Xaica-alpha64K
Security Target Lite

December 14, 2007

NTT DATA CORPORATION

COLOR-PRINTING IS RECOMMENDED

Index

1. INTRODUCTION

This chapter identifies this security target (**ST**), and describes the overview of ST, conformance claims, and the structure of this security target.

1.1. ST Identification

Title: Xaica-alpha64K Security Target Lite

Document Identification: NTTD-STL-XAICAALPHA64K-ST19

Document version: 1.00

Date: December 14, 2007

Company: NTTDATA

Product name: Xaica-alpha64K

TOE version;

- ROM code: SPEC5V014
- Soft Mask: -
- Security Personalization ID: SPI-001-01

1.2. ST overview

The aim of this document is to describe the Security Target for Xaica-alpha64K for Passport Booklet IC. This security target is a composite ST, composed of this one and the ST19WR66 security target[30], produced by STMicroelectronics.

Xaica-alpha64K mainly consists of:

- Integrated Circuit Chip for smartcard (ST19WR66) provided by STMicroelectronics (STM)
- Dedicated Software provided in ST19WR66
- Smartcard platform software 'Xaica-PF' embedded on IC chip
- MRTD application embedded on Xaica-PF

The main objectives of this security target are:

- To identify the target of evaluation (**TOE**), the product type, the TOE environment and its lifecycle, and to define the physical and logical boundary of the TOE
- To identify the security environment of the TOE, assets to be protected, envisioned threats to be countered by the TOE and its supporting environment.
- To identify the security objectives for the TOE and for its supporting environment
- To specify the functional security requirements for TOE and IT environment as well as security assurance requirements
- To specify the TOE summary specification which explain overview of TOE security functionalities implemented in the product.
- To specify the rationale to demonstrate the completeness, cohesiveness and effectiveness among objectives, requirements and security countermeasures within the security environment.

1.3. Common Criteria Conformance Claims

This security target is compliant with the Common Criteria V2.3, part1, 2, 3

as follows:

- Part2 extended,
- Part3 conformant
- Package conformant to EAL4 augmented with
  ACM_SCP.3,
  ADV_IMP.2,
  ADV_SPM.3,
  ALC_DVS.2,
  ALC_LCD.2,
  ALC_TAT.2, and
  AVA_VLA.3.

The minimum strength level for the security function “SF_I&A” is “**SOF-high**”.

2. TOE DESCRIPTION

This chapter identifies the general IT features of the TOE and the main security concerns.

2.1. TOE definition

The Target of Evaluation (TOE) is contact-less integrated circuit chip: ST19WR66I with embedded software: Xaica-PF.

Xaica-PF is multi-application platform software, which is masked on ROM memory. MRTD application consists of related functions on the ROM and MRTD LDS files personalized on EEPROM.

The boundary of the TOE is in Figure 2-1. The TOE is comprised of the followings:

- Integrated Circuit Chip (ST19WR66I) provided by STMicroelectronics (STM)
- Dedicated Software of ST19WR66I.
- Platform software: ‘Xaica-PF’
- MRTD application

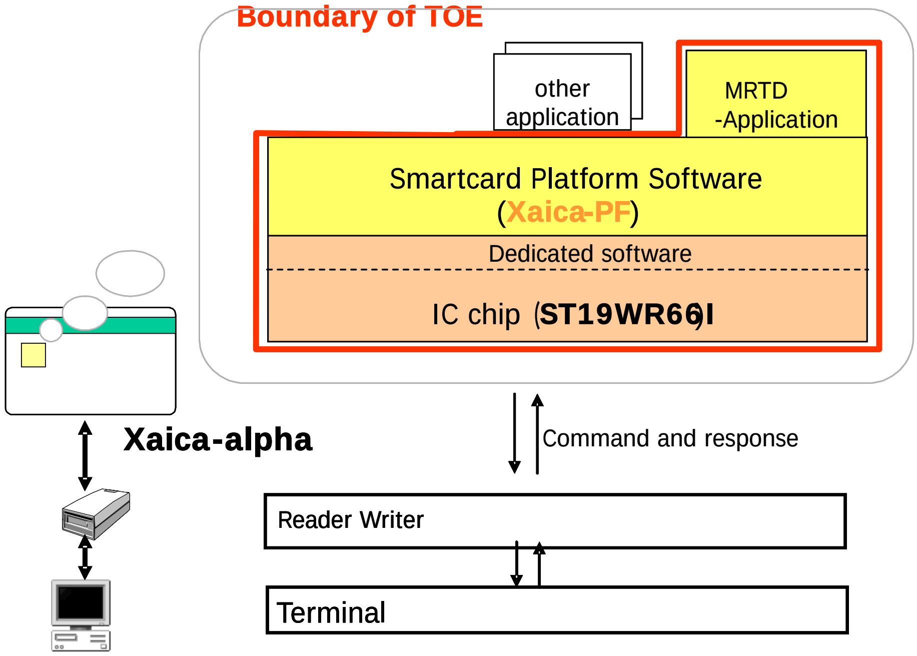

Figure 2-1

Note that no other applications shall be personalized or loaded on the TOE.

Xaica-PF provides the following functions:

- User identification and authentication
- Access control
- Cryptography
- Management of card-status
- Secure messaging
- Management of secure messaging key
- Management of key and password
- Management of temporary public key
- Creation of file-based application
- Management of SECURITY ENVIRONMENT
- Initialization and initial testing
- Security functions provided in the IC chip
    - Memory partition and access control
    - Cryptographic and random number generation libraries
    - Physical tampering countermeasure and internal integrity

The TOE provides some authentication mechanisms to identify the user, and has the access control function in order to avoid any unauthorized user's accessing to the object. The TOE always identifies its card-status applicable to lifecycle phase, and restricts the available functions for each card-status.

The TOE allows the user to store the key as usage, and has stored key management functionality as well. The provided Cryptographic function is dedicated not only to cryptographic key and authentication but also to secure messaging which ensures the communication data is protected by eavesdropping or illegal modification.

Some behavior of the security functions above could be managed in SECURITY ENVIRONMENT as defined in ISO7816[31].

Xaica-PF and IC chip provide the self-management functions so as to keep confidentiality, integrity and availability of TOE functionalities as followings; self-diagnosis, internal integrity checking, physical tampering and detecting, violation control, and so on.

The MRTD application which is compliant with ICAO's specifications: LDS[6], PKI[7], and [7]Annex, provides the following functions:

- Basic Access Control
- Passive Authentication
- Active Authentication

This security target refers to the ICAO documents [6], [7] for a complete generic description.

2.2. TOE usage and security features for operational use

Differences between this security target and [PP0017] in this chapter are described with blue color.

A state or an organisation issues MRTD to be used by a holder for international travel. The traveler presents a MRTD to an inspection system to prove his or her identity. The MRTD in this security target contains (i) visual (eye readable) biographical data and a portrait of the holder, (ii) MRZ data for visual and machine reading using OCR and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for the holder with the claimed identity as given on the bio 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. A receiving State trusts the genuine MRTD of the issuing State or Organization.

For this security target the MRTD is viewed as an 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 data page of the passport book,

  (2) 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 [6] as compliant with the ICAO specification 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, DG1),

  (2) the digitized portraits (DG2),

  (3) the optional biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both

  (4) the other data according to LDS (DG5 to DG16) and

(5) the Document security object.

The issuing State or organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and its data. The MRTD as a passport book and the MRTD's chip is uniquely identified by a document number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical security measure (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [8]. 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 Passive Authentication as the baseline security method and Basic Access Control as an optional advanced security method to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control and Data Encryption of additional biometrics as optional security measure in the ICAO Technical report [7]. The Passive Authentication Mechanism and Data Encryption are performed completely and independently on the TOE by the TOE environment.

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, (ii) in confidentiality by the Basic Access Control Mechanism, and (iii) for clone creation prevention by the Active Authentication Mechanism. This security target does not address Extended Access Control as the optional security mechanism.

The Basic Access Control is a security feature which shall be mandatory supported by the TOE. The inspection system reads the printed data in MRZ to generate and exchange cryptographic keys. When reading MRZ, the MRTD must be opened beforehand, which prevents illicit reading of the TOE data via contactless communication interface of the TOE. After reading out MRZ, the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [7], Annex E, and [6].

The Active Authentication Mechanism is a security feature which is supported by the TOE. The Mechanism ensures that the Inspection System can confirm the genuineness of the MRTD's chip. The inspection system authenticates the TOE through a protocol based on the Active Authentication Key Pair, using the trusted channel opened after successful Basic Access Control Authentication. The Inspection System has already read the digital data and the Document Security object, performed Passive Authentication and got back the Active Authentication Public Key. The inspection system asks the TOE to sign a given random data with its Active Authentication Private Key, and then checks the returned signature with the Active Authentication Public Key obtained in the previous step. This mechanism ensures that the personal data of the passport holder was signed for this specific MRTD.

2.3. TOE life cycle

The TOE life cycle is described in terms of the four life cycle phases: Development, Manufacturing, Personalization of the MRTD, and Operational use. Figure 2-2 shows the workflow of the phases. Table 2-1 shows the assignment of term in the phase description.

