encompass:

- **The eTravel Essential for Japan 1.0 Embedded Software (ES)**
- **The Infineon IC, reference SLC52GDA**
- **The guidance documentation [AGD]**

The integrated circuit being already evaluated and certified, security requirements specifically addressing the integrated circuit are not reproduced within the present ST.

The eTravel Essential for Japan 1.0 product requires a contactless inspection terminal to provide its services. This terminal is outside the scope of the present evaluation.

---

<sup>1</sup> Two SLC52GDA commercial derivatives may be used and are identified in the CPLC data: SLC52GDA348 ('IC Type' set to 1904h in CPLC table) or SLC52GDA448 ('IC Type' set to 1902h in CPLC table). More information on the structure and content of the CPLC table, and how to retrieve it, is available in [REF-MAN] table 6.

### 3.4 TOE DESCRIPTION

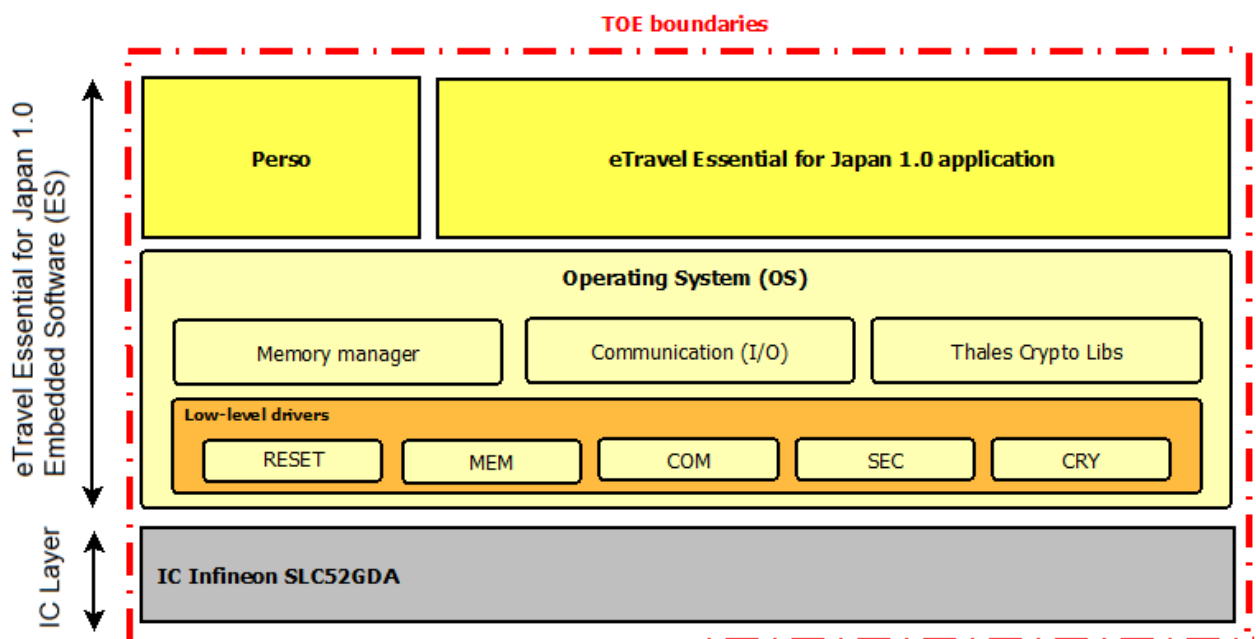
#### 3.4.1 TOE boundaries

The TOE is the module designed to be the core of an MRTD passport. The TOE is a contactless integrated circuit. The IC is connected to an antenna and capacitors and is mounted on a plastic film. This inlay is then embedded in the coversheet or datapage of the MRTD passport and provides a contactless interface for the passport holder identification.

The TOE is programmed according to the Logical Data Structure [ICAO-9303] and provides:

- Basic Access Control (BAC) according to the ICAO document [ICAO-9303]
- Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]
- PACE V2 Access Control (SAC) according to the ICAO document [ICAO-TR-SAC]

As shown by figure 1, the Target of Evaluation (TOE) is composed of the eTravel Essential for Japan 1.0 Embedded Software (ES), supported by the SLC52GDA integrated circuit. The eTravel Essential for Japan 1.0 data are also part of the TOE, as well as the guidance documentation [AGD].



**Figure 1: TOE boundaries**

The eTravel Essential for Japan 1.0 Embedded Software (ES) is implemented in the NVM memory (flash technology) of the chip. The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition, the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent or from the Personalization Agent to the MRTD Manufacturer.

#### 3.4.2 TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveller presents an MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD.



The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

- a) The physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder
  - (1) The biographical data on the biographical data page of the passport book,
  - (2) The printed data in the Machine Readable Zone (MRZ) and
  - (3) The printed portrait.
- b) The logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [ICAO-9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder
  - (1) The digital Machine Readable Zone Data (digital MRZ data, EF.DG1),
  - (2) The digitized portraits (EF.DG2),
  - (3) The other data according to LDS (EF.DG5 to EF.DG13, EF.DG15 and EF.DG16)
  - (4) The Document security object (EF.SOD), the security information file for PACE protocol (EF.CardAccess) and the Header and Data Group Presence Information (EF.COM).

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [ICAO-9303]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication, and optional advanced security methods. For the present TOE, the Active Authentication of the MRTD's chip and the Password Authenticated Connection Establishment (PACE, defined in [ICAO-TR-SAC]) are implemented. Note that the Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

Keys for Active Authentication can be generated in the card or loaded into it. These operations take place at personalization time.

### 3.4.3 TOE lifecycle

The TOE life cycle is described in terms of the four life cycle phases. With respect to the [PP/0084], these four phases are additionally subdivided into 7 steps.

#### **Phase 1 "Development":**

(Step1) The IC Developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The Embedded Software Developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the MRTD application and the associated guidance documentation.

#### **Phase 2 "Manufacturing":**

(Step3) The TOE integrated circuit is produced by the IC Manufacturer conforming to Thales requirements. The IC Manufacturer writes the IC Identification Data onto the chip to control the IC during the IC manufacturing and the delivery process to the MRTD Manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD Manufacturer or to the Inlay Manufacturer.

(Step4) The MRTD Manufacturer initializes the IC/inlay by loading the MRTD application in the IC flash memory.

(Step5) The MRTD Manufacturer (i) Initializes the MRTD application and (ii) equips MRTD's chips with Prepersonalization Data. The pre-personalized MRTD together with the IC Identifier are securely delivered

from the MRTD Manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

**Phase 3 “Personalization of the MRTD”:**

(Step 6) The personalization of the MRTD includes (i) the survey of the MRTD holder’s biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object. The signing of the Document security object by the Document signer finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

**Phase 4 “Operational Use”:**

(Step7) The TOE is used as MRTD chip by the traveller and the inspection systems in the “Operational Use” phase. The user data can be read according to the security policy of the issuing State or Organization and can be used according to the security policy of the issuing State but they can never be modified.

Application note: In this ST, the role of the Personalization Agent is strictly limited to the phase 3 Personalization. In the phase 4 (Operational Use), updating and addition of the data groups of the MRTD application is forbidden.

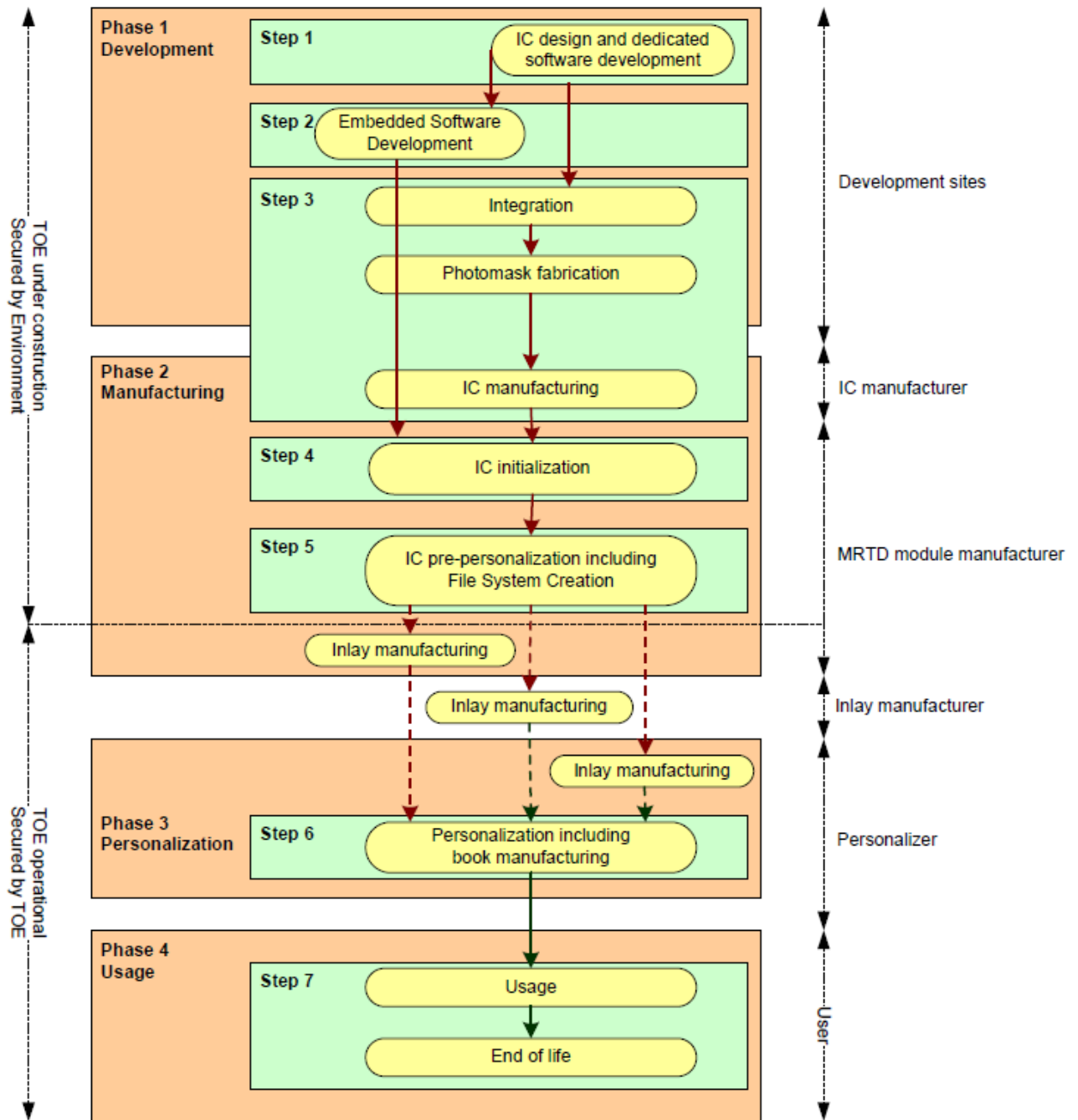
The following actors are identified during the life-cycle phases:

| Actor                                | Identification  |
|--------------------------------------|---|
| Integrated Circuit (IC) Developer    | Infineon  |
| Embedded Software Developer          | Thales  |
| Integrated Circuit (IC) Manufacturer | Infineon  |
| MRTD Module Manufacturer             | Thales  |
| Pre-personalizer                     | Thales  |
| Inlay Manufacturer                   | Thales or another inlay manufacturer  |
| Book Manufacturer                    | Thales or another printer   |
| Personalization Agent                | The agent who is acting on the behalf of the issuing State or Organization and personalizes the MRTD for the holder by activities establishing the identity of the holder with biographic data. |
| MRTD Holder                          | The rightful holder of the MRTD for whom the issuing State or Organization personalizes the MRTD.   |

Two TOE life cycles are possible and are described in figure 2 and figure 3. Whatever the life cycle, the TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of step 5.

Note: the guidance documentation [AGD] is delivered in the form of electronic documents (pdf format) by the Thales technical representative to the Personalizer and the passport issuing authorities. The files are encrypted and sent by email.

**TOE life-cycle: 'Init on module at Thales site'**

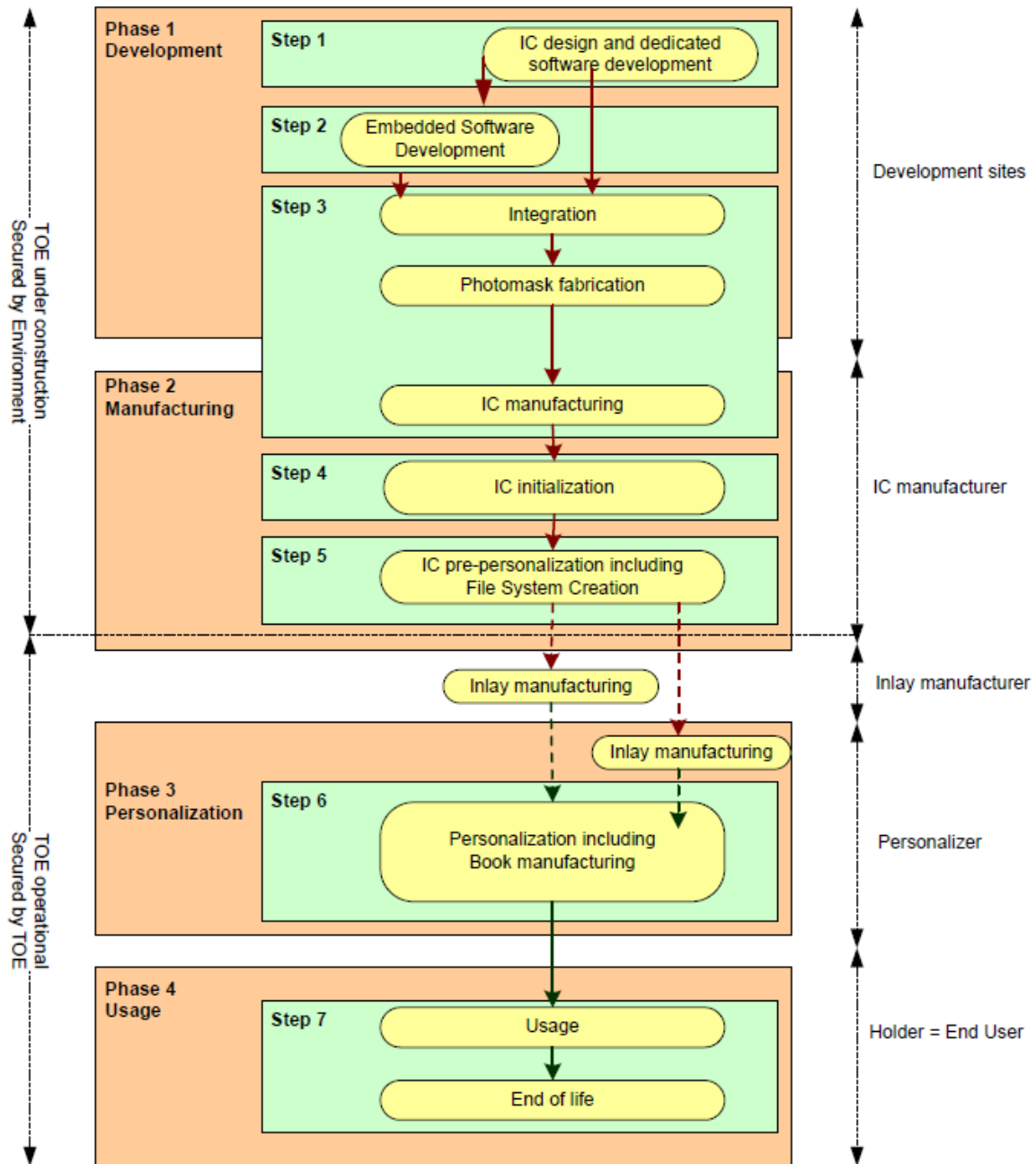


**Figure 2: TOE life-cycle 'Init on module at Thales site'**

The IC is manufactured at the founder site. It is then shipped to Thales site where it is initialized (OS loading) and pre-personalized. The transformation of wafers into modules can be performed either at the founder site or at Thales site. The modules are then shipped to the Personalizer or to the Inlay manufacturer. In the latter case, the Inlay manufacturer ships the inlays to the Personalizer.

During the shipment from Thales to the Personalizer or the Inlay manufacturer, the module is protected by a diversified key.

**TOE life-cycle: ‘Wafer Initialization process’**



**Figure 3: TOE life-cycle ‘Wafer Init process’**

The wafers are directly shipped from the founder to the Personalizer. This specific Life Cycle requires initialization (OS loading) and pre-personalization of the chip at the founder site.

During the shipment from the founder to the Personalizer, each die is protected with a diversified key.

**3.4.4 Non-TOE hardware/software/firmware required by the TOE**

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

## 4. CONFORMANCE CLAIMS

### Common criteria Version:

This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

### Conformance to CC part 2 and 3:

This ST is CC part 2 extended and CC part 3 conformant.

### Assurance package conformance:

EAL4 augmented (EAL4+)

This ST conforms to the assurance package EAL4 augmented by ADV\_FSP.5, ADV\_INT.2, ADV\_TDS.4, ALC\_CMS.5, ALC\_DVS.2, ALC\_TAT.2, ATE\_DPT.3.

### Evaluation type

This is a composite evaluation, which relies on the SLC52GDA chip certificate and evaluation results.

#### SLC52GDA chip certificate:

- Certification done under the BSI scheme
- Certification report BSI-DSZ-CC-1110-V3-2020 (Common Criteria Certification Identifier IFX\_CCI\_000005h)
- Security Target [ST\_IC] strictly conformant to IC Protection Profile [PP/0084]
- Common criteria version: 3.1
- Assurance level: EAL6 augmented by ALC\_FLR.1

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

### Protection Profile conformance claim:

This ST claims strict conformance to the [JISEC C0500] Protection Profile.

## 5. SECURITY PROBLEM DEFINITION

### 5.1 THREATS

This section describes the threats that the TOE shall counter. These threats shall be countered by the TOE, its operational environment or combination of these two.

| Threat identifier             | Threat description  |
|-------------------------------|---|
| <b>T.Copy</b>                 | An attacker trying to forge an ePassport may do so by reading personal information along with digital signature from the TOE and writing the copied data in an IC chip having the same functionality as that of the TOE. This attack damages the credibility of the entire passport booklet system including TOEs.  |
| <b>T.Logical_Attack</b>       | In the operational environment after issuing a TOE embedded passport booklet, an attacker who can read the MRZ data of the passport booklet may try to read confidential information (Active Authentication Private Key) stored in the TOE through the contactless communication interface of the TOE.  |
| <b>T.Communication_Attack</b> | In the operational environment after issuing a TOE embedded passport booklet, an attacker who does not know about MRZ data may interfere with the communication between the TOE and a terminal to disclose and/or alter communication data that should be concealed.  |
| <b>T.Physical_Attack</b>      | In the operational environment after issuing a TOE embedded passport booklet, an attacker may attempt to disclose confidential information (Active Authentication Private Key) stored in the TOE, unlock the state of the locked key, or reactivate a deactivated access control function by physical means. This physical means include both of nondestructive attacks made without impairing the TOE functions and destructive attacks made by destroying part of the TOE to have mechanical access to the inside of the TOE. |

### 5.2 ORGANIZATIONAL SECURITY POLICIES

This section describes the organizational security policies that apply to the TOE and its operational environment. These organizational security policies include conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan.

| OSP identifier | OSP content  |
|----------------|--|
| <b>P.BAC</b>   | In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read certain information from the TOE in accordance with the BAC procedure defined by Part 11 of [ICAO-9303]. This procedure includes mutual authentication and Secure Messaging between the TOE and terminal devices. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD under the rules stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined. Note that this organizational security policy will not be applied after disabling BAC with P.Disable_BAC. |
| <b>P.PACE</b>  | In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read a certain information from the TOE in accordance with the PACE procedure defined by Part 11 of [ICAO-9303]. This procedure includes mutual authentication and Secure Messaging between the TOE and terminal devices. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD under the rules stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined.  |

|                      |  |
|----------------------|--|
| <b>P.Authority</b>   | The TOE under the control of the passport issuing authorities shall allow only authorized users (persons who succeeded in verification of readout key, transport key, or Active Authentication Information Access Key) to have access to the internal data of the TOE, as shown in Table 1.  |
| <b>P.Data_Lock</b>   | When the TOE detects a failure in authentication with the transport key, readout key or Active Authentication Information Access Key, it will permanently disable authentication related to each key, thereby prohibiting reading or writing the file based on successful authentication thereof. Table 1 shows the relationship between the key used for authentication and its corresponding file in the TOE.  |
| <b>P.Prohibit</b>    | Any and all writings to the files in the TOE and readings from the files in the TOE based on successful authentication with readout key are prohibited after issuing an ePassport to the passport holder. Disabling authentication through authentication failure with the transport key, readout key, and Active Authentication Information Access Key (see P.Data_Lock) shall be used as the means for that purpose.   |
| <b>P.Disable_BAC</b> | In accordance with the passport issuing authorities' policies against compromise of BAC, TOEs issued after a certain time shall not accept the BAC procedure. As a means to achieve it, a TOE provides the procedure of disabling the BAC functions, and a user authorized by the passport issuing authorities disables the BAC function by implementing the procedure.<br><br>Note: This organizational security policy shall be applied only if the passport issuing authorities demand to terminate issuing IC chip equipped with the BAC function. |

| Authentication status <sup>2</sup>         | File subject to access control   | Operation permitted | Reference: data to be operated  |
|--|--|---------------------|---|
| Successful verification with readout key   | EF.DG13 <sup>3</sup>   | Read                | IC chip serial number (entered by manufacturer)   |
| Successful verification with transport key | Transport key file   | Write               | Transport key data (update of old data)   |
|  | Basic access key file  |                     | Basic access key (Encryption key)<br>Basic access key (Message Authentication Code key) |
|  | Password key file  |                     | Password key  |
|  | EF.DG1   | Read or Write       | MRZ data  |
|  | EF.DG2   |                     | Facial image  |
|  | EF.DG13  |                     | Management data (Passport number and Booklet management number)                         |
|  | EF.DG14  |                     | PACE v2 Security information<br>Active Authentication hash function information         |
|  | EF.COM <sup>4</sup>  |                     | Common data   |
| EF.SOD                                     | Security data related to Passive Authentication defined by Part 10 of [ICAO-9303]. |                     |   |

<sup>2</sup> The readout key, transport key, and Active Authentication Information Access Key are configured by the manufacturer. The transport key can be changed (updated) by an authorized user. With regard to the files subject to access control included in this table and files storing the read key and Active Authentication Information Access Key which may vary the authentication status, user access that is not stated in this table or PP Notes is prohibited. (The access controls to information in the TOE from terminals after issuing a TOE embedded passport booklet to the passport holder, i.e., BAC and PACE are separately specified.)

<sup>3</sup> In EF.DG13, an IC chip serial number has been recorded by the manufacturer, and the management data is appended to the file by the passport issuing authorities.

<sup>4</sup> EF.COM file may not be created according to the passport issuing authorities' instructions.

|   |                  |       |                                   |
|---|------------------|-------|-----------------------------------|
|   | EF.CardAccess    | Write | PACE v2 Security information      |
|   | EF.DG15          | Read  | Active Authentication Public Key  |
| Successful verification with Active Authentication Information Access Key | EF.DG15          | Write | Active Authentication Public Key  |
|   | Private key file |       | Active Authentication Private Key |

Table 1: Internal data of the TOE access control by passport issuing authorities

### 5.3 ASSUMPTIONS

This section describes the assumptions to be addressed in the operational environment of the TOE. These assumptions need to be true for the TOE security functionality to become effective.

| Assumption identifier       | Content  |
|-----------------------------|--|
| <b>A.Administrative_Env</b> | The TOE that was delivered from the TOE manufacturer to the passport issuing authorities and is under the control of the authorities shall be securely controlled and go through an issuing process until it is finally issued to the passport holder.   |
| <b>A.PKI</b>                | In order for the passport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuer and stored in the TOE (including the Active Authentication Public Key), the interoperability of the PKI environment both of the issuing and receiving states or organizations of the passport shall be maintained by passport issuing authorities. |

### 5.4 COMPOSITION TASKS – SECURITY PROBLEM DEFINITION PART

#### 5.4.1 Statement of Compatibility – Threats part

The following table (see next page) lists the relevant threats of the [ST\_IC] security target, and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.



eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| IC relevant threat label | IC relevant threat title                | IC relevant threat content   | Link to the composite-product threats |
|--------------------------|---|--|---------------------------------------|
| T.Leak-Inherent          | Inherent Information Leakage            | <p>An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data as part of the assets.</p> <p>No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.</p>   | T.Physical_Attack                     |
| T.Phys-Probing           | Physical Probing                        | <p>An attacker may perform physical probing of the TOE in order</p> <ul style="list-style-type: none"> <li>(i) To disclose user data while stored in protected memory areas</li> <li>(ii) To disclose/reconstruct the user data while processed or</li> <li>(iii) To disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.</li> </ul>   | T.Physical_Attack                     |
| T.Malfunction            | Malfunction due to Environmental Stress | <p>An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to</p> <ul style="list-style-type: none"> <li>(i) Modify security services of the TOE or</li> <li>(ii) Modify functions of the Security IC Embedded Software</li> <li>(iii) Deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.</li> </ul> <p>This may be achieved by operating the Security IC outside the normal operating conditions.</p> | T.Physical_Attack                     |
| T.Phys-Manipulation      | Physical Manipulation                   | <p>An attacker may physically modify the Security IC in order to</p> <ul style="list-style-type: none"> <li>(i) Modify user data of the Composite TOE</li> <li>(ii) Modify the Security IC Embedded Software</li> <li>(iii) Modify or deactivate security services of the TOE, or</li> <li>(iv) Modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.</li> </ul>   | T.Physical_Attack                     |
| T.Leak-Forced            | Forced Information Leakage              | <p>An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the Composite TOE as part of the assets even if the information leakage is not inherent but caused by the attacker.</p>   | T.Physical_Attack                     |
| T.Abuse-Func             | Abuse of Functionality                  | <p>An attacker may use functions of the TOE which may not be used after TOE Delivery in order to</p> <ul style="list-style-type: none"> <li>(i) Disclose or manipulate user data of the Composite TOE</li> <li>(ii) Manipulate (explore, bypass, deactivate or change) security services of the TOE or</li> <li>(iii) Manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or</li> </ul>  | T.Copy                                |

## eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

|                          |                              |   |  |
|--------------------------|------------------------------|---|--|
|                          |                              | (iv) Enable an attack disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.   |  |
| T.RND                    | Deficiency of Random Numbers | An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.  | T.Logical_Attack<br>T.Communication_Attack |
| T.Masquerade_TOE         | Masquerade the TOE           | An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.  | T.Copy                                     |
| T.Mem-Access             | Memory Access Violation      | Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code) or privilege levels. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.  | T.Copy                                     |
| T.Open_Samples_Diffusion | Diffusion of open samples    | An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code ...). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography...). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by deactivating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC. | T.Physical_Attack                          |

### 5.4.2 Statement of compatibility – OSPs part

The following table lists the relevant OSPs of the [ST\_IC] security target, and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.