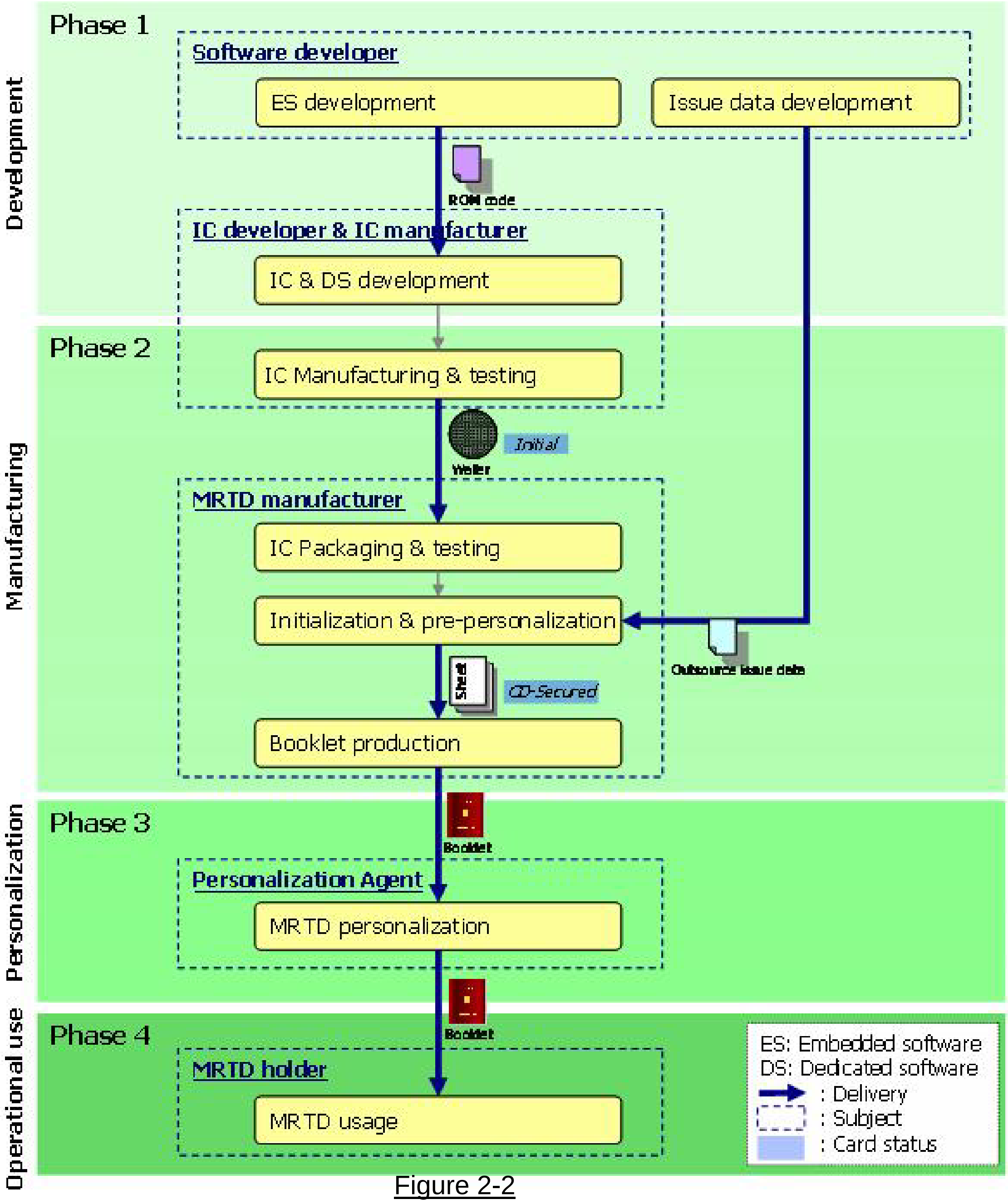

Figure 2-2

Table 2-1

term	assignment	remarks
IC developer	STMicroelectronics	
software developer	NTT DATA	TOPPAN(sub developer)
IC manufacturer	STMicroelectronics	
IC Embedded Software	Xaica-PF	

Differences between this security target and [PP0017] in below description are described with blue color.

Phase 1 “Development”

The TOE is developed in Phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

The software developer uses guidance documentation for the integrated circuit and guidance documentation for relevant parts of the IC Dedicated Software and then develops the IC Embedded Software (ROM code) with MRTD application and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC Dedicated Software and the IC Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

The software developer designs and produces the issue data for the Initialization and the pre-personalization in MRTD manufacturer.

The initialization data and pre-personalization data are encrypted with Outsource mechanism.

Phase 2 “Manufacturing”

As the first step, the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software in the non-volatile non-programmable memories (ROM). And the IC manufacturer writes the IC Identification Data (IC) onto chip to control the IC as MRTD material during the IC manufacturing and delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.
The MRTD manufacturer (i) add the parts of the IC Embedded Software in the non-volatile programmable memories (with outsource mechanism) (~~for instance~~ EEPROM) if necessary, (ii) creates the MRTD application (with outsource mechanism), and (iii) equips MRTD's chip with Pre-personalization Data (with outsource mechanism) and (iv) packs the IC with hardware for the contact-less interface in the passport book.

The pre-personalized MRTD with the IC Identification Data (MRTD) written by the MRTD manufacturer is 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.

Application data: IC Identification data (IC) written by IC manufacturer is the traceability data between IC manufacturer and MRTD manufacturer, and is not allowed to be read after phase 2. IC Identification data (MRTD) written by MRTD manufacturer is the traceability data between MRTD manufacturer and Personalization Agent, and is used in phase 3 (not allowed to read in phase 4). In this Security Target, IC Identification data indicates IC Identification data (MRTD) hereafter.

Phase 3 "Personalization of the MRTD"

The personalization of the MRTD includes (i) the survey of a MRTD holder biographical data, (ii) enrollment of MRTD holder biometric reference data (i.e. digitized portraits and optional biometric reference data), (iii) printing visual readable data onto the physical MRTD, (iv) writing TOE User Data and TSF Data into logical MRTD and (v) writing TSF Data into the logical MRTD and 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) digital MRZ data (DG1), (ii) the digitized portrait (DG2), and (iii) the Document Security Object.

Signing Document Security Object by Document Signer [7] finalizes the personalization of genuine MRTD for a MRTD holder. The personalized MRTD (together with guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Application note: To be exact, MRTD manufacturer can be divided into two sub-subjects. One sub-subject (Subject 2-A) produces the IC sheet using wafer. The other sub-subject (Subject 2-B) produces the MRTD booklet using IC sheet. And, Subject 2-A writes the identification data for the delivery to the Subject 2-B.

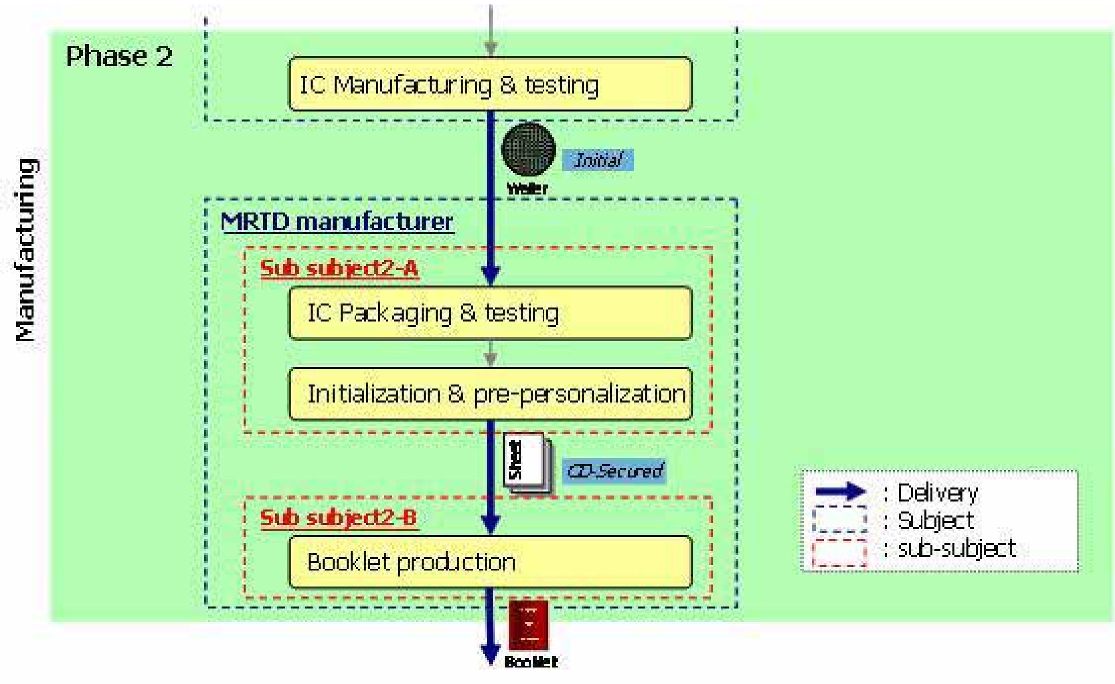

Figure 2-3

Application note 1: This security target distinguishes between the personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [7]. This approach allows but does not enforce the separation of these roles. The selection of the authentication keys should consider the organisation, the productivity and the security of the personalization process. Asymmetric authentication keys provide comfortable security for distributed personalization but their use may be more time consuming than authentication using symmetric cryptographic primitives. Authentication using symmetric cryptographic primitives allows for fast authentication protocols appropriate for centralised personalization schemes but

relies on stronger security protection in the personalization environment (cf. section 5.5.3 Personalization Terminals for further details).
In this evaluation, Personalization Agent uses PIN verification, but does not use symmetric cryptographic mechanism authentication for personalization.

Application note: Personalization Agent has two keys. One is Personalization Agent key (Perso) for personalization, and the other is Personalization Agent key (IDread) for reading IC identification data.

Phase 4 "Operational Use"

The TOE is used as the MRTD's chip by a traveler and an inspection system in the "Operational Use" phase. The user data can be read and used according to the security policy of the Issuing State or Organization and used according to a security policy of the Issuing State but they can never be modified.

Application note 2: ~~The authorized Personalization Agents might be allowed to add (not to modify) data in the other data groups of the MRTD application (e.g. person(s) to notify DG16) in the Phase 4 Operational Use. This will imply an update of the Document Security Object including the re-signing by the Document Signer.~~

In case of this evaluation, the authorized Personalization Agent is not allowed to add data in the other data groups of the MRTD application in the Phase 4 Operational Use. The Document Security Object is never updated in any Phase.

Application note 3: The intention of the PP is to consider at least the phases 1 and 2 as part of the evaluation and therefore define TOE delivery according to CC after phase 2 or later. The personalization process and its environment may depend on specific security needs of an issuing state or organisation. The Security Target shall describe the instantiation of the life cycle defined in this PP relevant for the product evaluation process. It is of importance to define the point of TOE delivery in the life cycle required for the evaluation according to CC requirements ADO_DEL. All development and production steps before TOE delivery have to be part of the evaluation under ACM, ALC and ADO assurance classes as specifically relevant before TOE delivery. All production, generation and installation procedures after TOE delivery up to the operational use (phase 4) have to be considered in the product evaluation process under ADO and AGD assurance classes. Therefore, the Security Target has to outline the split up of P.Manufact, P.Personalization and the related security objectives into aspects relevant before vs. after TOE delivery. Note: In many cases security aspects for phase 3 are defined and controlled by the issuing state or organisation.