| IC OSP label       | IC OSP content   | Link to the composite product   |
|--------------------|--|---|
| P.Process-TOE      | <p>Identification during TOE Development and Production:</p> <p>An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.</p>   | No contradiction with the present evaluation; the chip traceability information is used to identify the composite TOE.                                |
| P.Add-Functions    | <p>Additional Specific Security Functionality:</p> <p>The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:</p> <ul style="list-style-type: none"> <li>▪ Rivest-Shamir-Adleman Cryptography (RSA)</li> <li>▪ Elliptic Curve Cryptography (EC)</li> <li>▪ CIPURSE™ Cryptographic Library (CCL)</li> <li>▪ Cipher based Message Authentication Code (CMAC by the SCL-1)</li> <li>▪ Secure Hash Computation (SHA by the HCL)</li> </ul> | Not used as the Composite TOE implements its own cryptographic libraries.   |
| P.Crypto-Service   | <p>Cryptographic services of the TOE</p> <p>The TOE provides secure hardware based cryptographic services for the IC Embedded Software:</p> <ul style="list-style-type: none"> <li>▪ Triple Data Encryption Standard (TDES)</li> <li>▪ Advanced Encryption Standard (AES)</li> </ul>   | <p>The AES hardware functionality is used by the composite TOE.</p> <p>The TDES hardware functionality is used by the composite TOE.</p>              |
| P.Lim_Block_Loader | <p>Limiting and Blocking the Loader Functionality</p> <p>The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.</p>   | Enforced by the MRTD Manufacturer, which irreversibly deactivates the Infineon Loader after the eTravel for Japan 1.0 Embedded Software (ES) loading. |
| P.Ctrl_Loader      | <p>Controlled usage to Loader Functionality</p> <p>Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation.</p>  | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7.                           |

### 5.4.3 Statement of compatibility – Assumptions part

The following table (see next page) lists the relevant assumptions of the [ST\_IC] security target, and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| IC assumption label | IC assumption title  | IC assumption content  | IrPA | CfPA | SgPA | Link to the composite product |
|---------------------|--|--|------|------|------|-------------------------------|
| A.Process-Sec-IC    | Protection during Packaging, Finishing and Personalization | It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).   |      |      | X    | A.Administrative_Env          |
| A.Resp-Appl         | Treatment of User data of the Composite TOE                | All User data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User data of the composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.   |      | X    |      | O.Logical_Attack              |
| A.Key-Function      | Usage of key-dependent functions                           | Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).<br><br>Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address the cryptographic routines which are part of the TOE. |      | X    |      | O.Physical_Attack             |

## 6. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and its environment for the security problems described in Chapter 5. Section 6.1 describes the security objectives to be addressed by the TOE, while Section 6.2 describes those to be addressed by its environment. In addition, Section 6.3 describes rationales for the appropriateness of the security objectives for solving the security problems.

The security objectives for the TOE and the security objectives for the operational environment are represented by an identifier with the prefix “O.” or “OE.” respectively.

### 6.1 SECURITY OBJECTIVES FOR THE TOE

This section describes the security objectives that the TOE should address to solve problems with regard to the threats and organizational security policies that are defined as the security problems.

| Objective identifier     | Objective description  |
|--------------------------|--|
| <b>O.AA</b>              | The TOE shall provide a means to verify the authenticity of the IC chip itself that composes the TOE in order to prevent the copy of personal information including the digital signature on an illicit IC chip and the forgery of the passport. This means shall be standardized so as to ensure the global interoperability of ePassport and, for this purpose, shall support the Active Authentication defined by Part 11 of [ICAO-9303].   |
| <b>O.Logical_Attack</b>  | The TOE shall, under any circumstances, prevent confidential information in them (Active Authentication Private Key) from being externally read through the contactless communication interface of the TOE.  |
| <b>O.Physical_Attack</b> | The TOE shall prevent the confidential information (Active Authentication Private Key) within the TOE from being disclosed or the information relating to the security from being tampered with by the attackers using physical means. The TOE shall counter attacks applicable to the TOE itself out of known attacks against IC chips, considering physical means including both nondestructive attacks and destructive attacks.   |
| <b>O.BAC</b>             | This security objective applies to the operational environment after issuing the passport booklet. The BAC procedure defined by Part 11 of [ICAO-9303], if the terminals require, shall be used to ensure the global interoperability of the ePassport. This procedure shall be used in the mutual authentication and Secure Messaging between the TOE and terminals.<br>Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD files among the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to read the files stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined. |
| <b>O.PACE</b>            | This security objective applies to the operational environment after issuing the passport booklet. PACE procedure defined by Part 11 of [ICAO-9303], if the terminals require, shall be used to ensure the global interoperability of the ePassport. This procedure shall be used in the mutual authentication and Secure Messaging between the TOE and terminals.<br>Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD files among the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to read the files stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined.    |
| <b>O.Authority</b>       | The TOE shall limit users who can access the internal TOE data and their operations, in the environment under the control of the passport issuing authorities according to Table 1 described in the organizational security policy P. Authority.   |
| <b>O.Data_Lock</b>       | The operation of the internal TOE data shall be available only to the authorized user (i.e., authorized personnel under the control of the passport issuing authorities or the terminal after issuing the passport) to prevent illicit reading and writing by any users other than those stated above. As a means for this purpose, if the TOE detects an authentication failure with the readout key, transport key, or Active Authentication   |

|                      |  |
|----------------------|--|
|                      | Information Access Key, it shall be permanently prohibited to read or to write the internal TOE data permitted according to authentication related to each of the said keys. This security objective shall also apply in the event that the passport issuing authorities disable readout key, transport key, or Active Authentication Information Access Key by causing an authentication failure intentionally before the TOE is issued to the passport holder. The relationship between the readout key, transport key, and Active Authentication Information Access Key and their corresponding internal TOE data is as listed in Table 1 of the organizational security policy P.Authority. After the security objective O.Data_Lock is achieved, only the access to TOE stated in the security objectives O.BAC or O.PACE is permitted. |
| <b>O.Disable_BAC</b> | TOEs with the BAC function shall provide procedure to disable the functions.   |

## 6.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section describes the security objectives that should be addressed in the operational environment to solve problems with regard to the threats and organizational security policies and assumptions defined as the security problems.

| Objective identifier         | Objective description  |
|------------------------------|--|
| <b>OE.Administrative_Env</b> | The TOE under the control of the passport issuing authorities is subjected to secure management and treatment until it is delivered to the passport holder through the issuing procedures.   |
| <b>OE.Disable_BAC</b>        | A user authorized by the passport issuing authorities shall perform a procedure for disabling the BAC function of TOE in accordance with the passport issuing authorities.   |
| <b>OE.PKI</b>                | In order for the ePassport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuing state or organization and stored in the TOE (i.e., information on the passport holder and the Active Authentication Public Key), passport issuing authorities shall maintain the interoperability of the PKI environment in both the passport issuing state and receiving state. |

## 6.3 SECURITY OBJECTIVES RATIONALES

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition. Section 6.3.1 describes that each of the security objective can be traced back to any of the security problems, while Section 6.3.2 describes that any of the security problems is effectively addressed by the corresponding security objective.

### 6.3.1 Correspondence between Security Problem Definition and Security Objectives

The following table shows the correspondence between the security problem definition and the security objectives. As shown in the table, all security objectives can be traced back to one (or more) item(s) in the security problem definition.

|                        | O.AA | O.Logical_Attack | O.Physical_Attack | O.BAC | O.PACE | O.Authority | O.Data_Lock | O.Disable_BAC | OE.Administrative_Env | OE.Disable_BAC | OE.PKI |
|------------------------|------|------------------|-------------------|-------|--------|-------------|-------------|---------------|-----------------------|----------------|--------|
| T.Copy                 | X    |                  |                   |       |        |             |             |               |                       |                |        |
| T.Logical_Attack       |      | X                |                   |       |        |             |             |               |                       |                |        |
| T.Communication_Attack |      |                  |                   | X     | X      |             |             |               |                       |                |        |
| T.Physical_Attack      |      |                  | X                 |       |        |             |             |               |                       |                |        |
| P.BAC                  |      |                  |                   | X     |        |             |             |               |                       |                |        |
| P.PACE                 |      |                  |                   |       | X      |             |             |               |                       |                |        |
| P.Authority            |      |                  |                   |       |        | X           |             |               |                       |                |        |
| P.Data_Lock            |      |                  |                   |       |        |             | X           |               |                       |                |        |
| P.Prohibit             |      |                  |                   |       |        |             | X           |               |                       |                |        |
| P.Disable_BAC          |      |                  |                   |       |        |             |             | X             |                       | X              |        |
| A.Administrative_Env   |      |                  |                   |       |        |             |             |               | X                     |                |        |
| A.PKI                  |      |                  |                   |       |        |             |             |               |                       |                | X      |

### 6.3.2 Security Objectives Rationale

This section describes rationales for the security objectives for the TOE and the operational environment to thoroughly counter all identified threats, implement organizational security policies, and also properly meet the assumptions.

| Item in the Security Problem Definition | Rationale  |
|---|--|
| T.Copy                                  | If an attacker copies the personal information (with digital signature) read from the TOE to the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through the verification of digital signature. To prevent this attack, the security objective for the TOE: O.AA addresses embedding of data that enable verifying the authenticity of the IC chip itself in the TOE. This enables the TOE to detect illicit IC chips and prevent the forgery of passports, thus removing the threat of T.Copy. |
| T.Logical_Attack                        | The security objective for the TOE: O.Logical_Attack makes it possible to prohibit reading confidential information (Active Authentication Private Key) in the TOE through the contactless communication interface of the TOE, under any circumstances. Thus the threat of T.Logical_Attack is removed.  |
| T.Communication_Attack                  | The security objectives for the TOE: O.BAC and O.PACE makes it possible to use a secure communication path for the communication between the terminals and the TOE. Thus the threat of disclosure and alteration of the communication data of T.Communication_Attack can be diminished to an adequate level for the practical use.   |
| T.Physical_Attack                       | The security objective for the TOE: O.Physical_Attack makes it possible to counter an attack to disclose confidential information (Active Authentication Private Key) in the TOE or tamper security-related information not via the  |

|                             |  |
|-----------------------------|--|
|                             | contactless communication interface of the TOE but physical means. Regarding the physical means, both nondestructive attacks and destructive attacks are considered, and countermeasures shall be implemented so that the TOE can counter known attacks against the IC chip. Thus the threat can be diminished to an adequate level for the practical use.   |
| <b>P.BAC</b>                | The security objective for the TOE: O.BAC allows only the authorized personnel (terminal) to read the internal TOE data through a secure communication path by applying the BAC procedure defined by [ICAO-9303] Part 11. O.BAC includes all contents of P.BAC, thus the organizational security policy P.BAC is properly implemented.   |
| <b>P.PACE</b>               | The security objective for the TOE: O.PACE allows only the authorized personnel (terminal) to read the internal TOE data through a secure communication path by applying PACE procedure defined by Part 11 of [ICAO-9303]. O.PACE includes all contents of P.PACE, thus the organizational security policy P.PACE is properly implemented.   |
| <b>P.Authority</b>          | The security objective for the TOE: O.Authority provides the contents to directly implement the organizational security policy P.Authority.  |
| <b>P.Data_Lock</b>          | The security objective for the TOE: O.Data_Lock includes the contents required by the organizational security policy P.Data_Lock and properly implements P.Data_Lock.  |
| <b>P.Prohibit</b>           | The organizational security policy P.Prohibit requires the implementation of an intentional authentication failure by the authorized TOE user as the implementation means. Actions required for the TOE to address P.Prohibit are the same as those for the organizational security policy P.Data_Lock that has assumed an illicit attack on the TOE. Therefore, the security objective for the TOE: O.Data_Lock will also implement the contents of P.Prohibit. |
| <b>P.Disable_BAC</b>        | The security objective for the TOE: O.Disable_BAC and the security objective for the Operational Environment: OE.Disable_BAC includes the contents required by the organizational security policy P.Disable_BAC and properly implements P.Disable_BAC.   |
| <b>A.Administrative_Env</b> | The security objective for the operational environment: OE.Administrative_Env directly corresponds to the assumption A.Administrative_Env, thus this assumption is met.  |
| <b>A.PKI</b>                | The security objective for the operational environment: OE.PKI directly corresponds to the assumption A.PKI, thus this assumption is met.  |

## 6.4 COMPOSITION TASKS – OBJECTIVES PART

### 6.4.1 Statement of compatibility – TOE Objectives part

The following table (see next page) lists the relevant TOE security objectives of the underlying IC, and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.



eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Label of the chip TOE security objective | Title of the chip TOE security objective        | Content of the chip TOE security objective   | Linked Composite-product TOE security objectives |
|--|---|--|--|
| O.Leak-Inherent                          | Protection against Inherent Information Leakage | <p>The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC</p> <ul style="list-style-type: none"> <li>- By measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and</li> <li>- By measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).</li> </ul> <p>This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface.</p>   | O.Physical_Attack                                |
| O.Phys-Probing                           | Protection against Physical Probing             | <p>The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE. This includes protection against</p> <ul style="list-style-type: none"> <li>- Measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or</li> <li>- Measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)</li> </ul> <p>with a prior reverse-engineering to understand the design and its properties and functions.</p> | O.Physical_Attack                                |
| O.Malfunction                            | Protection against Malfunctions                 | <p>The TOE must ensure its correct operation.</p> <p>The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.</p>  | O.Physical_Attack                                |
| O.Phys-Manipulation                      | Protection against Physical Manipulation        | <p>The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Security IC Embedded Software and the user data of the Composite TOE. This includes protection against</p> <ul style="list-style-type: none"> <li>- reverse-engineering (understanding the design and its properties and functions),</li> <li>- manipulation of the hardware and any data, as well as</li> <li>- controlled manipulation of memory contents.</li> </ul>  | O.Physical_Attack                                |
| O.Leak-Forced                            | Protection against Forced Information Leakage   | <p>The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker</p> <ul style="list-style-type: none"> <li>- By forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or</li> <li>- By a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”.</li> </ul> <p>If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.</p>   | O.Physical_Attack                                |

## eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

|                    |  |  |  |
|--------------------|--|--|--|
| O.Abuse-Func       | Protection against Abuse of Functionality      | The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE, (ii) manipulate critical user data of the Composite TOE, (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here. | O.AA<br>O.Logical_Attack<br>O.Authority<br>O.Data_Lock   |
| O.Identification   | TOE Identification                             | The TOE must provide means to store Initialisation Data and Pre-personalization Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.   | No direct link to the composite-product TOE objectives, however chip traceability information stored in NVM is used by the TOE to answer identification CC assurance requirements.   |
| O.RND              | Random Numbers                                 | The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.   | O.AA<br>O.BAC<br>O.PACE  |
| O.Cap_Avail_Loader | Capability and availability of the Loader      | The TSF provides limited capability of the Loader functionality and irreversible termination of the Loader in order to protect stored user data from disclosure and manipulation.  | O.AA<br>O.Logical_Attack<br>O.Authority<br>O.Data_Lock   |
| O.Authentication   | Authentication to external entities            | The TOE shall be able to authenticate itself to external entities. The Initialization Data (or parts of them) are used for TOE authentication verification data.   | No direct link to the composite-product TOE objectives, however it is relevant for the phases before the TOE delivery point (when the eTravel for Japan 1.0 software is not loaded yet in the IC), as it supports authentication to the Infineon Loader. |
| O.Ctrl_Auth_Loader | Access control and authenticity for the Loader | The TSF provides trusted communication channel with authorized user, supports confidentiality protection and authentication of the user data to be loaded and access control for usage of the Loader functionality.  | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7.  |
| O.TDES             | Cryptographic service Triple-DES               | The TOE provides secure hardware based cryptographic services implementing the Triple-DES for encryption and decryption.   | O.BAC<br>O.PACE  |
| O.AES              | Cryptographic service AES                      | The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.   | O.PACE   |
| O.Add-Functions    | Additional Specific                            | The TOE must provide the following specific security functionality to the Smartcard Embedded Software: <ul style="list-style-type: none"> <li>▪ Rivest-Shamir-Adleman cryptography (RSA)</li> </ul>  | Irrelevant as Thales has implemented its own cryptographic libraries   |

## eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

|                            |  |  |   |
|----------------------------|--|--|---|
|                            | Security Functionality                       | <ul style="list-style-type: none"> <li>▪ Elliptic Curve Cryptography (EC)</li> <li>▪ CIPURSE™ Cryptography</li> <li>▪ Cipher base Message authentication code (CMAC)</li> <li>▪ Hash Cryptographic Library (HCL)</li> </ul>  |   |
| O.Mem-Access               | Area based Memory Access Control             | The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas and privilege levels is controlled as required, for example, in a multi-application environment. | O.Authority   |
| O.Prot_TSF_Confidentiality | Protection of the confidentiality of the TSF | The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit...) through the use of a dedicated code loaded on open samples.   | No contradiction with the security objectives of the composite TOE. |
| O.Ctrl_Auth_CCL            | Authentication of entities                   | The CIPURSE™ CL must implement mutual authentication to establish a ready to use secure communication channel between two authenticated entities before any other communication between the two entities is applied.   | Not used by the Composite TOE.                                      |
| O.Prot_Integrity           | Integrity protection                         | The CIPURSE™ CL must implement integrity protection functionality for the user data to be exchanged via the secure communication channel.  | Not used by the Composite TOE.                                      |
| O.Prot_Confidentiality     | Confidentiality protection                   | The CIPURSE™ CL must protect the confidentiality of the user data to be exchanged via the secure communication channel if the user configures accordingly.   | Not used by the Composite TOE.                                      |
| O.Data_IntegrityService    | User data integrity service                  | The Hash Cryptographic Library HCL provides secure hash digest computation upon provided user data.  | Not used by the Composite TOE.                                      |

## 6.4.2 Statement of compatibility – ENV Objectives part

The following table lists the relevant ENV security objectives related to the underlying IC, and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

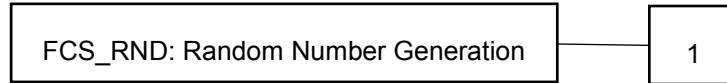
| IC ENV security objective label | IC ENV security objective title                   | IC ENV security objective content   | Link to the composite-product   |
|---------------------------------|---|---|---|
| OE.Resp-Appl                    | Treatment of user data of the composite TOE       | Security relevant user data of the composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.<br><br>For example the Security IC Embedded Software will not disclose security relevant user data of the composite TOE to unauthorized users or processes when communicating with a terminal. | Covered by TOE Security Objectives:<br>O.Logical_Attack<br>O.Authority<br>O.Data_Lock                                       |
| OE.Process-Sec-IC               | Protection during composite product manufacturing | The protection during packaging, finishing and personalization includes also the personalization process (Flash Loader) and the personalization data (TOE software components) during Phase 4, Phase 5 and Phase 6.   | OE.Administrative_Env   |
| OE.Lim_Block_Loader             | Limitation of capability and blocking the Loader  | The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.   | Enforced by the composite Product Manufacturer.   |
| OE.TOE_Auth                     | Authentication to external entities               | The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.  | Enforced by the composite Product Manufacturer.   |
| OE.Loader_Usage                 | Secure communication and usage of the Loader      | The authorized user must support the trusted communication with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader.  | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |

## 7. EXTENDED COMPONENTS DEFINITION

### FCS\_RND: Random number generation

**Family Behaviour:** This family defines quality requirements for the generation of random numbers to be used for cryptographic purposes.

**Component levelling:**



FCS\_RND.1 Random number generation requires the random numbers to meet defined quality standards.

**Management, FCS\_RND.1:** There is no management activity foreseen.

**Audit, FCS\_RND.1:** There is no auditable event foreseen.

FCS\_RND.1 Quality standards for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

**FCS\_RND.1.1** The TSF shall provide a random number generation mechanism that meet *[Assignment: defined quality standard]*.

## 8. SECURITY REQUIREMENTS

This section specifies the requirements that apply to the TOE:

- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)

The stated requirements lead to the development of a TOE that meets its security objectives.

The security requirements specifically applying to the IC are not reproduced in the present Security Target.

### 8.1 SECURITY FUNCTIONAL REQUIREMENTS

Typographical conventions:

- Selections and assignments that have already been made in the [JISEC C0500] Protection Profile are *italicized and underlined*, and the original text on which the selection or assignment has been made is not reminded.
- Selections and assignments made in this ST are ***in bold, italicized and underlined***, and the PP original text on which the selection or assignment has been made is indicated in a footnote.

#### 8.1.1 Class FCS: Cryptographic support

##### FCS\_CKM.1b Cryptographic key generation (BAC)

Hierarchical to: No other components.

Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.1.1b** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Session key generation algorithm in the Basic Access Control specified by Part 11 of [ICAO-9303]* and specified cryptographic key sizes *112 bits* that meet the following: *Standards for session key generation in the Basic Access Control specified by Part 11 of [ICAO-9303]*.

##### FCS\_CKM.1p Cryptographic key generation (PACE, session keys)

Hierarchical to: No other components.

Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.1.1p** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Session key generation algorithm in PACE specified by Part 11 of [ICAO-9303] and [TR-03111]* and specified cryptographic key sizes *128 bits and 256 bits* that meet the following: *Standards for session key generation in PACE specified by Part 11 of [ICAO-9303] and [TR-03111]*.

##### FCS\_CKM.1e Cryptographic key generation (PACE, ephemeral key pairs)

Hierarchical to: No other components.

Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_CKM.1.1e** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Elliptic Curve Key Pair Generation* and specified cryptographic key sizes *256 bits and 384 bits* that meet the following: *Standards for the key pair generation specified by [TR-03111]*.

#### FCS\_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the data with random numbers**<sup>5</sup> that meets the following: none.

#### FCS\_COP.1a Cryptographic operation (Active Authentication, signature generation)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1a** The TSF shall perform Generation of digital signature for Active Authentication data in accordance with a specified cryptographic algorithm ECDSA and cryptographic key sizes 256 bits and 384 bits that meet the following: the Digital Signature Standards specified by [TR-03111].

Application note: Only the combination of 256 bits and SHA-256 or that of 384 bits and SHA-384 is permitted as the key sizes for this requirement and the hash algorithm of FCS\_COP.1h.

#### FCS\_COP.1h Cryptographic operation (Active Authentication, hash functions)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1h** The TSF shall perform Generation of data for Active Authentication in accordance with a specified cryptographic algorithm SHA-256 and SHA-384 and cryptographic key sizes none that meet the following: the Digital Signature Standards specified by [TR-03111].

#### FCS\_COP.1hb Cryptographic operation (BAC, hash functions)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]

FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1hb** The TSF shall perform Generation of session keys used for BAC in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: Standards for session key generation in the Basic Access Control specified by Part 11 of [ICAO-9303].

#### FCS\_COP.1mb Cryptographic operation (BAC, mutual authentication)

Hierarchical to: No other components.

<sup>5</sup> [selection: method for erasing cryptographic keys on volatile memory by shutting down power supply, overwriting new cryptographic key data, and [assignment: other cryptographic key destruction method]]

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
 FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1mb** The TSF shall perform Cryptographic operation shown in Table 2 in accordance with a specified cryptographic algorithm Cryptographic algorithm shown in Table 2 and cryptographic key sizes Cryptographic key sizes shown in Table 2 that meet the following: Standards for mutual authentication included in the Basic Access Control specified by Part 11 of [ICAO-9303].

| Cryptographic algorithm | Cryptographic key sizes | Cryptographic operation  |
|-------------------------|-------------------------|--|
| Single DES in CBC mode  | 56 bits                 | Message Authentication Code and verification (excluding the final block of message)                        |
| Triple DES in CBC mode  | 112 bits                | Message encryption and decryption<br>Message Authentication Code and verification (final block of message) |

Table 2: Cryptographic mechanisms in Mutual authentication (BAC)

Application note: The Message Authentication Code generation process shown in Table 2 is equivalent to that specified by ISO/IEC 9797-1 MAC Algorithm3.

**FCS\_COP.1sb Cryptographic operation (BAC, Secure Messaging)**

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
 FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1sb** The TSF shall perform Cryptographic operation shown in Table 3 in accordance with a specified cryptographic algorithm Cryptographic algorithm shown in Table 3 and cryptographic key sizes Cryptographic key sizes shown in Table 3 that meet the following: Standards for Secure Messaging included in the Basic Access Control defined by Part 11 of [ICAO-9303].

| Cryptographic algorithm | Cryptographic key sizes | Cryptographic operation  |
|-------------------------|-------------------------|--|
| Single DES in CBC mode  | 56 bits                 | Message Authentication Code and verification (excluding the final block of message)                        |
| Triple DES in CBC mode  | 112 bits                | Message encryption and decryption<br>Message Authentication Code and verification (final block of message) |

Table 3: Cryptographic mechanisms in Secure Messaging (BAC)

Application notes:

- The Message Authentication Code generation process shown in Table 3 is equivalent to that specified by ISO/IEC 9797-1 MAC Algorithm3.
- Whether the Secure Messaging is applied or not depends on the type of commands. Therefore, not all commands and responses are assigned data encryption and Message Authentication Codes.



### FCS\_COP.1n Cryptographic operation (Nonce encryption)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1n** The TSF shall perform Nonce encryption in accordance with a specified cryptographic algorithm AES-CBC and cryptographic key sizes 128 bits and 256 bits that meet the following: Standards for the PACE procedure specified by Part 11 of [ICAO-9303].

### FCS\_COP.1e Cryptographic operation (Key agreement)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1e** The TSF shall perform Key agreement in accordance with a specified cryptographic algorithm ECDH and cryptographic key sizes 256 bits and 384 bits that meet the following: Standards for the PACE procedure specified by Part 11 of [ICAO-9303].

### FCS\_COP.1hp Cryptographic operation (PACE, hash functions)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1hp** The TSF shall perform Generation of session keys for PACE in accordance with a specified cryptographic algorithm SHA-1 and SHA-256 and cryptographic key sizes none that meet the following: Standards for session key generation in PACE specified by Part 11 of [ICAO-9303].

### FCS\_COP.1mp Cryptographic operation (PACE, mutual authentication)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1mp** The TSF shall perform Authentication token generation and verification in accordance with a specified cryptographic algorithm AES-CMAC and cryptographic key sizes 128 bits and 256 bits that meet the following: Standards for mutual authentication included in PACE specified by Part 11 of [ICAO-9303].

### FCS\_COP.1sp Cryptographic operation (PACE, Secure Messaging)

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes or FDP\_ITC.2 Import of user data with security attributes or FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

**FCS\_COP.1.1sp** The TSF shall perform Cryptographic operation shown in Table 4 in accordance with a specified cryptographic algorithm Cryptographic algorithm shown in Table 4 and cryptographic key sizes Cryptographic key sizes shown in Table 4 that meet the following: Standards for Secure Messaging included in PACE specified by [ICAO-9303].

| Cryptographic algorithm | Cryptographic key sizes | Cryptographic operation                                 |
|-------------------------|-------------------------|---|
| AES in CBC mode         | 128 bits and 256 bits   | Message encryption and decryption                       |
| AES-CMAC                | 128 bits and 256 bits   | Message Authentication Code generation and verification |

Table 4: Cryptographic mechanisms in Secure Messaging (PACE)

Application note: Whether the Secure Messaging is applied or not depends on the type of commands. Therefore, data encryption and message authentication codes are not necessarily applied to all commands and responses.

### FCS\_RND.1 Quality standards for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

**FCS\_RND.1.1** The TSF shall provide a random number generation mechanism that meets the following: [RGS-B1] and [SP800-90] with seed entropy of at least 128 bits<sup>6</sup>.