Application note: The security policy of TOE itself is completed in IC developer and IC manufacturer site. The scope of site audit in this evaluation is the stages before TOE itself changes to self-protected state and is described below (Figure 2-4). [33]

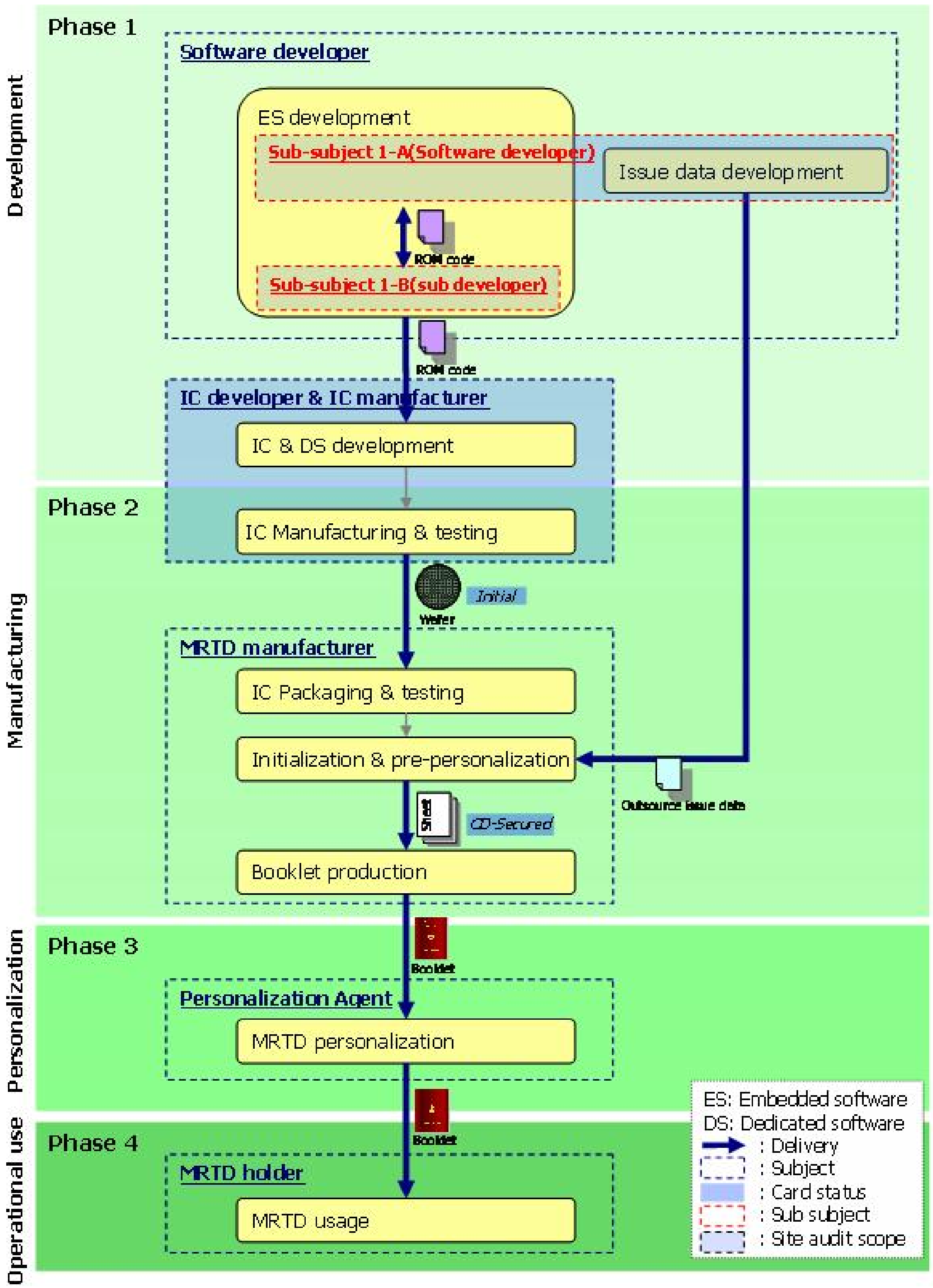
Development
Manufacturing
Personalization
Operational use
Phase 1
Software developer
ES development
Sub-subject 1-A(Software developer)
Issue data development
ROM code
Sub-subject 1-B(sub developer)
ROM code
IC developer & IC manufacturer
IC & DS development
Phase 2
IC Manufacturing & testing
Initial
Wafer
MRTD manufacturer
IC Packaging & testing
Initialization & pre-personalization
Outsource issue data
Sheet
CD-Secured
Booklet production
Phase 3
Booklet
Personalization Agent
MRTD personalization
Booklet
Phase 4
MRTD holder
MRTD usage
ES: Embedded software
DS: Dedicated software
: Delivery
: Subject
: Card status
: Sub subject
: Site audit scope

Figure 2-4

3. TOE security environment

This chapter identifies the following contents:

- **Assets** to be protected by the TOE and/or environment
- **Subjects** to be relative to the TOE
- **Assumptions** as an intended usage of the TOE, possible limitation of use, physical, personnel, or connectivity aspects of
- **Threats** to assets against which specific protection either in the TOE or in its environment is required
- **Organizational security policies** required in MRTD to be enforced in the TOE and its environment

Differences between this security target and [PP0017] about Assets, Subjects, Assumptions, Threats and Organizational security policies in chapter 3 are described with blue color.

3.1. Introduction

Assets

The assets to be protected by the TOE include the User Data on the MRTD's chip.

Logical MRTD Data

The logical MRTD data consists of the data groups DG1 to DG16 and the Document security object according to LDS [6]. These data are user data of the TOE. The data groups DG1 to DG14 and DG 16 contain personal data of the MRTD holder. The Active Authentication Public Key Info in DG 15 is used by the inspection system for Active Authentication of the chip. The Document security object is used by the inspection system for Passive Authentication of the logical MRTD.

Application note: The TOE addresses only DG1, DG2, DG13, DG15.

An additional asset is the following more general one.

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD's holder is used by the traveler to authenticate himself as possessing a genuine MRTD.

Subjects

This security target considers the following subjects:

Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users IC Manufacturer and MRTD Manufacturer using this role Manufacturer.

MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalised the MRTD.

Traveller

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Personalization Agent

The agent is acting on the behalf of the issuing State or Organisation to personalize the MRTD for the holder by some or all of the following activities (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability and (iv) signing the Document Security Object defined in [6].

Inspection system

A 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. ~~The Primary Inspection System (PIS) (i) contains a terminal for the contactless communication with the MRTD's chip and~~

~~(ii) does not implement the terminals part of the Basic Access Control Mechanism. The Primary Inspection System can read the logical MRTD only if the Basic Access Control is disabled.~~ The ~~**Basic**~~ **Inspection System** (i) contains a terminal for the contactless communication with the MRTD's chip, (ii) implements the terminals part of the Basic Access Control Mechanism, (iii) gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the printed data in the MRZ or other parts of the passport book providing this information and ~~The **Extended Inspection System** (EIS) in addition to the Basic Inspection System~~ (iv) implements the Active Authentication Mechanism.~~, (ii) supports the terminals part of the Extended Access Control Authentication Mechanism and (iii) is authorized by the issuing State or Organization to read the optional biometric reference data.~~

~~Application note 4: This protection profile does not distinguish between the BIS and EIS because the Active Authentication and the Extended Access Control is outside the scope.~~

Application note: Inspection System addresses the Basic Access Control Mechanism and the Active Authentication Mechanism except for Extended Access Control Authentication Mechanism.

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface.

Attacker

A threat agent trying (i) to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Application note 5: An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but his or her attack itself is not relevant for the TOE.

3.2. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.Pers_Agent Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Active Authentication Public Key Info (DG15) ~~if stored on the MRTD's chip~~, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by ~~symmetric cryptographic mechanisms~~ PIN verification mechanism.

Application note: The TOE need PIN verification mechanism (not symmetric cryptographic mechanisms) for Personalization Agent.

A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is 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. The ~~Primary~~ Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [7]. The ~~Primary~~ Inspection System performs the Passive Authentication to verify the logical MRTD and ~~if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System~~ implements the terminal part of the Basic Access Control and reads the logical MRTD and performs the Active Authentication Mechanism being under Basic access Control.

Application note 6: ~~According to [7] the support of (i) the Passive Authentication mechanism is mandatory, and (ii) the Basic Access Control is optional. In the context of this security target the Primary Inspection System does not implement the terminal part of the Basic Access Control. It is therefore not able to read the logical MRTD if the logical MRTD is protected by Basic Access Control. The TOE~~

~~allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems.~~

Application note: In this evaluation, the Basic Access Control and the Active Authentication Mechanism in addition to Passive Authentication mechanism are mandatory (scope).

A.MRTD_holder Handling of the MRZ by MRTD holder

The holder shall not disclose the MRZ to any unauthorized people to prevent attempts to disclose the logical MRTD.

Application note: This assumption is added here according to DCSSI application note [34] regarding the BAC mechanism.

3.3. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Chip_ID Identification of MRTD's chip

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.Skimming Skimming the logical MRTD

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know this data in advance.

Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

T.Forgery Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an inspection system by means of the changed MRTD holders identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim an other identity of the traveller. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MTRD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD in an other contactless chip.

The TOE shall avert the threat as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

Application note: To be more precise, T.Abuse-Func addresses new (code based) application download onto TOE and not necessary crypto algorithms usage.

T.Information_Leakage Information Leakage from MRTD's chip

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) to modify User Data or (iv) to modify TSF data.

The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used.

Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misuse of administration function. To exploit this an attacker needs information about the functional operation.

T.Clone **Clone of MRTD**

An attacker may produce a clone MRTD by using MRTD data and MRZ, which are leaked from real MRTD.

3.4. Organisational Security Policies

The TOE shall comply to the following organisation security policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations (see CC part 1, sec. 3.2).

P.Manufact Manufacturing of the MRTD's chip

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. The Initialization Data are written by the MRTD ~~IC~~ Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Keys.

Application note: The MRTD Manufacturer writes the Initialization Data (IC Identification data) to the TOE.

P.Personalization Personalization of the MRTD by issuing State or Organization only

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitised portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by authorized agents of the issuing State or Organization only.

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitised portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [7]. The issuing State or Organization ~~decides (i) to~~ enables the Basic Access Control for the protection of the MRTD holder personal data~~ or (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD~~.

Application note 7: The organisational security policy P.Personal_Data is drawn from the ICAO Technical Report [7]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent.

Application note: The Basic Access Control mechanism is a mandatory for the TOE. The issuing state or Organization doesn’t need to disable the Basic Access Control mechanism.

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into two security objectives (i) for the development and production environment and security objectives (ii) for the operational environment.

Differences between this security target and [PP0017] about security objectives in chapter 4 are described with blue color.

4.1. Security objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organisational security policies to be met by the TOE.

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data groups, the Document security object according to LDS [6] and the TSF data can be written by authorized Personalization Agents. The logical MRTD data groups DG1 to DG16, the Document security object and the TSF data can be written only once and can not be changed after personalization.~~The Document security object can be updated by authorized Personalization Agents if data in the data groups DG 3 to DG16 are added.~~ Only the Personalization Agent shall enable the TSF Basic Access Control.

Application note 8:The OT.AC_Pers implies that

(1) the data of the LDS groups written during personalization for MRTD holder (at least DG1 and DG2) can not be changed by write access after personalization,

~~(2) the Personalization Agents may (i) add (fill) data into the LDS data groups not written yet, and (ii) update and sign the Document Security Object accordantly.~~

Application note: The TOE addresses only DG1, DG2, DG13, DG15. The TOE restricts the addition of data in the data group DG and the update of the Document security object after Phase 3.

OT.Data_Int **Integrity of personal data**

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. ~~If the TOE is configured for the use with Basic Inspection Terminals only the~~ The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

Application note: The Basic Access Control mechanism is a mandatory for the TOE.

OT.Data_Conf **Confidentiality of personal data**

~~If the TOE is configured for the use with Basic Inspection Systems t~~The TOE must ensure the confidentiality of the logical MRTD data groups DG1 to DG16 by granting read access to terminals successfully authenticated by (i) as Personalization Agent or as (ii) ~~Basic~~ Inspection System. The ~~Basic~~ Inspection System shall authenticate themselves by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the ~~Basic~~ Inspection System.

Application note: The Basic Access Control mechanism is a mandatory for the TOE. The TOE addresses only DG1, DG2, DG13, DG15.

Application note 9:The traveler grants the authorization for reading the personal data in DG1 to DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication independent on the quality of the Document Basic Access Keys which is defined by the TOE environment and loaded into the TOE by the Personalization Agent. Any attack based on decision of the ICAO Technical Report

[7] that the inspection system derives Document Basic Access Keys from the printed MRZ data does not violate the security objective OT.Data_Conf.

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide an unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. ~~If the TOE is configured for use with Basic Inspection Terminals only in~~ In Phase 4 “Operational Use” the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note: The Basic Access Control mechanism is a mandatory for the TOE.

Application note 10: The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 “Manufacturing” and for traceability and/or to secure shipment of the TOE from Phase 2 “Manufacturing” into the Phase 3 “Personalization of the MRTD”. The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing environment as described in its security objective OD.Material. In the Phase 4 “Operational Use” the TOE is identified by the passport number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit serial number ICCSN) or a MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

OT.Prot_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 (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

Application note: To be more precise, OT.Prot_Abuse-Func prevents from new (code based) application download onto TOE, not necessary crypto algorithms usage and test features usage. The policy of such deactivation can not be changed after phase 2.

OT.ActiveAuth Active Authentication for clone MRTD

The TOE must provide the function of signature according to the Active Authentication mechanism. The TOE must ensure the confidentiality and the integrity of Active Authentication private key.

The following TOE security objectives address the protection provided by the MRTD's chip independent on the TOE environment.

OT.Prot_Inf_Leak Protection against Information Leakage

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

-by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

-by forcing a malfunction of the TOE and/or

-by a physical manipulation of the TOE.

Application note 11: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper Protection against Physical Tampering

The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with high attack potential by means of

-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

-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)
-manipulation of the hardware and its security features, as well as
-controlled manipulation of memory contents (User Data, TSF Data)
with a prior
-reverse-engineering to understand the design and its properties and functions.

Application note 12: In order to meet the security objectives OT.Prot_Phys-Tamper the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack. This is addressed by the security objective OD.Assurance.

OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application note 13: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE´s internals.

4.2. Security objectives for the Development and Manufacturing Environment

OD.Assurance Assurance Security Measures in Development and Manufacturing Environment

The developer and manufacturer ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. This includes the use of the Initialization Data for unique identification of the TOE and the pre-personalization of the TOE including the writing of the Personalization Agent Authentication key(s). The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against obvious penetration attacks with low attack potential and against direct attacks with high attack potential against security function that uses probabilistic or permutational mechanisms.

OD.Material Control over MRTD Material

The IC Manufacturer, the MRTD Manufacturer and the Personalization Agent must control all materials, equipment and information to produce, to initialise, to pre-personalize genuine MRTD materials and to personalize authentic MRTD in order to prevent counterfeit of MRTD using MRTD materials.

4.3. Security objectives for the Operational Environment

Issuing State or Organization

The Issuing State or Organization will implement the following security objectives of the TOE environment.

OE.Personalization Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organisation (i) establish the correct identity of the holder and create biographic data for the MRTD, (ii) enroll the biometric reference data of the MRTD holder i.e. the portrait~~, the encoded finger image(s) and/or the encoded iris image(s)~~ and (iii) personalize the MRTD for the holder together with the defined physical and logical security measures (including the digital signature in the Document Security Object and Active Authentication Private Key). The Personalization Agents enable~~ or disable~~ the Basic Access Control function of the TOE.~~ according to the decision of the issuing State or Organization. If the Basic Access Control function is enabled t~~The Personalization Agents generate the Document Basic Access Keys and store them in the MRTD's chip.

Application note: The TOE addresses only DG1, DG2, DG13, DG15 (doesn't address the encoded finger image(s) and the encoded iris image(s)).
The Basic Access Control mechanism is a mandatory for the TOE.
The TOE addresses the Active Authentication Mechanism.

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The Issuing State or Organization must (i) generate a cryptographic secure Country Signing Key Pair, (ii) ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity. The Issuing State or organization must (i) generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signing Public Key to receiving

States and organizations. The digital signature in the Document Security Object include all data in the data groups DG1 to DG16 if stored in the LDS according to [6].

Receiving State or organization

The Receiving State or Organization will implement the following security objectives of the TOE environment.

OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD.

OE.Passive_Auth_Verif Verification by Passive Authentication

The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and organizations must manage the Country Signing Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.

OE.Active_Auth_verif Verification by Active Authentication

The border control officer of the Receiving State uses the inspection system to verify the traveller as MRTD holder. The inspection systems must have successfully verified the signature of Active Authentication Private Key.

OE.Prot_Logical_MRTD Protection of data of the logical MRTD

The inspection system of the receiving State ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control, use the secure messaging with fresh generated keys for the protection of the transmitted data and implement the terminal part of the Active Authentication.~~ (i.e. Basic Inspection Systems). The receiving State examining the logical MRTD with Primary Inspection Systems will prevent eavesdropping to the communication between TOE and inspection system.~~

~~Application note 14: The Primary Inspection System may prevent unauthorized listening to or manipulation of the communication with the MRTD's chip e.g. by a Faraday cage.~~

Application note: The Basic Access Control mechanism is a mandatory for the TOE. Inspection System addresses the Basic Access Control Mechanism and the Active Authentication Mechanism except for Extended Access Control Authentication Mechanism. Security relevant data (especially the printed MRZ) shall be carefully treated by Inspection System as required by OE.Secure_handling_MRZ. (e.g. Inspection System will not disclose the printed MRZ to unauthorized users, nor store the data after processing with MRTD.)

MRTD Holder

~~**OE.Secure_Handling**~~ ~~**Secure handling of the MRTD by MRTD holder**~~

~~The holder of a MRTD configured for use with Primary Inspection Systems (i.e. MTRD with disabled Basic Access Control) will prevent unauthorized communication of the MRTD's chip with terminals through the contactless interface.~~

~~Application note 15: The MRTD holder may prevent unauthorized communication of the MRTD's chip with terminals e.g. by carrying the MRTD in a metal box working as Faraday cage.~~

OE.Secure_Handling_MRZ **Secure handling of the MRZ by MRTD holder**

The holder must not disclose the MRZ to any unauthorized people to prevent attempts to disclose the logical MRTD.

Application note: This security objective is added here according to DCSSI application note [34] regarding the BAC mechanism.

5. Security functional requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this security target.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “refinement” in bold text and the added/changed words are in bold text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as unlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

5.1. Definitions

Followings are definitions of subjects, objects and related security attributes.

5.1.1. Subjects

The necessary subjects are defined below.

Table 5-1

No	Subject	Note
1	Manufacturer	see subjects in 3.1
2	Personalization Agent	see subjects in 3.1
3	Inspection system	see subjects in 3.1

5.1.2. Objects

The necessary objects are defined below.

Table 5-2

No	Objects	Note
1	Personalization Agent Key(Perso)	The PIN accessed to TOE by Personalization Agent for personalization
2	Personalization Agent Key(IDread)	The PIN accessed to TOE by Personalization Agent for reading IC identification data
3	Personalization Agent Keys	Personalization Agent Key(Perso) and Personalization Agent Key(IDread)
4	Document Basic Access Key(ENC)	Kenc(TDES2Key) for Basic Access Control according to [7]
5	Document Basic Access Key(MAC)	Kmac(TDES2Key) for Basic Access

		Control according to [7]
6	Document Basic Access Keys	Document Basic Access Key(ENC) and Document Basic Access Key(MAC)
7	Session key(KS_ENC)	The session key(KS_ENC) generated by Basic Access Control according to [7]
8	Session key(KS_MAC)	The session key(KS_MAC) generated by Basic Access Control according to [7]
9	Session keys	Session key(KS_ENC) and Session key(KS_MAC)
10	Active Authentication Private Key	The private key(RSA1024) for Active Authentication
11	DG1-16	Data group 1-16 according to [6]
12	SOD	Document Security Object according to [6]
13	COM	Common information according to [6]

5.1.3. Roles

The overview of each role is described below.

Table 5-3

Role	Note
ROL.CARDMAN	This role has the key for ROL.CARDMAN which is for Manufacturer. The role is privileged: - to set system track - to change lifecycle - to set the keys of ISSUER1 - to set the keys of ISSUER2 - to create CD
ROL.ISSUER1	This role has the key for ROL.ISSUER1 which is for Manufacturer. The role is privileged:

	- to create file areas or keys as required by MRTD application - to set EEPROM related attributes
ROL.ISSUER2	This role has the key for ROL.ISSUER2 which is for Manufacturer. The role is privileged: - to set EEPROM related attributes
ROL.EP.Perso	This role has the keys for Personalization Agent Keys which are for Personalization Agent. The role is privileged: - to personalize personalization data - to read the IC Identification data

5.1.4. Access control policy

This subsection describes the overview of the concept of access control polices stated in this security target.

Access control policy	SFP.ACCESS_MRTD
SFP.ACCESS_MRTD is the dedicated access control function of MRTD application which is used by only MRTD application and the generic access control function of Xaica-PF which is commonly used by all application.	

Access control policy	SFP.SM_MRTD
SFP.SM_MRTD is the dedicated secure messaging function of MRTD application which is used by only MRTD application according to [7].	

Application note: The detail information of these SFP is described at the deliverables of ADV_SPM.

5.1.5. Key erasing method

The session key erasing(destruction) method is described below.

Key erasing method	MET.ERASE_SMKEY_MRTD
The session keys are erased(destructed) under below conditions. - error is occurred after session key distribution(generation) - selection of other application, CD and SD. - electrical deactivation of MRTD chip (including 'deselect')	

5.1.6. Key distribution method for secure messaging

The session key distribution(generation) method is described below.

Key distribution method	MET.MUTUAL_AUTHENTICATE
TOE distributes(generates) the session keys by 'MUTUAL_AUTHENTICATE' command (of Basic Access Contrl) according to [7] Annex E.	

5.1.7. Authenticated status

Following symbols indicate the status of authentication.

Authenticated status	AST_MRTD.SC1
PIN-verification with PIN for ROL.EP.Perso is succeeded by using 'VERIFY' command.	

Authenticated status	AST_MRTD.SC2
Dynamic authentication with Document Basic Access Keys is succeeded by using 'MUTUAL AUTHENTICATE command'.	

5.2. Extended Components Definition

This security target uses components defined as extensions to CC part 2. Some of these components are defined in [20], other components are defined in this security target.

5.2.1. Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

This family defines functional requirements for the storage of audit data.

Component leveling

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

Dependencies: No dependencies.

5.2.2. Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.
The family "Generation of random numbers (FCS_RND)" is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component leveling:

FCS_RND Generation of random numbers
1

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

Dependencies: No dependencies.

5.2.3. Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE an additional family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of a claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

Application note 16: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter Explicitly stated IT security requirements (APE_SRE)) from a TOE point of view. Note that this security target uses this explicit stated SFR for the personalization terminal in the IT environment only. Therefore the word "TSF" is substituted by the word "Personalization terminal".