## 8.1.2 Class FDP: User Data Protection

### FDP\_ACC.1a Subset access control (Issuance procedure)

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

**FDP\_ACC.1.1a** The TSF shall enforce the Issuance procedure access control SFP on Subject [User process], Objects [Files shown in Table 1 of Organizational security policy P.Authority] and List of operations among subjects and objects addressed by SFP [Data Input/output operation to/from object].

### FDP\_ACC.1b Subset access control (BAC)

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

**FDP\_ACC.1.1b** The TSF shall enforce the BAC SFP on Subject [Process on behalf of terminal], Objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, basic access key file, password key file, transport key file, and private key file] and list of operations among subjects and objects addressed by SFP [Reading data from object].

Application note: BAC SFP is the access control policy applied after succeeding in mutual authentication based on BAC.

<sup>6</sup> [assignment: defined quality standard]

### FDP\_ACC.1p Subset access control (PACE)

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1 Security attribute based access control

**FDP\_ACC.1.1p** The TSF shall enforce the *PACE SFP* on Subject *[Process on behalf of terminal]*, Objects *[Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, password key file, transport key file, and private key file]* and *list of operations among subjects and objects addressed by SFP [Reading data from object]*.

Application note: PACE SFP is the access control policy applied after succeeding in mutual authentication based on PACE.

### FDP\_ACF.1a Security attribute based access control (Issuance procedure)

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1 Subset access control

FMT\_MSA.3 Static attribute initialisation

**FDP\_ACF.1.1a** The TSF shall enforce the *Issuance procedure access control SFP* to objects based on the following: *Subject controlled under the indicated SFP [User process], objects [Files shown in Table 1 of the organizational security policy P.Authority], and, the SFP-relevant security attributes [Authentication status shown in Table 1 of the organizational security policy P.Authority] according to each.*

**FDP\_ACF.1.2a** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *When the authentication status shown in Table 1 of the organizational security policy P.Authority is met, an operation to the file associated with the said authentication status is allowed.*

**FDP\_ACF.1.3a** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

**FDP\_ACF.1.4a** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *Access to files that are not listed in Table 1 of the organizational security policy P.Authority is prohibited.*

### FDP\_ACF.1b Security attribute based access control (BAC)

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1 Subset access control

FMT\_MSA.3 Static attribute initialisation

**FDP\_ACF.1.1b** The TSF shall enforce the *BAC SFP* to objects based on the following: *Subject controlled under the indicated SFP [Process on behalf of terminal], objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD, basic access key file, password key file, transport key file, and private key file], and the SFP-related security attributes [Authentication status of terminal based on mutual authentication].*

**FDP\_ACF.1.2b** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Where the authentication status of terminal has been successful, subjects are allowed to read data from objects.*

**FDP\_ACF.1.3b** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

**FDP\_ACF.1.4b** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *Subjects are prohibited to write data to or read data from the transport key file, basic access key file, password key file, and private key file.*

### FDP\_ACF.1p Security attribute based access control (PACE)

Hierarchical to: No other components.

|                     |  |
|---------------------|--|
| Dependencies:       | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation   |
| <b>FDP_ACF.1.1p</b> | The TSF shall enforce the <u>PACE SFP</u> to objects based on the following: <u>Subject controlled under the indicated SFP [Process on behalf of terminal], objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD password key file, transport key file, and private key file], and the SFP-related security attributes [Authentication status of terminal based on mutual authentication].</u> |
| <b>FDP_ACF.1.2p</b> | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <u>Where the authentication status of terminal has been successful, subjects are allowed to read data from objects.</u>  |
| <b>FDP_ACF.1.3p</b> | The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: <u>none.</u>   |
| <b>FDP_ACF.1.4p</b> | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <u>Subjects are prohibited to write data to or read data from the transport key file, password key file, and private key file.</u>  |

#### **FDP\_ITC.1 Import of user data without security attributes**

|                    |   |
|--------------------|---|
| Hierarchical to:   | No other components.  |
| Dependencies:      | [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]<br>FMT_MSA.3 Static attribute initialisation                         |
| <b>FDP_ITC.1.1</b> | The TSF shall enforce the <u>Issuance procedure access control SFP</u> when importing user data, controlled under the SFP, from outside of the TOE. |
| <b>FDP_ITC.1.2</b> | The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.                                      |
| <b>FDP_ITC.1.3</b> | The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: <u>none.</u>                      |

#### **FDP\_UCT.1b Basic data exchange confidentiality (BAC)**

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] |
| <b>FDP_UCT.1.1b</b> | The TSF shall enforce of <u>BAC SFP</u> to <u>transmit, receive</u> user data in a manner protected from unauthorized disclosure.                 |

#### **FDP\_UCT.1p Basic data exchange confidentiality (PACE)**

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | [FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]<br>[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] |
| <b>FDP_UCT.1.1p</b> | The TSF shall enforce of <u>PACE SFP</u> to <u>transmit, receive</u> user data in a manner protected from unauthorized disclosure.                |

#### **FDP\_UIT.1b Data exchange integrity (BAC)**

|                  |   |
|------------------|---|
| Hierarchical to: | No other components.  |
| Dependencies:    | [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path] |

|                     |  |
|---------------------|--|
| <b>FDP_UIT.1.1b</b> | The TSF shall enforce the <i>BAC SFP</i> to <i>transmit, receive</i> user data in a manner protected from <i>modification, deletion, insertion, replay</i> errors. |
| <b>FDP_UIT.1.2b</b> | The TSF shall be able to determine, on receipt of user data, whether <i>modification, deletion, insertion, replay</i> has occurred.                                |

#### FDP\_UIT.1p Data exchange integrity (PACE)

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path]                   |
| <b>FDP_UIT.1.1p</b> | The TSF shall enforce the <i>PACE SFP</i> to <i>transmit, receive</i> user data in a manner protected from <i>modification, deletion, insertion, replay</i> errors. |
| <b>FDP_UIT.1.2p</b> | The TSF shall be able to determine, on receipt of user data, whether <i>modification, deletion, insertion, replay</i> has occurred.                                 |

### 8.1.3 Class FIA: Identification and Authentication

#### FIA\_AFL.1a Authentication failure handling (Active Authentication Information Access Key)

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | FIA_UAU.1 Timing of authentication  |
| <b>FIA_AFL.1.1a</b> | The TSF shall detect when <b>three</b> <sup>7</sup> unsuccessful authentication attempts occur related to <i>Authentication with the Active Authentication Information Access Key</i> .   |
| <b>FIA_AFL.1.2a</b> | When the defined number of unsuccessful authentication attempts has been <i>met</i> , the TSF shall <i>permanently stop authentication with the Active Authentication Information Access Key (fix the authentication status with the Active Authentication Information Access Key to “Not authenticated yet”)</i> . |

#### FIA\_AFL.1d Authentication failure handling (Transport key)

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | FIA_UAU.1 Timing of authentication  |
| <b>FIA_AFL.1.1d</b> | The TSF shall detect when <b>three</b> <sup>8</sup> unsuccessful authentication attempts occur related to <i>Authentication with the transport key</i> .  |
| <b>FIA_AFL.1.2d</b> | When the defined number of unsuccessful authentication attempts has been <i>met</i> , the TSF shall <i>permanently stop authentication with the transport key (fix the authentication status with the transport key to “Not authenticated yet”)</i> . |

#### FIA\_AFL.1r Authentication failure handling (Readout key)

|                     |   |
|---------------------|---|
| Hierarchical to:    | No other components.  |
| Dependencies:       | FIA_UAU.1 Timing of authentication  |
| <b>FIA_AFL.1.1r</b> | The TSF shall detect when <b>three</b> <sup>9</sup> unsuccessful authentication attempts occur related to <i>Authentication with the readout key</i> .  |
| <b>FIA_AFL.1.2r</b> | When the defined number of unsuccessful authentication attempts has been <i>met</i> , the TSF shall <i>permanently stop authentication with the readout key (fix the authentication status with the readout key to “Not authenticated yet”)</i> . |

<sup>7</sup> [assignment: positive integer number]

<sup>8</sup> [assignment: positive integer number]

<sup>9</sup> [assignment: positive integer number]

**FIA\_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification

**FIA\_UAU.1.1** The TSF shall allow readout of EF.CardAccess and EF.ATR/INFO, on behalf of the user to be performed before the user is authenticated.

**FIA\_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**FIA\_UAU.4 Single-use authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_UAU.4.1** The TSF shall prevent reuse of authentication data related to mutual authentication mechanism with the BAC procedure and the PACE procedure.

**FIA\_UAU.5 Multiple authentication mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies

**FIA\_UAU.5.1** The TSF shall provide multiple authentication mechanisms shown in Table 5 to support user authentication.

**FIA\_UAU.5.2** The TSF shall authenticate any user's claimed identity according to the rules describing how the multiple authentication mechanisms shown in Table 5 provide authentication.

| Authentication mechanism name                | Rule applicable to authentication mechanism   |
|--|---|
| Transport key                                | Rule of authenticating the authorized personnel of the passport issuing authorities by verifying transport key that have been already stored in the TOE.  |
| Readout key                                  | Rule of authenticating the authorized personnel of the passport issuing authorities by verification with readout key that have been already stored in the TOE.                                  |
| Active Authentication Information Access Key | Rule of authenticating the authorized personnel of the passport issuing authorities by verification with Active Authentication Information Access Key that have been already stored in the TOE. |
| Mutual authentication                        | Rule of authenticating terminals according to the mutual authentication procedure in BAC and PACE defined by [ICAO-9303].   |

Table 5: Multiple authentication mechanisms

**FIA\_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FIA\_UID.1.1** The TSF shall allow readout of EF.CardAccess and EF.ATR/INFO, on behalf of the user to be performed before the user is identified.

**FIA\_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

## 8.1.4 Class FMT: Security management

### FMT\_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.  
 Dependencies: FMT\_SMR.1 Security roles  
 FMT\_SMF.1 Specification of management functions

**FMT\_MOF.1.1** The TSF shall restrict the ability to *disable, enable* the functions *Basic access control* to *the authorized personnel of the passport issuing authorities*.

### FMT\_MTD.1 Management of TSF data

Hierarchical to: No other components.  
 Dependencies: FMT\_SMR.1 Security roles  
 FMT\_SMF.1 Specification of management functions

**FMT\_MTD.1.1** The TSF shall restrict the ability to *modify* the *transport key* to *the authorized personnel of the passport issuing authorities*.

Application note: This requirement has to do with the configuration of transport key used to transport the TOE from the passport booklet manufacturer to a regional passport office in Phase 3. In this requirement, the authorized personnel who are allowed to manage TSF data are the staff of the passport manufacturer. The staff has no chance to rewrite the transport key after the TOE has been transported to the regional passport office. On the other hand, when the TOE is located in either the passport manufacturer or a regional passport office, there is also no threat that an attacker illicitly rewrites the transport key. Therefore, there is no necessity to distinguish between the staff of the passport manufacturer and that of the regional passport office. For this reason, this requirement makes no particular distinction between them and refers the authorized administrator as the “authorized personnel of the passport issuing authorities.”

### FMT\_SMF.1 Specification of management functions

Hierarchical to: No other components.  
 Dependencies: No dependencies.

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions: *modification of transport key and disabling the BAC function*.

### FMT\_SMR.1 Security roles

Hierarchical to: No other components.  
 Dependencies: FIA\_UID.1 Timing of identification

**FMT\_SMR.1.1** The TSF shall maintain the roles *authorized personnel of the passport issuing authorities*.

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

## 8.1.5 Class FPT: Protection of the TSF

### FPT\_PHP.3 Resistance to physical attack

Hierarchical to: No other components.  
 Dependencies: No dependencies.

**FPT\_PHP.3.1** The TSF shall resist *attacks defined by the CC Supporting Documents related to Smartcards to the hardware of the TOE and software composing the TSF* by responding automatically such that the SFRs are always enforced.

Application note: The supporting documents that are the latest version at the time of the evaluation for the TOE are applied. The document at the time of PP issuance is the “Application of Attack Potential to Smartcards, Version 2.9, May 2013.”

### 8.1.6 Class FTP: Trusted paths / Channels

#### FTP\_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTP\_ITC.1.1** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of channel data from modification or disclosure.

**FTP\_ITC.1.2** The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for *reading data from the TOE*.

Application note: Communication between terminal and TSF shall be performed via the Secure Messaging channel defined by [ICAO-9303]. After the Secure Messaging channel is established, only the Secure Messaging channel is to be available for the communication path between terminal and TOE.

## 8.2 SECURITY ASSURANCE REQUIREMENTS

This ST is based on the EAL4 assurance package augmented with the components ADV\_FSP.5, ADV\_INT.2, ADV\_TDS.4, ALC\_CMS.5, ALC\_DVS.2, ALC\_TAT.2 and ATE\_DPT.3.