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component leveling:

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT:

Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or rule].

Dependencies: No dependencies.

5.2.4. Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component leveling:

FMT_LIM Limited capabilities and availability
1
2

FMT_LIM.1 Limited capabilities require that the TSF is built to provide only the capabilities (perform action, gather information) necessary for their genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements are defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.2 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.1 Limited capabilities.

Application note 17: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced
or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

5.2.5. Definition of the Family FPT_EMSEC

The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires not to emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not to emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Dependencies: No other components.

5.3. Security Functional Requirement for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

Differences between this security target and [PP0017] about SFRs in chapter 5.3 are described with blue color.

5.3.1. Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2).

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the Manufacturer [assignment: *authorised users*] with the capability to store the IC Identification Data [assignment: *list of audit information*] in the audit records.

Dependencies: No dependencies.

Application note 18: The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS). The security measures in the manufacturing environment assessed under ADO_IGS and ADO_DEL ensure that the audit records will be used to fulfil the security objective OD.Assurance.

5.3.2. Class Cryptographic Support(FCS)

The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/BAC_MRTD Cryptographic key generation – Generation of ~~Document Basic Access~~Session Keys by the TOE

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_MRTD

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm MET.MUTUAL_AUTHENTICATE[assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes 112 bit [assignment: *cryptographic key sizes*] that meet the following: [7], Annex E [assignment: *list of standards*].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note: The Title ‘Generation of Document Basic access Keys’ is revised to ‘Generation of Session Keys’ in order to more correctly stand for this SFR. The Session Keys indicates session key(KS_ENC) and session key(KS_MAC) and are generated by MET.MUTUAL_AUTHENTICATE.

Application note 19: The TOE is equipped with the Document Basic Access Key generated and downloaded by the Personalization Agent. The Basic Access Control Authentication Protocol described in [7], Annex E.2, produces agreed parameters to generate the Triple-DES key and the Retail-MAC message authentication keys for secure messaging by the algorithm in [7], Annex E.1. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below (Common Criteria Part 2).

FCS_CKM.4 Cryptographic key destruction - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1/MRTD

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method MET.ERASE_SMKEY_MRTD[assignment: *cryptographic key destruction method*] that meets the following: none[assignment: *list of standards*].

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]
FMT_MSA.2 Secure security attributes

Application note 20: The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging.

(1). Cryptographic operation (FCS_COP.1)

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the TOE.

FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD

The TSF shall perform hashing[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm SHA-1[assignment: *cryptographic algorith*m] and cryptographic key sizes none[assignment: *cryptographic key sizes*] that meet the following: FIPS 180-2[assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

Application note 21: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also ~~FIA_UAU.4/BAC_MRTD~~FCS_CKM.1/BAC_MRTD) according to [7].

Application note: This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Active Authentication Mechanism (see also FCS_COP.1/RSA_MRTD) according to [7].

FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES

Hierarchical to: No other components.

FCS_COP.1.1/TDES_MRTD

The TSF shall perform secure messaging – encryption and decryption/outsouce – decryption[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[assignment: *cryptographic algorithm*] and cryptographic key sizes 112 bit[assignment: *cryptographic key sizes*] that meet the following: FIPS 46-3 [14] and [7]; Annex E[assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

Application note 22: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_BT. ~~Note the Triple-DES in CBC mode with zero initial vector include also the Triple-DES in ECB mode for blocks of 8 byte used to check the authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism.~~

Application note: The Outsource mechanism addresses only decryption of cryptographic operation.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD

The TSF shall perform secure messaging – message authentication code[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm Retail MAC[assignment: *cryptographic algorithm*] and cryptographic key sizes 112 bit[assignment: *cryptographic key sizes*] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2) [assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

Application note 23: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1/BAC_MRTD and FIA_UAU.4/BAC_MRTD.

FCS_COP.1/RSA_MRTD Cryptographic operation – Signature RSA

Hierarchical to: No other components.

FCS_COP.1.1/ RSA_MRTD

The TSF shall perform signature generation[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm RSA[assignment: *cryptographic algorithm*] and cryptographic key sizes 1024 bit[assignment: *cryptographic key sizes*] that meet the following: ISO/IEC 9796-2:2002(Digital Signature Scheme1)[assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

(2). Random Number Generation (FCS_RND.1)

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD

The TSF shall provide a mechanism to generate random numbers that meet [AIS20] of random number according to both NIST FIPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module(statistical test upon demand) and P2 class of [AIS31][assignment: *a defined quality metric*].

Dependencies: No dependencies.

Application note 24: This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4/BAC_MRTD.

5.3.3. Class FIA Identification and Authentication

Application note 25: The Table 5-4 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [7], Annex E, and [22]
Basic Access Control Authentication Mechanism	FIA_UAU.4/MRTD and FIA_UAU.6/MRTD	FIA_UAU.4/BAC_T and FIA_UAU.6/T	Triple-DES, 112 bit keys and Retail-MAC, 112 bit keys
~~Symmetric Authentication Mechanism for Personalization Agents~~	~~FIA_UAU.4/MRTD~~	~~FIA_API.1/SYM-PIN_PT~~	~~Triple-DES with 112 bit keys~~
PIN verification Mechanism for Personalization Agent	FIA_UAU.5/MRTD	FIA_API.1/PIN_PT	plain PIN

Table 5-4 Overview on authentication SFR

The TOE shall meet the requirement “Timing of identification (FIA_UID.1)” as specified below (Common Criteria Part 2).

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

~~(1) to read the Initialization Data in Phase 2 “Manufacturing”,~~

(2) to read the ATQB and ATA~~ATS~~ in Phase 3 “Personalization of the MRTD”,

(3) to read the ATQB and ATA~~ATS if the TOE is configured for use with Basic Inspection Systems only~~ in Phase 4 “Operational Use”,

~~(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 “Operational Use”~~ ~~[assignment: *list of TSF-mediated actions*~~]

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.

Dependencies: No dependencies.

Application note: TOE doesn’t allow to be read the Initialization Data under non-authentication.

The Basic Access Control mechanism is mandatory for the TOE. The TOE doesn’t care the Inspection System which doesn’t have Basic Access Control Mechanism.

The TOE addresses TypeB protocol not TypeA, and the PUPI information of ATQB is not identification data of the Chip because that information is random number not fixed number.

Application note 26: The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System created by writing the Document Basic Access Keys. ~~If the TOE is configured for use Primary Inspection System s any terminal is assumed as Primary Inspection System and allowed to read the logical MRTD. If the TOE is configured for use with Basic Inspection Systems only the Basic Inspection System is identified as default user after power up or reset the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System according to the SFR FIA_UAU.4/BT.~~

Application note: The Basic Access Control mechanism is a mandatory for the TOE.

Application note 27: In the operation phase the MRTD must not allow anybody to read ICCSN or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID).~~ Note that the terminal and the MRTD's chip use an identifier for communication channel to allow the terminal for communication with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification. If this identifier fixed the ST writer should consider the possibility to misuse this identifier to perform attacks addressed by T.Chip_ID.~~

Application note: Any identification data of the TOE is not read before BAC authentication. And the PUPI of TOE is not fixed value (random number is generated in each activation).

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow

~~(1) to read the Initialization Data in Phase 2 "Manufacturing",~~

(2) to read the ATQB and ATA~~ATS~~ in Phase 3 "Personalization of the MRTD",

(3) to read the ATQB and ATA~~ATS if the TOE is configured for use with Basic Inspection Systems only~~ in Phase 4 "Operational Use",

~~(4) to read the logical MRTD if the TOE is configured for use with Primary Inspection System in Phase 4 "Operational Use"~~

~~[assignment: *list of TSF-mediated actions*]~~

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.

Dependencies: FIA_UID.1 Timing of identification.

~~Application note 28: The Primary Inspection System does not authenticate themselves. Only the Basic Inspection System and the Personalization Agent authenticate themselves.~~

Application note: TOE doesn't allow to be read the Initialization Data under non-authentication.
The Basic Access Control mechanism is a mandatory for the TOE. The TOE doesn't care the Inspection System which doesn't have Basic Access Control Mechanism.
The TOE addresses TypeB protocol not TypeA, and the PUPI information of ATQB is not identification data of the Chip because that information is random number not fixed number.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4/MRTD Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.

FIA_UAU.4.1/ MRTD

The TSF shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,

~~2. Authentication Mechanism based on Triple-DES~~[assignment: *identified authentication mechanism(s)*].

Dependencies: No dependencies.

Application note 29: All listed authentication mechanisms uses a challenge of 8 Bytes freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt: the Basic Access Control Authentication Mechanism uses RND.ICC [7], and the Authentication Mechanism based on Triple-DES shall use a Challenge as well.

Application note 30: The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [7]. In the first step the terminal authenticates themselves to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop the communication with the terminal not successfully authenticated in the first step of the protocol to fulfil the security objective OT.Identification and to prevent T.Chip_ID.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

Application note: The TOE addresses the PIN verification Mechanism (not the Symmetric Authentication Mechanism) for the authentication of Personalization

Agent.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism
2. ~~Symmetric Authentication Mechanism based on Triple-DES~~
2. PIN verification Mechanism[assignment: *list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

1. the TOE accepts the authentication attempt as Personalization Agent by the following mechanisms

~~(a) the Basic Access Control Authentication Mechanism with the Personalization Agent Keys,~~

(a) the PIN verification Mechanism with the Personalization Agent Keys

2. the TOE accepts the authentication attempt as ~~Basic~~ Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys[assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

Dependencies: No dependencies.

Application note: The TOE addresses the PIN verification Mechanism (not the Symmetric Authentication Mechanism) for the authentication of Personalization Agent.
Personalization Agent doesn't access to the TOE with Basic Access Control.

Application note 31: Depending on the authentication methods used the Personalization Agent holds (i) ~~a pair of a Triple-DES encryption key and a~~

~~retail-MAC key for the Basic Access Control Mechanism specified in [7], or~~ the key for PIN verification~~(ii) a Triple-DES key for the Symmetric Authentication Mechanism~~. The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use PIN verification ~~Symmetric Authentication Mechanism~~ without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. ~~Note, the successful authenticated Personalization Agent may disable the Basic Access Control Mechanism.~~

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

FIA_UAU.6.1/ MRTD

The TSF shall re-authenticate the user under the conditions each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism[assignment: *list of conditions under which re-authentication is required*].

Dependencies: No dependencies.

Application note 32: The Basic Access Control Mechanism specified in [7] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC_MRTD for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticate the user for each received command and accept only those commands received from the initially authenticated by means of BAC user.

5.3.4. Class FDP User Data Protection

(1). Subset access control (FDP_ACC.1)

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

FDP_ACC.1 Subset access control – Primary Access Control

Hierarchical to: No other components.

~~FDP_ACC.1.1/ PRIM~~

~~The TSF shall enforce the Primary Access Control SFP [assignment: *access control SFP*] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].~~

~~Dependencies: FDP_ACF.1 Security attribute based access control~~

~~Application note 33: The data groups DG1 to DG16 of the logical MRTD as defined in [6] are the only TOE User data. The Primary Access Control SFP address the TOE usage with Primary Inspection Systems and Basic Inspection Systems independent on the configuration of the TOE.~~

~~FDP_ACC.1 Subset access control – Basic Access control~~

~~Hierarchical to: No other components.~~

~~FDP_ACC.1.1/ BASIC~~

~~The TSF shall enforce the Basic Access Control SFP[assignment: *access control SFP*] on terminals gaining write, read and modification access to data groups DG1 to DG16 of the logical MRTD[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].~~

~~Dependencies: FDP_ACF.1 Security attribute based access control~~

~~Application note 34: The Basic Access Control SFP address the configuration of the TOE for usage with Basic Inspection Systems only.~~

FDP_ACC.1.1/MRTD

The TSF shall enforce the SFP.ACCESS_MRTD [assignment: *access control SFP*] on Personalization Agent and Inspection system terminal gaining write and read access to data groups DG1 to DG16 of the logical MRTD[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Dependencies: FDP_ACF.1 Security attribute based access control

(2). Security attribute based access control (FDP_ACF.1)

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 address different SFP.

FDP_ACF.1 Security attribute based access control – Primary Access Control

Hierarchical to: No other components.

~~FDP_ACF.1.1/ PRIM~~

~~The TSF shall enforce the Primary Access Control SFP[assignment: *access control SFP*] to objects based on the~~

~~following:~~

~~1. Subjects:~~

~~a. Personalization Agent,~~

~~b. Terminals,~~

~~2. Objects: data in the data groups DG1 to DG16 of the logical MRTD,~~

~~3. security attributes~~

~~a. configuration of the TOE according to FMT_MOF.1,~~

~~b. authentication status of terminals[assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].~~

~~FDP_ACF.1.2/ PRIM~~

~~The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Primary Inspection Systems~~

~~1. the successfully authenticated Personalization Agent is allowed to write the data of the data groups DG1 to DG16 of the logical MRTD,~~

~~2. the Terminals are allowed to read the data of the groups DG1 to DG16 of the logical MRTD[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].~~

~~FDP_ACF.1.3/ PRIM~~

~~The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].~~

~~FDP_ACF.1.4/ PRIM~~

~~The TSF shall explicitly deny access of subjects to objects based on the rule: the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD[assignment: *rules, based*~~

~~*on security attributes, that explicitly deny access of subjects to objects*].~~

~~Dependencies: FDP_ACC.1 Subset access control~~
~~FMT_MSA.3 Static attribute initialization~~

~~Application note 35: The MRTD access control prevents changes of data groups by write access to the logical MRTD after their creation by the Personalization Agent (i.e. no update of successful written data in the data groups DG1 to DG16). The Passive Authentication Mechanism detects any unauthorised changes.~~

~~FDP_ACF.1/Basic Security attribute based access control – Basic Access Control~~

~~Hierarchical to: No other components.~~

~~FDP_ACF.1.1/ BASIC~~

~~The TSF shall enforce the Basic Access Control SFP[assignment: *access control SFP*] to objects based on the following:~~

~~1. Subjects:~~

~~a. Personalization Agent,~~

~~b. Basic Inspection System,~~

~~c. Terminal,~~

~~2. Objects: data in the data groups DG1 to DG16 of the logical MRTD~~

~~3. Security attributes~~

~~a. configuration of the TOE according to FMT_MOF.1,~~

~~b. authentication status of terminals[assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].~~

~~FDP_ACF.1.2/ BASIC~~

~~The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: in the TOE configuration for use with Basic Inspection~~

~~Systems only~~

~~1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the data groups DG1 to DG16 of the logical MRTD,~~

~~2. the successfully authenticated Basic Inspection System is allowed to read data of the groups DG1 to DG16 of the logical~~ MRTD[assignment: ~~*rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*~~]~~.~~

~~FDP_ACF.1.3/ BASIC~~

~~The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:~~ none[assignment: ~~*rules, based on security attributes, that explicitly authorise access of subjects to objects*~~]~~.~~

~~FDP_ACF.1.4/ BASIC~~

~~The TSF shall explicitly deny access of subjects to objects based on the rule: the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD~~[assignment: ~~*rules, based on security attributes, that explicitly deny access of subjects to objects*~~]~~.~~

~~Dependencies: FDP_ACC.1 Subset access control~~
~~FMT_MSA.3 Static attribute initialization~~

FDP_ACF.1/MRTD MRTD access control

Hierarchical to: No other components.

FDP_ACF.1.1/MRTD

The TSF shall enforce the SFP.ACCESS_MRTD[assignment: *access control SFP*] to objects based on the following:

1. Subjects:

a. Personalization Agent,

b. Inspection System,

2. Objects: data in the data groups DG1 to DG16 of the logical MRTD

3. Security attributes

a. security status

b. Error Counter

c. Error Limit.

Application note: TOE has "the configuration of the TOE according to FMT_MOF.1" as a default function, not an attribute. The function of the Basic Access Control is available by setting Document Basic Access Keys by Personalization Agent.

FDP_ACF.1.2/MRTD

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: as following(Table 5-5, Table 5-6)[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

Table 5-5

subjects	objects	operation	Conditions	Phase
Personalization Agent	DG1-16	read	AST_MRTD.SC1	3
		write*	AST_MRTD.SC1	3
Inspection System	DG1-16	read	AST_MRTD.SC2	4

Table 5-6

Access control policy	Authenticated status
SFP.ACCESS_MRTD	AST_MRTD.SC1
	AST_MRTD.SC2

FDP_ACF.1.3/ MRTD

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/ MRTD

The TSF shall explicitly deny access of subjects to objects based on the rule:

- the Terminals are not allowed to modify any of the data groups DG1 to DG16 of the logical MRTD and
- the Personalization Agent is not allowed to modify any of the data group DG1 to DG16 of the logical MRTD after Phase2[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

Application note: The TOE restricts any user data and any TSF data to be written/modified by any subjects after Phase3.

(3). Inter-TSF-Transfer

Application note 36: FDP_UCT.1/MRTD and FDP_UIT.1/MRTD require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful authentication of the terminal. The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP_UCT.1)” as specified below (Common Criteria Part 2).

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

FDP_UCT.1.1/ MRTD

The TSF shall enforce the SFP.SM_MRTD[assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to transmit and receive[selection: *transmit, receive*] objects in a manner protected from unauthorised disclosure.

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

The TOE shall meet the requirement "Basic data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

Application note: The outsource mechanism addresses only "receive" of the selection because the outsource mechanism (TOE) doesn't send the encrypted data.

FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

FDP_UIT.1.1/ MRTD

The TSF shall enforce the SFP.SM_MRTD[assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to transmit and receive[selection: *transmit, receive*] user data in a manner protected from modification, deletion, insertion and replay[selection: *modification, deletion, insertion, replay*] errors.

Application note: The outsource mechanism addresses only "receive" of the selection because the outsource mechanism (TOE) checks the integrity of received data (issue data).

FDP_UIT.1.2/ MRTD

The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[selection: modification, deletion, insertion, replay] has occurred.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

5.3.5. Class FMT Security Management

The TOE shall meet the requirement "Management of functions in TSF (FMT_MOF.1)" as specified below (Common Criteria Part 2).

FMT_MOF.1 Management of functions in TSF

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to enable ~~and disable~~[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions Basic Access Control[assignment: *list of functions*] to ROL.EP.Perso (Personalization Agent)[assignment: *the authorised identified roles*].

Dependencies: No Dependencies

Application note 37: The enabling (by setting (loading) Document Basic Access Keys) ~~and disabling~~ the TSF Basic Access Control defines the configuration of the TOE in Phase 3 "Personalization of the MRTD" before use in the phase 4 "Operational Use":

~~1. The TOE is configured with Primary Inspection systems when the TSF Basic Access Control is disabled. In this configuration the TOE enforces the Primary Access Control SFP according to FDP_ACC.1/PRIM and FDP_ACF.1/PRIM. In this case the logical MRTD may be read without successful authentication as Basic Inspection System or Personalization Agent.~~

2. The TOE is configured with Basic Inspection Systems only when the TSF Basic Access Control is enabled. In this configuration the TOE enforces the Basic Access Control SFP according to FDP_ACC.1/~~BASIC~~MRTD and FDP_ACF.1/~~ BASIC~~MRTD. In this case the reading of the logical MRTD requires successful authentication as Basic Inspection System or Personalization Agent.

~~It is up to the security target writer to decide whether the disabling of the TSF Basic Access Control is accompanied with the disabling of the Basic Access Control Authentication Mechanism. Even if the TOE will be configured for use in the phase 4 “Operational Use” with Primary Inspection systems the Personalization Agent may use this mechanism with the Personalization Agent Authentication Keys or a Basic Inspection System may use this mechanisms together with secure messaging to protect the logical MRTD against eavesdropping to the communication between TOE and inspection system.~~

Application note: The TOE activates Basic Access Control Mechanism by the Personalization Agent setting Document Basic Access Keys on the TOE.

FMT_MOF.1/Deactive Management of functions in TSF - Deactive

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to ~~enable and ~~disable[selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions of Application Downloading, and Crypto Algorithm[assignment: *list of functions*] to ROL.CARDMAN, ROL.ISSUER1 and ROL.ISSUER2 (Manufacturer)[assignment: *the authorised* *identified roles*].

Dependencies: No Dependencies

Application note 38: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

1. Initialization(Pre-personalization),
2. Personalization,
3. Configuration[assignment: *list of security management functions to be provided by the TSF*].

Dependencies: No Dependencies

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2).

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles

1. ROL.CARDMAN,
2. ROL.ISSUER1,
3. ROL.ISSUER2

4. ROL.EP.Perso [assignment: *the authorised identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: FIA_UID.1 Timing of identification.

Application note: The relation between Subjects and the roles of the TOE is described as follows(Table 5-7).

Table 5-7

subjects	role	note
Manufacturer	ROL.CARDMAN	
	ROL.ISSUER1	
	ROL.ISSUER2	
Personalization Agent	ROL.EP.Perso	

Application note 39: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated

2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.2 Limited availability.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow

1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks.

Dependencies: FMT_LIM.1 Limited capabilities.

Application note 40: The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_ENA

The TSF shall restrict the ability to write[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the Initialization Data and Pre-personalization Data[assignment: *list of TSF data*] to ROL.CARDMAN, ROL.ISSUER1 and ROL.ISSUER2(the Manufacturer)[assignment: *the authorised identified roles*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 41: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is ~~the symmetric cryptographic Personalization Agent Authentication Key~~ the key for PIN verification.

FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data

Hierarchical to: No other components.