The corresponding Security Assurance Components can be split in three subset packages, all being required to meet TOE assurance requirements:

- **ASE package:** ASE\_INT.1, ASE\_CCL.1, ASE\_ECD.1, ASE\_SPD.1, ASE\_OBJ.2, ASE\_REQ.2, ASE\_TSS.1
- **Assurance package for passport product**

| Assurance package for smartcard product |   |
|---|---|
| Assurance Class                         | Assurance Components – Product related                |
| ADV                                     | ADV_FSP.5, ADV_INT.2, ADV.TDS.4, ADV_IMP.1, ADV_ARC.1 |
| AGD                                     | AGD_OPE.1   |
| ALC                                     | ALC_CMS.5   |
| ATE                                     | ATE_COV.2, ATE_DPT.3, ATE_FUN.1, ATE_IND.2            |
| AVA                                     | AVA_VAN.3   |



- Assurance package for development process and lifecycle coverage

| Assurance package for development process and lifecycle coverage |  |
|--|--|
| Assurance Class  | Assurance Components – Process related                               |
| AGD  | AGD_PRE.1  |
| ALC  | ALC_CMC.4, ALC_DEL.1, <b>ALC_DVS.2</b> , ALC_LCD.1, <b>ALC_TAT.2</b> |

### 8.3 SECURITY REQUIREMENTS RATIONALE

#### 8.3.1 SFR rationale – Coverage with the TOE security objectives

|             | O.Logical_Attack | O.Physical_Attack | O.AA | O.BAC | O.PACE | O.Authority | O.Data_Lock | O.Disable_BAC |
|-------------|------------------|-------------------|------|-------|--------|-------------|-------------|---------------|
| FCS_CKM.1b  |                  |                   |      | X     |        |             |             |               |
| FCS_CKM.1p  |                  |                   |      |       | X      |             |             |               |
| FCS_CKM.1e  |                  |                   |      |       | X      |             |             |               |
| FCS_CKM.4   |                  |                   | X    | X     | X      |             |             |               |
| FCS_COP.1a  |                  |                   | X    |       |        |             |             |               |
| FCS_COP.1h  |                  |                   | X    |       |        |             |             |               |
| FCS_COP.1hb |                  |                   |      | X     |        |             |             |               |
| FCS_COP.1mb |                  |                   |      | X     |        |             |             |               |
| FCS_COP.1sb |                  |                   |      | X     |        |             |             |               |
| FCS_COP.1n  |                  |                   |      |       | X      |             |             |               |
| FCS_COP.1e  |                  |                   |      |       | X      |             |             |               |
| FCS_COP.1hp |                  |                   |      |       | X      |             |             |               |
| FCS_COP.1mp |                  |                   |      |       | X      |             |             |               |
| FCS_COP.1sp |                  |                   |      |       | X      |             |             |               |
| FCS_RND.1   |                  |                   |      |       | X      |             |             |               |
| FDP_ACC.1a  |                  |                   | X    |       |        | X           |             |               |
| FDP_ACC.1b  | X                |                   |      | X     |        |             |             |               |
| FDP_ACC.1p  | X                |                   |      |       | X      |             |             |               |
| FDP_ACF.1a  |                  |                   | X    |       |        | X           |             |               |
| FDP_ACF.1b  | X                |                   |      | X     |        |             |             |               |
| FDP_ACF.1p  | X                |                   |      |       | X      |             |             |               |

|            |  |   |   |   |   |   |   |   |
|------------|--|---|---|---|---|---|---|---|
| FDP_ITC.1  |  |   | X | X | X | X |   |   |
| FDP_UCT.1b |  |   |   | X |   |   |   |   |
| FDP_UCT.1p |  |   |   |   | X |   |   |   |
| FDP_UIT.1b |  |   |   | X |   |   |   |   |
| FDP_UIT.1p |  |   |   |   | X |   |   |   |
| FIA_AFL.1a |  |   |   |   |   |   | X |   |
| FIA_AFL.1d |  |   |   |   |   |   | X |   |
| FIA_AFL.1r |  |   |   |   |   |   | X |   |
| FIA_UAU.1  |  |   |   | X | X | X |   | X |
| FIA_UAU.4  |  |   |   | X | X |   |   |   |
| FIA_UAU.5  |  |   |   | X | X | X |   | X |
| FIA_UID.1  |  |   |   | X | X | X |   | X |
| FMT_MOF.1  |  |   |   |   |   |   |   | X |
| FMT_MTD.1  |  |   |   |   |   | X |   |   |
| FMT_SMF.1  |  |   |   |   |   | X |   | X |
| FMT_SMR.1  |  |   |   |   |   | X |   | X |
| FPT_PHP.3  |  | X |   |   |   |   |   |   |
| FPT_ITC.1  |  |   |   | X | X |   |   |   |

### 8.3.2 SFR rationale sufficiency

| TOE Security Objective | Rationale   |
|------------------------|---|
| O.AA                   | To achieve the security objective O.AA, it shall address the Active Authentication procedure defined by Part 11 of [ICAO-9303]. This Active Authentication is a process for a terminal to authenticate the IC chip of the TOE, and the TOE itself is not required to provide any authentication mechanism. The TOE is authenticated by properly responding the authentication procedure. To meet requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair, performs cryptographic operation using the private key defined by FCS_COP.1a, and hashing operation defined by FCS_COP.1h. The public key and private key pair is imported to the TOE by FDP_ITC.1. Access control associated with FDP_ITC.1 is defined by FDP_ACC.1a and FDP_ACF.1a. Destruction of the private key on RAM is defined by FCS_CKM.4. The security objective O.AA is sufficiently achieved by the said SFRs. |
| O.Logical_Attack       | Confidential information (Active Authentication Private Key) subject to protection is stored in the private key file of the TOE. It is denied for the user process on behalf of the terminal to read data from the private key file, by FDP_ACC.1p and FDP_ACF.1p applied to the TOE after issuing the TOE embedded passport. The security objective O.Logical_Attack is sufficiently achieved by the said SFRs.  |
| O.Physical_Attack      | Attack scenarios trying to disclose the Active Authentication Private Key that is confidential information, and to tamper security-related information within the TOE, by physical means are stated in the list of attacks shown in the FPT_PHP.3 section. The TSF automatically resists the attacks according to FPT_PHP.3 to protect against the disclosure of the confidential information. With that, the security objective O.Physical_Attack is sufficiently achieved.  |

|                           |   |
|---------------------------|---|
| <p><b>O.BAC</b></p>       | <p>The TOE provides its services to the user (equivalent to a terminal) who has succeeded in identification and authentication by FIA_UID.1 and FIA_UAU.1. User authentication requires the mutual authentication procedure with the BAC defined by ICAO, which is defined by FIA_UAU.5. This mutual authentication procedure requires new authentication data based on random numbers for each authentication, which is defined by FIA_UAU.4. Likewise, Secure Messaging required by BAC is defined by the requirement for the protection of transmitted and received data by FDP_UCT.1b and FDP_UIT.1b, and the requirement of cryptographic communication channels by FTP_ITC.1. Furthermore, with regard to cryptographic processing required for the BAC procedure, FCS_COP.1mb defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1sb defines cryptographic operations for Secure Messaging. With regard to the cryptographic keys used for Secure Messaging, FDP_ITC.1 defines the import of basic access keys, FCS_CKM.1b and FCS_COP.1hb define the generation of session keys, and FCS_CKM.4 defines the destruction of these keys. In order for only permitted personnel to read given information from the TOE, rules governing access control with FDP_ACC.1b and FDP_ACF.1b are defined. The security objective O.BAC is sufficiently achieved by the said SFRs.</p>  |
| <p><b>O.PACE</b></p>      | <p>The TOE provides its services to the user who has succeeded in identification and authentication by FIA_UID.1 and FIA_UAU.1. User authentication requires the mutual authentication procedure with PACE defined by ICAO, which is defined by FIA_UAU.5. The mutual authentication procedure requires new authentication data based on a random number for each authentication, which is defined by FIA_UAU.4. Likewise, Secure Messaging required by PACE is defined by the requirements for the protection of transmitted and received data by FDP_UCT.1p and FDP_UIT.1p, and the requirement of cryptographic communication channels by FTP_ITC.1. Furthermore, with regard to cryptographic processing required for the PACE procedure, FCS_COP.1mp defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1sp defines cryptographic operations for Secure Messaging. With regard to the cryptographic keys used for Secure Messaging, FDP_ITC.1 defines the import of password key, FCS_CKM.1e defines the generation of ephemeral key pairs, FCS_COP.1e defines the key agreement, FCS_CKM.1p and FCS_COP.1hp define the generation of session keys, FCS_RND.1 defines the generation of random numbers such as random Nonce, FCS_COP.1n defines the encryption of Nonce, and FCS_CKM.4 defines the destruction of these keys. In order for only permitted personnel to read given information from the TOE, rules governing access control with FDP_ACC.1p and FDP_ACF.1p are defined. O.PACE is sufficiently achieved by the said SFRs.</p> |
| <p><b>O.Authority</b></p> | <p>During the TOE process done by the passport issuing authorities, the identification and authentication requirements FIA_UID.1 and FIA_UAU.1 are applied in order to grant the processing authority only to the duly authorized user. As for the user authentication mechanisms, FIA_UAU.5 defines the use of the transport key, readout key, or Active Authentication Information Access Key. If a user is successfully authenticated by the verification with the key, the user is permitted to access to the internal data of the TOE defined by O.Authority, applying the access control rule FDP_ACC.1a and FDP_ACF.1a. The user operation includes writing of the authentication key (transport key), cryptographic keys (Active Authentication Public Key and private key pair, basic access key and password key for Secure Messaging), and other user data in the TOE. The association between objects and security attributes when writing is defined by FDP_ITC.1. O.Authority includes updating (rewriting) of the transport keys by the authorized personnel of the passport issuing authorities and is defined by FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. The security objective O.Authority is sufficiently achieved by the said SFRs.</p>  |

|                      |  |
|----------------------|--|
| <b>O.Data_Lock</b>   | In the event of an authentication failure with the transport key, readout key or Active Authentication Information Access Key, authentication corresponding to the relevant key is permanently prohibited, and as the result, the security objective of permanently prohibiting readout and write of the internal data of the TOE is sufficiently achieved by the three SFRs: FIA_AFL.1a, FIA_AFL.1d, and FIA_AFL.1r.  |
| <b>O.Disable_BAC</b> | During the TOE process done by the passport issuing authorities, the identification and authentication requirements FIA_UID.1 and FIA_UAU.1 are applied in order to grant the processing authority only to the duly authorized user. It is allowed to disable the BAC function, which is defined by FMT_MOF.1, FMT_SMF.1, and FMT_SMR.1, for the user that has been succeeded in authentication by verification with the transport key by FIA_UAU.5. The security objective O.Disable_BAC is sufficiently achieved by the said SFRs. |

### 8.3.3 SFR dependency rationale

The following table shows dependencies and support for the dependencies defined for SFRs. In the table, the Dependencies column describes dependencies defined for SFRs, and the Support for the Dependencies column describes by what SFRs the defined dependencies are satisfied or rationales indicating the justification for non-satisfied dependencies.

| SFR         | Dependencies  | Support for the Dependencies   |
|-------------|---|--|
| FCS_CKM.1b  | [FCS_CKM.2 or FCS_COP.1]<br>FCS_CKM.4                 | FCS_COP.1sb and FCS_CKM.4 support to satisfy the dependencies.   |
| FCS_CKM.1p  | [FCS_CKM.2 or FCS_COP.1]<br>FCS_CKM.4                 | FCS_COP.1sp, FCS_COP.1mp, and FCS_CKM.4 support to satisfy the dependencies.   |
| FCS_CKM.1e  | [FCS_CKM.2 or FCS_COP.1]<br>FCS_CKM.4                 | FCS_COP.1e and FCS_CKM.4 support to satisfy the dependencies.  |
| FCS_CKM.4   | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]              | FDP_ITC.1, FCS_CKM.1b, FCS_CKM.1e, and FCS_CKM.1p support to satisfy the dependency. FDP_ITC.1 supports keys only on volatile memory.  |
| FCS_COP.1a  | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FDP_ITC.1 supports. FCS_CKM.4 supports keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.    |
| FCS_COP.1h  | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | Since keys do not exist, any requirements do not apply to.   |
| FCS_COP.1hb | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | Since keys do not exist, any requirements do not apply to.   |
| FCS_COP.1mb | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FDP_ITC.1 supports. FCS_CKM.4 supports keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.    |
| FCS_COP.1sb | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1b and FCS_CKM.4 support to satisfy the dependencies.  |
| FCS_COP.1n  | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FDP_ITC.1 supports. FCS.CKM.4 supports on keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to. |
| FCS_COP.1e  | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1e and FCS_CKM.4 support to satisfy the dependencies.  |
| FCS_COP.1hp | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]<br>FCS_CKM.4 | Since keys do not exist, any requirements do not apply to.   |
| FCS_COP.1mp | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1]              | FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.  |

|             |  |  |
|-------------|--|--|
|             | FCS_CKM.4  |  |
| FCS_COP.1sp | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]<br>FCS_CKM.4   | FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.  |
| FCS_RND.1   | No dependencies                                      | N/A  |
| FDP_ACC.1a  | FDP_ACF.1  | FDP_ACF.1a supports to satisfy the dependency.   |
| FDP_ACC.1b  | FDP_ACF.1  | FDP_ACF.1b supports to satisfy the dependency.   |
| FDP_ACC.1p  | FDP_ACF.1  | FDP_ACF.1p supports to satisfy the dependency.   |
| FDP_ACF.1a  | FDP_ACC.1<br>FMT_MSA.3                               | FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to. |
| FDP_ACF.1b  | FDP_ACC.1<br>FMT_MSA.3                               | FDP_ACC.1b supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to. |
| FDP_ACF.1p  | FDP_ACC.1<br>FMT_MSA.3                               | FDP_ACC.1p supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to. |
| FDP_ITC.1   | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_MSA.3                | FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to. |
| FDP_UCT.1b  | [FTP_ITC.1 or FTP_TRP.1]<br>[FDP_ACC.1 or FDP_IFC.1] | FTP_ITC.1 and FDP_ACC.1b support to satisfy the dependencies.  |
| FDP_UCT.1p  | [FTP_ITC.1 or FTP_TRP.1]<br>[FDP_ACC.1 or FDP_IFC.1] | FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.  |
| FDP_UIT.1b  | [FDP_ACC.1 or FDP_IFC.1]<br>[FTP_ITC.1 or FTP_TRP.1] | FTP_ITC.1 and FDP_ACC.1b support to satisfy the dependencies.  |
| FDP_UIT.1p  | [FDP_ACC.1 or FDP_IFC.1]<br>[FTP_ITC.1 or FTP_TRP.1] | FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.  |
| FIA_AFL.1a  | FIA_UAU.1  | FIA_UAU.1 supports to satisfy the dependency.  |
| FIA_AFL.1d  | FIA_UAU.1  | FIA_UAU.1 supports to satisfy the dependency.  |
| FIA_AFL.1r  | FIA_UAU.1  | FIA_UAU.1 supports to satisfy the dependency.  |
| FIA_UAU.1   | FIA_UID.1  | FIA_UID.1 supports to satisfy the dependency.  |
| FIA_UAU.4   | No dependencies                                      | N/A  |
| FIA_UAU.5   | No dependencies                                      | N/A  |
| FIA_UID.1   | No dependencies                                      | N/A  |
| FMT_MOF.1   | FMT_SMR.1<br>FMT_SMF.1                               | FMT_SMR.1 and FMT_SMF.1 support to satisfy the dependencies.   |
| FMT_MTD.1   | FMT_SMR.1<br>FMT_SMF.1                               | FMT_SMR.1 and FMT_SMF.1 support to satisfy the dependencies.   |
| FMT_SMF.1   | No dependencies                                      | N/A  |
| FMT_SMR.1   | FIA_UID.1  | FIA_UID.1 supports to satisfy the dependency.  |
| FPT_PHP.3   | No dependencies                                      | N/A  |
| FTP_ITC.1   | No dependencies                                      | N/A  |

### 8.3.4 Security Assurance Requirements Rationale

In environments that the TOE is used, communication with inspection terminals that the BAC procedure is used for is assumed. The BAC procedure is assumed to thwart attackers possessing an Enhanced-Basic attack potential, and AVA\_VAN.3 is adopted as the security assurance requirement for the vulnerability assessment of the TOE to assure that it can counter such level of the attack. In addition, ALC\_DVS.2 is adopted as the development security assurance requirement to provide stricter protection of development information used for an attack means.

When using the IC chip as the TOE, state of the art technologies are required for SFRs and design methods to realize such SFRs. However, there are no significant variations in the security functionality of product, and points to be checked for the vulnerability assessment are also well-defined. Consequently, EAL4, which is the top level for commercial product but does not require stringency as high as that for EAL5 whose target application is military use, is adopted as the development and manufacturing assurance requirements except development security.

The following augmentations have also been considered for the present evaluation since the related documentation is already fulfilling the corresponding requirements: ADV\_FSP.5, ADV\_INT.2, ADV\_TDS.4, ALC\_CMS.5, ALC\_DVS.2, ALC\_TAT.2 and ATE\_DPT.3.

Note that the dependencies among these augmented security assurance components are all satisfied.

### 8.4 COMPOSITION TASKS – SFR PART

The following table (see next page) lists the SFRs that are declared in the [ST\_IC] security target, and separates them in relevant platform<sup>10</sup>-SFRs (RP\_SFR-SERV and RP\_SFR-MECH) and irrelevant platform-SFRs (IP\_SFR), as requested in [CCDB]. The table also provides the link between the relevant platform-SFRs and the composite product SFRs.

---

<sup>10</sup> In the present ST, the platform is the SLC52GDA chip.

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Platform-SFR      | Platform-SFR content  | Platform-SFR additional information | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs   |
|-------------------|---|-------------------------------------|-------------|-------------|--------|--|
| FAU_SAS.1         | The TSF shall provide the test process before TOE Delivery with the capability to store the Initialization Data (GCIM) and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software in the not changeable configuration page area and non-volatile memory. | None                                | X           |             |        | No link to TOE SFRs but used for the composite-product identification. |
| FCS_CKM.1 /RSA    | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [...]   | None                                |             |             | X      | Not used by the composite TOE.   |
| FCS_CKM.1 / EC    | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [...]   | None                                |             |             | X      | Not used by the composite TOE.   |
| FCS_COP.1 / TDES  | The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm TDES [...]   | None                                | X           |             |        | FCS_COP.1mb<br>FCS_COP.1sb   |
| FCS_CKM.4 / TDES  | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting or zeroing that meets the following: none.   | None                                | X           |             |        | FCS_CKM.4  |
| FCS_COP.1 / AES   | The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES [...]  | None                                | X           |             |        | FCS_COP.1n<br>FCS_COP.1mp<br>FCS_COP.1sp                               |
| FCS_CKM.4 / AES   | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting or zeroing that meets the following: none.   | None                                | X           |             |        | FCS_CKM.4  |
| FCS_COP.1 / RSA   | The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) [...]  | None                                |             |             | X      | Not used by the composite TOE.   |
| FCS_COP.1 / ECDSA | The TSF shall perform signature generation and signature verification in accordance with a specified cryptographic algorithm ECDSA [...]  | None                                |             |             | X      | Not used by the composite TOE.   |
| FCS_COP.1 / ECDH  | The TSF shall perform elliptic curve Diffie-Hellman key agreement in accordance with a specified cryptographic algorithm ECDH [...]   | None                                |             |             | X      | Not used by the composite TOE.   |
| FCS_RNG.1/T RNG   | Random numbers generation Class PTG.2<br>The TSF shall provide a physical random number generator that implements [...]   | None                                | X           |             |        | FCS_RND.1  |
| FCS_RNG.1/H PRG   | Random numbers generation Class PTG.3   | None                                |             |             | X      | Not used by the composite TOE.   |

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Platform-SFR    | Platform-SFR content   | Platform-SFR additional information   | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs                 |
|-----------------|--|---|-------------|-------------|--------|--|
|                 | The TSF shall provide a hybrid physical random number generator that implements [...]  |   |             |             |        |  |
| FCS_RNG.1/D RNG | Random numbers generation Class DRG.3<br>The TSF shall provide a deterministic random number generator that implements [...]   | None  |             |             | X      | Not used by the composite TOE.         |
| FCS_RNG.1/K SG  | Random numbers generation Class DRG.2<br>The TSF shall provide a deterministic random number generator that implements [...]   | None  |             |             | X      | Not used by the composite TOE.         |
| FDP_ACC.1       | The TSF shall enforce the Memory Access Control Policy on all subjects (software running at the defined and assigned privilege levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. privilege levels.  |   | X           |             |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b |
| FDP_ACF.1       | <p>The TSF shall enforce the Memory Access Control Policy to objects based on the following:</p> <p>Subject:</p> <ul style="list-style-type: none"> <li>- Software running at the IFX, OS1 and OS2 privilege levels required to securely operate the chip. This includes also privilege levels running interrupt routines.</li> <li>- software running at the privilege levels containing the application software</li> </ul> <p>Object:</p> <ul style="list-style-type: none"> <li>- data including code stored in memories</li> </ul> <p>Attributes:</p> <ul style="list-style-type: none"> <li>- the memory area where the access is performed to and/or</li> <li>- the operation to be performed.</li> </ul> <p>The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: evaluate the corresponding permission control information of the relevant memory range before and during</p> | <p><b>Memory Access Control Policy</b></p> <p>The TOE shall control read, write, delete and execute accesses of software running at the privilege levels as defined below. Any access is controlled, regardless whether the access is on code or data or a jump on any other privilege level outside the current one.</p> |             |             |        | FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b |



| Platform-SFR | Platform-SFR content   | Platform-SFR additional information | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs   |
|--------------|--|-------------------------------------|-------------|-------------|--------|--|
|              | the access so that accesses to be denied cannot be utilized by the subject attempting to perform the operation.  |                                     |             |             |        |  |
| FMT_MSA.1    | The TSF shall enforce the Memory Access Control Policy to restrict the ability to change default, modify or delete the security attributes permission control information to the software running on the privilege levels.   |                                     |             |             | X      | Not used by the composite TOE.   |
| FMT_MSA.3    | The TSF shall enforce the Memory Access Control Policy to provide well-defined default values for security attributes that are used to enforce the SFP.<br><br>The TSF shall allow any subject, provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed, to specify alternative initial values to override the default values when an object or information is created. |                                     |             |             | X      | Not used by the composite TOE.   |
| FMT_SMF.1    | The TSF shall be capable of performing the following security management functions: access the configuration registers of the MMU.   |                                     | X           |             |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b<br>FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b |
| FDP_SDI.1    | The TSF shall monitor user data of the Composite TOE stored in containers controlled by the TSF for inconsistencies between stored data and corresponding EDC on all objects, based on the following attributes: EDC value for the RAM, ROM and SOLID FLASH NVM.   | None                                |             | X           |        | FPT_PHP.3  |
| FDP_SDI.2    | The TSF shall monitor user data of the composite TOE stored in containers controlled by the TSF for data integrity and one- and/or more-bit-errors on all objects, based on the following attributes: corresponding EDC value for RAM,   | None                                |             | X           |        | FPT_PHP.3  |

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Platform-SFR | Platform-SFR content  | Platform-SFR additional information   | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs  |
|--------------|---|---|-------------|-------------|--------|---|
|              | ROM and SOLID FLASH NVM and error correction ECC for the SOLID FLASH NVM.<br><br>Upon detection of a data integrity error, the TSF shall correct 1 bit errors in the SOLID FLASH NVM automatically and inform the user about more bit errors.                     |   |             |             |        |   |
| FDP_IFC.1    | The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.  | <b>Data Processing Policy</b><br><br>User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software. |             | X           |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b<br>FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b<br>FPT_PHP.3 |
| FDP_ITT.1    | The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.   |   |             | X           |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b<br>FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b<br>FPT_PHP.3 |
| FPT_ITT.1    | The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.<br><br>The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE. |   |             | X           |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b<br>FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b<br>FPT_PHP.3 |
| FMT_LIM.1    | The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Limited capability and availability Policy.                                 | <b>Limited capability and availability Policy</b>   | X           |             |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b  |

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Platform-SFR       | Platform-SFR content  | Platform-SFR additional information  | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs  |
|--------------------|---|--|-------------|-------------|--------|---|
|                    |   | Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks. |             |             |        | FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b  |
| FMT_LIM.2          | The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: Limited capability and availability Policy.   |  | X           |             |        | FDP_ACC.1a<br>FDP_ACC.1p<br>FDP_ACC.1b<br>FDP_ACF.1a<br>FDP_ACF.1p<br>FDP_ACF.1b  |
| FPT_FLS.1          | <b>Failure with preservation of secure state:</b> The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.   | None   | X           |             |        | FPT_PHP.3   |
| FRU_FLT.2          | <b>Limited fault tolerance:</b> The TSF shall ensure the operation of all the TOE’s capabilities when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).   | None   | X           |             |        | FPT_PHP.3   |
| FPT_PHP.3          | The TSF shall resist physical manipulation and physical probing, to the TSF by responding automatically such that the SFRs are always enforced.   | None   | X           |             |        | FPT_PHP.3   |
| FPT_TST.2          | The TSF shall run a suite of self-tests at the request of the authorized user to demonstrate the correct operation of the alarm lines and/or following environmental sensor mechanisms: [...]   | None   | X           |             |        | FPT_PHP.3   |
| FDP_SDC.1          | The TSF shall ensure the confidentiality of the information of the user data of the Composite TOE while it is stored in the RAM, ROM, Cache and SOLID FLASH NVM.  | None   |             | X           |        | FDP_ACC.1a, FDP_ACC.1p<br>FDP_ACC.1b, FDP_ACF.1a<br>FDP_ACF.1p, FDP_ACF.1b<br>FPT_PHP.3   |
| FMT_LIM.1 / Loader | The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Loader functionality after permanent deactivation does not allow stored user data of the Composite TOE to be disclosed or manipulated by unauthorized user. | None   |             | X           |        | Essential to the security of the Composite TOE as the IC Loader shall not be re-activated by an attacker to bypass the composite TOE SFRs |

eTravel Essential for Japan 1.0, with SAC (BAC+PACE) and AA – Security Target

| Platform-SFR       | Platform-SFR content   | Platform-SFR additional information | RP_SFR-SERV | RP_SFR-MECH | IP_SFR | Composite product SFRs  |
|--------------------|--|-------------------------------------|-------------|-------------|--------|---|
| FMT_LIM.2 / Loader | The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: The TSF prevents deploying the Loader functionality after permanent deactivation.      | None                                |             | X           |        |   |
| FIA_API.1 (Loader) | The TSF shall provide an authentication mechanism according to [...] Three path authentication based on the security attributes (keys) Kc or Kd.   | None                                |             | X           |        | Participates to the security of the eTravel for Japan Embedded Software loading within the IC.                              |
| FTP_ITC.1 (Loader) | The TSF shall provide a communication channel between itself and the administrator user [...]  | None                                |             |             | X      | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |
| FDP_UCT.1 (Loader) | The TSF shall enforce the Loader SFP to receive user data in a manner protected from unauthorized disclosure.  | None                                |             |             | X      | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |
| FDP_UIT.1 (Loader) | The TSF shall enforce the Loader SFP to receive user data in a manner protected from modification, deletion or insertion errors.<br>The TSF shall be able to determine on receipt of user data, whether modification, deletion or insertion have occurred. | None                                |             |             | X      | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |
| FDP_ACC.1 / Loader | The TSF shall enforce the Loader SFP [...]   | None                                |             |             | X      | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |
| FDP_ACF.1 / Loader | The TSF shall enforce the Loader SFP to objects based on the following [...]   | None                                |             |             | X      | Initially coming from the optional Package 2 in [PP/0084]. Not relevant here as the Loader is deactivated prior to Phase 7. |

## 9. TOE SUMMARY SPECIFICATION

### 9.1 CRYPTOGRAPHY

#### 9.1.1 Cryptographic key generation

|  |  |
|--|--|
| Session key generation for BAC         | The TOE generates session keys for BAC as specified in [ICAO-9303] part 11. Related key length is 112 bits.                              |
| Session key generation for PACE        | The TOE generates session keys for PACE as specified in [ICAO-9303] part 11 and [TR-03111]. Related key length is 128 bits and 256 bits. |
| Ephemeral key pair generation for PACE | The TOE generates Elliptic Curve key pairs for PACE as specified in [TR-03111]. Related key length is 256 bits and 384 bits.             |

#### 9.1.2 Cryptographic key destruction

The TSF destroys cryptographic keys by overwriting the data with random numbers.