FMT_MTD.1.1/ INI_DIS

The TSF shall restrict the ability to disable read access without Basic Access Control for users to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the Initialization Data[assignment: list of TSF data] to ROL.EP.Perso(the Personalization Agent)[assignment: the authorised identified roles].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 42: According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 “Manufacturing” but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by (i) allowing to write these data only once and (ii) blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides an unique identification of the IC which is used to trace the IC in the Phase 2 and 3 “personalization” but is not needed and may be misused in the Phase 4 “Operational Use”. Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_WRITE

The TSF shall restrict the ability to write[selection: change_default, query, modify, delete, clear, [assignment: other operations]] the Document Basic Access Keys and Active Authentication Private Key[assignment: list of TSF data] to ROL.EP.Perso(the Personalization Agent)[assignment: the authorised identified roles].

Dependencies: FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MTD.1/KEY_READ Management of TSF data – Key Read

Hierarchical to: No other components.

FMT_MTD.1.1/ KEY_READ

The TSF shall restrict the ability to read[selection: change_default, query, modify, delete, clear, [assignment: other operations]] the Document Basic Access Keys, Active Authentication Private Key and Personalization Agent Keys[assignment: list of TSF data] to none[assignment: the authorised identified roles].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application note 43: The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys if the Basic Access Control is enabled. Note the Document Basic Access Keys may be used for the Basic Access Control Authentication Mechanism and secure messaging even if the Basic Access Control is disabled (cf. Application note 37).

Application note: The summary table of FMT_MTD.1 is described below (Table 5-8).

Table 5-8

subects	TSF data	restrict the ability to	note
Manufacturer	Initialization Data Pre-Personalizationdata	write	INI_ENA
Personalization Agent	Initialization Data (IC Identification Data)	disable read access without Basic Access Control for users	INI_DIS
Personalization Agent	Document Basic Access Keys Active Authentication Private Key	Write	KEY_WRITE
none	Document Basic Access Keys Active Authentication Private Key Personalization Agent Keys	Read	KEY_READ

5.3.6. Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFR "Non-bypassability of the TSP (FPT_RVM.1)" and "TSF domain separation (FPT_SEP.1)" together with "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement "Subset information flow control (FDP_IFC.1)" as specified below:

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1

The TOE shall not emit electromagnetic emissions[assignment: *types of emissions*] in excess of levels which could be measured and analyzed[assignment: *specified limits*] enabling access to Personalization Agent Keys, Document Basic Access Keys and Active Authentication Private Key [assignment: *list of types of TSF data*] and none[assignment: *list of types of user data*].

Application note: STMicroelectronics assigns "none" in [assignment: *list of types of user data*].

FPT_EMSEC.1.2

The TSF shall ensure any unauthorized users[assignment: *type of users*] are unable to use the following interface smart card circuit contacts[assignment: *type of connection*] to gain access to Personalization Agent Keys[assignment: *list of types of TSF data*] and none[assignment: *list of types of user data*].

Dependencies: No other components.

Application note 44: The ST writer shall perform the operation in FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The MRTD's chip has to provide a smart card contactless interface~~ but may have also (not used by the terminal but maybe by an attacker) additional contacts according to ISO/IEC 7816-2 as well~~. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

Application note: The TOE (IC sheet) has only contact-less interface physically.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below (Common Criteria Part 2).

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) Exposure to operating conditions where therefore a malfunction could occur,,

(2) failure detected by TSF according to FPT_TST.1[assignment: *list of types of failures in the TSF*].

Dependencies: ADV_SPM.1 Informal TOE security policy model

The TOE shall meet the requirement "TSF testing (FPT_TST.1)" as specified below (Common Criteria Part 2).

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests as follws(Table 5-9)[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]*] to demonstrate the correct operation of the TSF. operation of as follws(Table 5-9)[selection: *[assignment: parts of TSF], the TSF*].

Table 5-9

parts of TSF/the TSF	timing	note
EEPROM/RAM	during initial start	functional check
random number generation	during initial start	GUN checking
internal clock	during initial start	check internal clock in register P6
configuration status	during initial start	check configuration status(mode*) in regster P1 *: defined by STMicroelectronics
security status	during initial start	check security status* in

		register P4 *: detecting NMI in previous session

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of as follows(Table 5-10)[selection: [assignment: *parts of TSF*], TSF data].

Table 5-10

parts of TSF/TSF data	how to check	note
IEF data	CRC	key data on EEPROM
EF/DF directory data	CRC	attribute data of EF/DF on EEPROM
system flag/directory	CRC	function flag, configuration data, etc. on EEPROM
Security status	CRC	security status on RAM

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing.

Application note: The descriptions of FPT_TST.1.1 and FPT_TST.1.2 are changed according to [2].

Application note 45: The ST writer shall perform the operation in FPR_TST.1.1. If the MRTD's chip uses state of the art smart card technology it will run the some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the "authorised user" Manufacturer in the Phase 2 Manufactoring. Other self tests may run automatically to detect failure and to preserve of secure state according to

FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operation claimed by the concrete product under evaluation.

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below (Common Criteria Part 2).

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[assignment: *physical tampering scenarios*] to the TSF[assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

Application note 46: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

The following security functional requirements protect the TSF against bypassing. and support the separation of TOE parts.

The TOE shall meet the requirement "Non-bypassability of the TSP (FPT_RVM.1)" as specified below (Common Criteria Part 2).

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

The TOE shall meet the requirement “TSF domain separation (FPT_SEP.1)” as specified below (Common Criteria Part 2).

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC

Dependencies: No dependencies.

Application note 47: The parts of the TOE which support the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” should be protected from interference of the other security enforcing parts of the MRTD’s chip Embedded Software.

5.4. Security Assurance Requirements for the TOE

Differences between this security target and [PP0017] about SFRs in chapter 5.4 are described with blue color.

The for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ACM_SCP.3, ADV_IMP.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2 ATE_TAT.2, and AVA_VLA.3

The minimum strength of function is SOF-high.

Application note 48: The high minimum strength of function covers but is not limited to the TSF required by the SFR FIA_UAU.4, FCS_RND.1 and FPT_FLS.1 as far as probabilistic or permutational mechanisms are involved, e.g. due to challenges generated by the TOE and sent to the terminal or probabilistic self tests.

This security target does not contain any security functional requirement for which an explicit stated strength of function claim is required.

5.5. Security Requirements for the IT environment

This section describes the security functional requirements for the IT environment using the CC part 2 components.

Due to CCIMB Final Interpretation #58 these components are editorial changed to express the security requirements for the components in the IT environment where the original components are directed for TOE security functions. The editorial changes are indicated in bold.

Differences between this security target and [PP0017] about SFRs in chapter 5.5 are described with blue color.

5.5.1. Passive Authentication

The ICAO, the Issuing States or Organizations and the Receiving States or Organization run a public key infrastructure for the Passive Authentication. This public key infrastructure distributes and protects the Country Signing CA Keys and the Document Signing Keys to support the signing of the User Data (DG1 to DG16) by means of the Document Security Object. The Technical Report [7] describes the requirements to the public key infrastructure for the Passive Authentication.

The Document Signer of the Issuing State or Organization shall meet the requirement “Basic data authentication (FDP_DAU.1)” as specified below (Common Criteria Part 2).

FDP_DAU.1/DS Basic data authentication – Passive Authentication

Hierarchical to: No other components.

FDP_DAU.1.1/ DS

The Document Signer shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical the MRTD (DG1 to DG16) and the Document Security Object[assignment: *list of objects or information types*].

FDP_DAU.1.2/ DS

The Document Signer shall provide Inspection Systems of Receiving States or Organization[assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

Dependencies: No dependencies

5.5.2. Inspection Systems

This section describes common security functional requirements to the Inspection Systems. This are called “Basic Terminals” (BT) in this section.

The Basic Terminal shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

FCS_CKM.1/BAC_BT Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal

Hierarchical to: No other components.

FCS_CKM.1.1/ BAC_BT

The Basic Terminal shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes 112 bit[assignment: *cryptographic key sizes*] that meet the following: [7], Annex E[assignment: *list of standards*].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FDP_ITC.2 Import of user data with security attributes, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Application note 49: The terminals derive the Document Basic Access Keys from the second line of the printed MRZ data by the algorithm described in [7], 3.2.2 and Annex E.1, use them to generate the Document Basic Access Keys. The Personalization Agent downloads these keys to the MRTD's chip as TSF data for FIA_UAU.4/BAC_MRTD.

Application note: The entropy of the printed MRZ data shall be kept 56 bits as minimum.

FCS_CKM.4/BT Cryptographic key destruction - BT

Hierarchical to: No other components.

FCS_CKM.4.1/BT

The Basic Terminal shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with zeros or random data [assignment: *cryptographic key destruction method*] that meets the following: none[assignment: *list of standards*].

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]
FMT_MSA.2 Secure security attributes

Application note 50: The ST writer shall perform the operation in FCS_CKM.4.1/BT. The basic terminal shall destroy the Document Basic Access Keys of the MRTD and the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging after inspection of the MRTD.

Application note: The basic terminal also addresses the destruction of Active Authentication Public Key.

The Basic Terminal shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic algorithms to be implemented by the Basic Terminal.

FCS_COP.1/SHA_BT Cryptographic operation – Hash Function by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_BT

The Basic Terminal shall perform hashing[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithms SHA-1[assignment: *cryptographic algorithm*] and cryptographic key sizes none[assignment: *cryptographic key sizes*] that meet the following: FIPS 180-2[assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

Application note 51: This SFR requires the terminal to implement the hash function SHA-1 for the cryptographic primitive to generate the Document Basic Access Keys according to FCS_CKM.1/BAC_BT.

FCS_COP.1/ENC_BT Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ ENC_BT

The Basic Terminal shall perform secure messaging – encryption and decryption[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[assignment: *cryptographic algorithm*] and cryptographic key sizes 112 bit[assignment: *cryptographic key sizes*] that meet the following: FIPS 46-3, ISO 11568-2, ISO 9797-1 (padding mode 2) [assignment: *list of standards*].

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
FMT_MSA.2 Secure security attributes

Application note 52: This SFR requires the Basic Terminal to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The key is agreed between the TOE and the terminal during the execution of the Basic Access Control Authentication Mechanism. The key size of 112 bit is chosen to resist attacks with high attack potential.

FCS_COP.1/MAC_BT Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_BT

The Basic Terminal shall perform secure messaging – message authentication code[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm Retail-MAC[assignment: *cryptographic algorithm*] and cryptographic key sizes 112 bit[assignment: *cryptographic key sizes*] that meet the following: FIPS 46-3, ISO 9797 (MAC algorithm 3, block cipher DES, zero IV 8 bytes, padding mode 2) [assignment:

list of standards].

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
FMT_MSA.2 Secure security attributes

Application note 53: This SFR requires the terminal to implement the cryptographic primitive for secure messaging with message authentication code over the transmitted data. The key is agreed or defined as the key for secure messaging encryption. The key size of 112 bit is chosen to resist attacks with high attack potential.

The Basic Terminal shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

FCS_COP.1/RSA_BT Cryptographic operation – Active Authentication by the Basic Terminal

Hierarchical to: No other components.