#### 9.1.3 Cryptographic operations

|   |   |
|---|---|
| Cryptographic operations related to Active Authentication | <p>The TOE performs ECDSA digital signature generation for Active Authentication data as specified in [TR-03111]. Related key length are 256 bits and 384 bits.</p> <p>The TOE generates data for Active Authentication using the SHA-256 and SHA-384 algorithms as specified in [TR-03111].</p>  |
| Cryptographic operations related to BAC                   | <p>The TOE generates session keys used for BAC using the SHA-1 algorithm as specified in Part 11 of [ICAO-9303].</p> <p>The TOE handles mutual authentication for BAC through the following cryptographic operations, as specified in Part 11 of [ICAO-9303]:</p> <ul style="list-style-type: none"> <li>▪ Message Authentication Code and verification (excluding the final block of message) using Single DES in CBC mode, with 56 bits key length.</li> <li>▪ Message encryption and decryption, and Message Authentication Code and verification (final block of message) using Triple DES in CBC mode, with 112 bits key length.</li> </ul> <p>The TOE handles Secure Messaging for BAC through the following cryptographic operations, as specified in Part 11 of [ICAO-9303]:</p> <ul style="list-style-type: none"> <li>▪ Message Authentication Code and verification (excluding the final block of message) using Single DES in CBC mode, with 56 bits key length.</li> <li>▪ Message encryption and decryption, and Message Authentication Code and verification (final block of message) using Triple DES in CBC mode, with 112 bits key length.</li> </ul> |
| Cryptographic operations related to PACE                  | <p>The TOE performs Nonce encryption using the AES-CBC algorithm, with 128 bits and 256 bits key length, as specified in Part 11 of [ICAO-9303].</p> <p>The TOE performs Key agreement using the ECDH algorithm, with 256 bits and 384 bits key length, as specified in Part 11 of [ICAO-9303].</p> <p>The TOE generates session keys for PACE using the SHA-1 and SHA-256 algorithms as specified by Part 11 of [ICAO-9303].</p> <p>The TOE handles mutual authentication for PACE by performing authentication token generation and verification using the AES-CMAC algorithm, with 128 bits and 256 bits key length, as specified by Part 11 of [ICAO-9303].</p>   |

|  |   |
|--|---|
|  | <p>The TOE handles Secure Messaging for PACE through the following cryptographic operations, as specified in [ICAO-9303]:</p> <ul style="list-style-type: none"> <li>▪ Message encryption and decryption using AES in CBC mode, with 128 bits and 256 bits key length.</li> <li>▪ Message Authentication Code generation and verification using AES-CMAC, with 128 bits and 256 bits key length.</li> </ul> |
|--|---|

#### 9.1.4 Generation of random numbers

The TOE provides a random number generation mechanism that meets the following quality standards: [RGS-B1] and [SP800-90] with seed entropy of at least 128 bits.

## 9.2 IDENTIFICATION AND AUTHENTICATION

### 9.2.1 Supported authentication mechanisms

The authentication mechanisms which are supported by the TOE, as well as the corresponding rules enforced to verify the identity of the users, are described in the following table:

| Authentication mechanism name                | Rule applicable to authentication mechanism   |
|--|---|
| Transport key                                | Rule of authenticating the authorized personnel of the passport issuing authorities by verifying transport key that have been already stored in the TOE.  |
| Readout key                                  | Rule of authenticating the authorized personnel of the passport issuing authorities by verification with readout key that have been already stored in the TOE.                                  |
| Active Authentication Information Access Key | Rule of authenticating the authorized personnel of the passport issuing authorities by verification with Active Authentication Information Access Key that have been already stored in the TOE. |
| Mutual authentication                        | Rule of authenticating terminals according to the mutual authentication procedure in BAC and PACE defined by [ICAO-9303].   |

### 9.2.2 Authentication failure handling

The TOE detects when 3 unsuccessful authentication attempts occur related to the authentication with the Active Authentication Information Access Key. When the defined number of unsuccessful authentication attempts has been met, the TOE permanently stops authentication with the Active Authentication Information Access Key (the authentication status with the Active Authentication Information Access Key is fixed to “Not authenticated yet”).

The TOE detects when 3 unsuccessful authentication attempts occur related to the authentication with the transport key. When the defined number of unsuccessful authentication attempts has been met, the TOE permanently stops authentication with the transport key (the authentication status with the transport key is fixed to “Not authenticated yet”).

The TOE detects when 3 unsuccessful authentication attempts occur related to the authentication with the readout key. When the defined number of unsuccessful authentication attempts has been met, the TOE permanently stops authentication with the readout key (the authentication status with the readout key is fixed to “Not authenticated yet”).

### 9.2.3 Timing of identification and authentication

The TOE allows the readout of EF.CardAccess and EF.ATR/INFO without user identification nor authentication. Any other action requires user identification and authentication.

**9.2.4 Single-use authentication mechanisms**

The TOE prevents reuse of authentication data related to mutual authentication mechanism with the BAC procedure and the PACE procedure.

**9.3 ACCESS CONTROL**

**9.3.1 Access control during the issuance procedure**

During the issuance procedure (i.e. before the TOE is issued to the legitimate passport holder), access to the files stored within the TOE is protected through authentication with the readout key, transport key and /or Active Authentication Information Access Key, according to the rules specified in the table below:

| Authentication status <sup>11</sup>                                       | File subject to access control | Operation permitted  | Reference: data to be operated                                  |
|---|--------------------------------|--|---|
| Successful verification with readout key                                  | EF.DG13 <sup>12</sup>          | Read   | IC chip serial number (entered by manufacturer)                 |
| Successful verification with transport key                                | Transport key file             | Write  | Transport key data (update of old data)                         |
|   | Basic access key file          |  | Basic access key (Encryption key)                               |
|   | Password key file              |  | Basic access key (Message Authentication Code key)              |
|   | EF.DG1                         | Read or Write  | Password key  |
|   | EF.DG2                         |  | MRZ data  |
|   | EF.DG13                        |  | Facial image  |
|   | EF.DG14                        |  | Management data (Passport number and Booklet management number) |
|   | EF.COM <sup>13</sup>           |  | PACE v2 Security information                                    |
|   | EF.SOD                         |  | Active Authentication hash function information                 |
|   | EF.CardAccess                  |  | Common data   |
| EF.DG15   | Write                          | Security data related to Passive Authentication defined by Part 10 of [ICAO-9303]. |   |
| Successful verification with Active Authentication Information Access Key | EF.DG15                        | Write  | PACE v2 Security information                                    |
|   | Private key file               |  | Active Authentication Public Key                                |
|   |                                |  | Active Authentication Private Key                               |

<sup>11</sup> The readout key, transport key, and Active Authentication Information Access Key are configured by the manufacturer. The transport key can be changed (updated) by an authorized user. With regard to the files subject to access control included in this table and files storing the read key and Active Authentication Information Access Key which may vary the authentication status, user access that is not stated in this table is prohibited. (The access controls to information in the TOE from terminals after issuing a TOE embedded passport booklet to the passport holder, i.e., BAC and PACE are separately specified.)

<sup>12</sup> In EF.DG13, an IC chip serial number has been recorded by the manufacturer, and the management data is appended to the file by the passport issuing authorities.

<sup>13</sup> EF.COM file may not be created according to the passport issuing authorities' instructions.

### 9.3.2 Access control during the operational phase (BAC procedure)

During the operational phase, when the communication with the TOE is initiated by a terminal according to the BAC procedure, access to the files stored within the TOE is conditioned by the successful authentication of the terminal during the mutual authentication step.

Once it is successfully authenticated by the TOE, the terminal is allowed to read data from the files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD. The writing of data to, as well as the reading of data from: the transport key file, basic access key file, password key file, and private key file are prohibited.

### 9.3.3 Access control during the operational phase (PACE procedure)

During the operational phase, when the communication with the TOE is initiated by a terminal according to the PACE procedure, access to the files stored within the TOE is conditioned by the successful authentication of the terminal during the mutual authentication step.

Once it is successfully authenticated by the TOE, the terminal is allowed to read data from the files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD. The writing of data to, as well as the reading of data from: the transport key file, password key file, and private key file are prohibited.

## 9.4 SECURE COMMUNICATION

### 9.4.1 Confidentiality and integrity protection for BAC

When performing the BAC procedure:

- The TOE transmits and receives user data in a manner protected from unauthorized disclosure.
- The TOE transmits and receives user data in a manner protected from modification, deletion, insertion and replay errors. The TOE is be able to determine, on receipt of user data, whether modification, deletion, insertion or replay has occurred.

### 9.4.2 Confidentiality and integrity protection for PACE

When performing the PACE procedure:

- The TOE transmits and receives user data in a manner protected from unauthorized disclosure.
- The TOE transmits and receives user data in a manner protected from modification, deletion, insertion and replay errors. The TOE is be able to determine, on receipt of user data, whether modification, deletion, insertion or replay has occurred.

### 9.4.3 Trusted channel between the terminal and the TOE

The TOE implements the Secure Messaging channel defined by [ICAO-9303]. The channel is logically distinct from other communication channels and provides assured identification of its end points and protection of channel data from modification or disclosure. After the Secure Messaging channel is established, only the Secure Messaging channel is available for the communication path between terminal and TOE.

The TOE allows the terminal to initiate communication via the trusted channel, or the TOE itself can initiate communication via the trusted channel for reading data from the TOE.

## 9.5 SECURITY MANAGEMENT

### 9.5.1 Privileged role in pre-issuance phase

The TOE maintains the role “authorized personnel of the passport issuing authorities”, and is able to associate users with this role.



The TOE is capable of performing the following management functions: modification of transport key and enabling / disabling the BAC function. However, these functions are restricted to the “authorized personnel of the passport issuing authorities” after successful authentication.

### 9.5.2 Import of user data in pre-issuance phase

During the issuance procedure (i.e. before the TOE is actually issued to the legitimate passport holder), the TOE ignores any security attributes associated with the user data when imported from outside the TOE.

## 9.6 RESISTANCE TO PHYSICAL ATTACK

The TOE is designed and implemented to resist attacks defined by the CC Supporting Documents related to Smartcards to the hardware and software of the TOE by responding automatically such that the SFRs are always enforced.

## 9.7 MAPPING OF SFRs TO TSS

| SFR         | Link to TSS   |
|-------------|---|
| FCS_CKM.1b  | Addressed in section 9.1.1 “Cryptographic key generation”                                 |
| FCS_CKM.1p  | Addressed in section 9.1.1 “Cryptographic key generation”                                 |
| FCS_CKM.1e  | Addressed in section 9.1.1 “Cryptographic key generation”                                 |
| FCS_CKM.4   | Addressed in section 9.1.2 “Cryptographic key destruction”                                |
| FCS_COP.1a  | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1h  | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1hb | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1mb | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1sb | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1n  | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1e  | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1hp | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1mp | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_COP.1sp | Addressed in section 9.1.3 “Cryptographic operations”                                     |
| FCS_RND.1   | Addressed in section 9.1.4 “Generation of random numbers”                                 |
| FDP_ACC.1a  | Addressed in section 9.3.1 “Access control during the issuance procedure”                 |
| FDP_ACC.1b  | Addressed in section 9.3.2 “Access control during the operational phase (BAC procedure)”  |
| FDP_ACC.1p  | Addressed in section 9.3.3 “Access control during the operational phase (PACE procedure)” |
| FDP_ACF.1a  | Addressed in section 9.3.1 “Access control during the issuance procedure”                 |
| FDP_ACF.1b  | Addressed in section 9.3.2 “Access control during the operational phase (BAC procedure)”  |
| FDP_ACF.1p  | Addressed in section 9.3.3 “Access control during the operational phase (PACE procedure)” |
| FDP_ITC.1   | Addressed in section 9.5.2 “Import of user data in pre-issuance phase”                    |
| FDP_UCT.1b  | Addressed in section 9.4.1 “Confidentiality and integrity protection for BAC”             |
| FDP_UCT.1p  | Addressed in section 9.4.2 “Confidentiality and integrity protection for PACE”            |
| FDP_UIT.1b  | Addressed in section 9.4.1 “Confidentiality and integrity protection for BAC”             |
| FDP_UIT.1p  | Addressed in section 9.4.2 “Confidentiality and integrity protection for PACE”            |
| FIA_AFL.1a  | Addressed in section 9.2.2 “Authentication failure handling”                              |
| FIA_AFL.1d  | Addressed in section 9.2.2 “Authentication failure handling”                              |
| FIA_AFL.1r  | Addressed in section 9.2.2 “Authentication failure handling”                              |
| FIA_UAU.1   | Addressed in section 9.2.3 “Timing of identification and authentication”                  |
| FIA_UAU.4   | Addressed in section 9.2.4 “Single-use authentication mechanisms”                         |
| FIA_UAU.5   | Addressed in section 9.2.1 “Supported authentication mechanisms”                          |
| FIA_UID.1   | Addressed in section 9.2.3 “Timing of identification and authentication”                  |
| FMT_MOF.1   | Addressed in section 9.5.1 “Privileged role in pre-issuance phase”                        |
| FMT_MTD.1   | Addressed in section 9.5.1 “Privileged role in pre-issuance phase”                        |
| FMT_SMF.1   | Addressed in section 9.5.1 “Privileged role in pre-issuance phase”                        |
| FMT_SMR.1   | Addressed in section 9.5.1 “Privileged role in pre-issuance phase”                        |

|                  |   |
|------------------|---|
| <b>FPT_PHP.3</b> | Addressed in section 9.6 “Resistance to physical attack”                      |
| <b>FTP_ITC.1</b> | Addressed in section 9.4.3 “Trusted channel between the terminal and the TOE” |

**END OF SECURITY TARGET**