FCS_COP.1.1/ RSA_BT

The Basic Terminal shall perform verification of signature according to Active Authentication Mechanism[7] Annex[assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm RSA[assignment: *cryptographic algorithm*] and cryptographic key sizes 1024 bit[assignment: *cryptographic key sizes*] that meet the following: ISO/IEC 9796-2:2002 [assignment: *list of standards*].

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

FMT_MSA.2 Secure security attributes

FCS_RND.1/BT Quality metric for random numbers - Basic Terminal

Hierarchical to: No other components.

FCS_RND.1.1/BT

The Basic Terminal shall provide a mechanism to generate random numbers that meets [assignment: *a defined quality metric*].

Dependencies: No dependencies.

Application note 54: The ST writer shall perform the operation in FCS_RND.1.1/BT. This SFR requires the terminal to generate random numbers used in the authentication protocols as required by FCS_CKM.1/BAC_BT and FIA_UAU.4 The quality metric shall be chosen to ensure at least the strength of function Basic Access Control Authentication for the challenges.

The Basic Terminal shall meet the requirements of “Single-use authentication mechanisms (FIA_UAU.4)” as specified below (Common Criteria Part 2).

FIA_UAU.4/BT Single-use authentication mechanisms – Basic Terminal

Hierarchical to: No other components.

FIA_UAU.4.1/BT

The Basic Terminal shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism[assignment: *identified authentication mechanism(s)*].

Dependencies: No dependencies.

Application note 55: The Basic Access Control Authentication Mechanism [7] uses a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by a MRTD's chip and of the session keys from a successful run of authentication protocol.

The Basic Terminal shall meet the requirement "Re-authentication (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6/BT Re-authentication - Basic Terminal

Hierarchical to: No other components.

FIA_UAU.6.1/BT

> The Basic Terminal shall re-authenticate the user under the conditions <u>each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism</u>[assignment: *list of conditions under which re-authentication is required*].

Dependencies: No dependencies.

Application note 56: The Basic Access Control Mechanism specified in [7] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The terminal checks by secure messaging in MAC_ENC mode each MRTD's chip response to a command based on Retail-MAC whether it was sent by the successfully authenticated MRTD's chip. The authentication fails if any response is received with incorrect message authentication code.

Application note 57: The Basic Access Control SFP of the TOE requires to protect the User Data by access control (cf. FDP_ACC.1/BASIC and FDP_ACF.1/BASIC) and by secure messaging (cf. FDP_UCT.1/MRTD and FDP_UIT.1/MRTD) for the communication between the TOE and the Basic Terminal. This secure messaging requires the Basic Terminal to support the protection of the TOE data by decryption and checking MAC and to protect its own data by secure messaging as well. The SFP of the Basic Terminal drawn from the TOE "Basic Access Control SFP" is named "BT part of Basic Access Control SFP" and the related SFR is described by FDP_UCT.1/BT and FDP_UIT.1/BT corresponding to FDP_UCT.1/MRTD and

FDP_UIT.1/MRTD of the communication partner (i.e. the TOE). Note the Basic Terminal does not enforce any named access control policy or information control policy to be defined by FDP_ACC and FDP_ACF or FDP_IFC and FDP_IFF families (respectively). The authentication mechanisms as part of Basic Access Control Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging.

The Basic Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UCT.1/BT Basic data exchange confidentiality - Basic Terminal

Hierarchical to: No other components.

FDP_UCT.1.1/BT

The Basic Terminal shall enforce the BT part of SFP.SM_MRTD[assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to transmit and receive[selection: *transmit, receive*] objects in a manner protected from unauthorised disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

The Basic Terminal shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UIT.1/BT Data exchange integrity - Basic Terminal

Hierarchical to: No other components.

FDP_UIT.1.1/BT

The Basic Terminal shall enforce the BT part of

SFP.SM_MRTD[assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to transmit and receive[selection: *transmit, receive*] user data in a manner protected from modification, deletion, insertion and replay[selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2/BT

The Basic Terminal shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[selection: *modification, deletion, insertion, replay*] has occurred.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

5.5.3. Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

(1) ~~The Basic Access Control Mechanism which may be used by the Personalization Agent with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the personalization terminal may be listen or manipulated.~~

(2) In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to ~~symmetric authentication~~ PIN verification of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple protocol as requested by the SFR

FIA_UAU.4/MRTD and FIA_API.1/~~SYM~~PIN_PT.

The Personalization Terminal shall meet the requirement “Authentication Prove of Identity (FIA_API)” as specified below (Common Criteria Part 2 extended).

FIA_API.1/~~SYM~~PIN_PT Authentication Proof of Identity - Personalization Terminal Authentication with ~~Symmetric~~ Key

Hierarchical to: No other components.

FIA_API.1.1/ ~~SYM~~PIN_PT

The Personalization Terminal shall provide a Authentication Mechanism based on ~~Triple-DES~~ PIN verification[assignment: *authentication mechanism*] to prove the identity of the Personalization Agent[assignment: *authorized user or rule*].

Dependencies: No dependencies.

Application note: The TOE needs PIN verification (not symmetric cryptographic mechanisms) for Personalization Agent.

~~Application note 58: The Symmetric Authentication Mechanism for Personalization Agents is intended to be used in a high secure personalization environment only. It uses the symmetric cryptographic Personalization Agent Authentication Secret key of 112 bits to encrypt a challenge of 8 Bytes with Triple-DES which the terminal receives from the MRTD’s chip e.g. as response of a GET CHALLENGE. The answer may be sent by means of the EXTERNAL AUTHENTICATE command according to ISO 7816-4 [23] command. In this case the communication may be performed without secure messaging (note that FIA_UAU.5.2 requires secure messaging only after run of Basic Access Control Authentication).~~

6. TOE security assurance requirements

This chapter describes the TOE security assurance requirements.

This security target claims EAL4 augmented with ACM_SCP.3, ADV_IMP.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, and AVA_VLA.3.

7. TOE summary specification

This chapter presents the overview specification of TOE functions.

7.1. MRTD application flow and TOE security functions

The overview of MRTD application flow (or issuing information) is described as follows. This flow addresses the primary TOE security functions with relation of procedure of this flow. The TSF which is used at various places (e.g. SF_TEST, SF_CRYPTO etc.) is omitted on this flow.

7.1.1. Phase2: Manufacturer

The outline of issuing component related to
- Initialization & Pre-personalization (MRTD manufacturer)

in Phase2 is described below.

Table 7-1

Issue	Outline of component	related primary TSF
Initialization	formatting and partitioning EEPROM with outsouce	SF_SM
	setting keys for ROL.ISSUER1 and ROL.ISSUER2 with outsouce	SF_SM
	changing **lifecycle** of TOE with outsouce	SF_SM SF_LIFECYCLE
	creating MRTD application with outsouce	SF_SM
	writing IC Identification Data (MRTD)	

Pre-personalization	setting Personalization Agent Keys	

Application note: The security policy configuration managed by SF_MASEC is completed in IC manufacturer and never changed after IC manufacturer.

7.1.2. Phase3: Personalization of the MRTD

The overview of MRTD application flow in Phase3(subject: Personalization Agent) is described below(Figure 7-1).

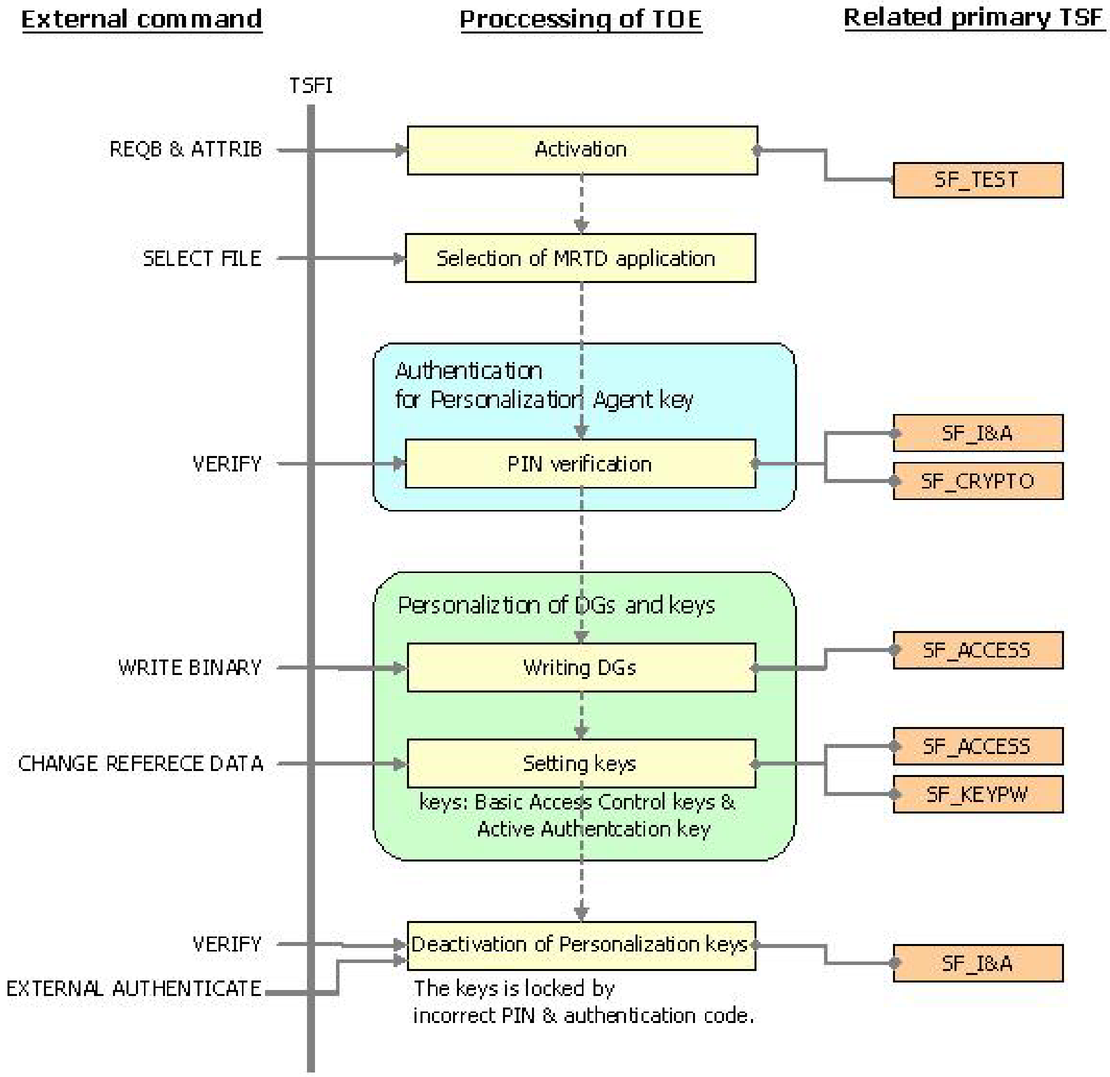

Figure 7-1

7.1.3. Phase4: Operational Use

The overview of MRTD application flow in Phase4(subject: Inspection System) is described below(Figure 7-2).

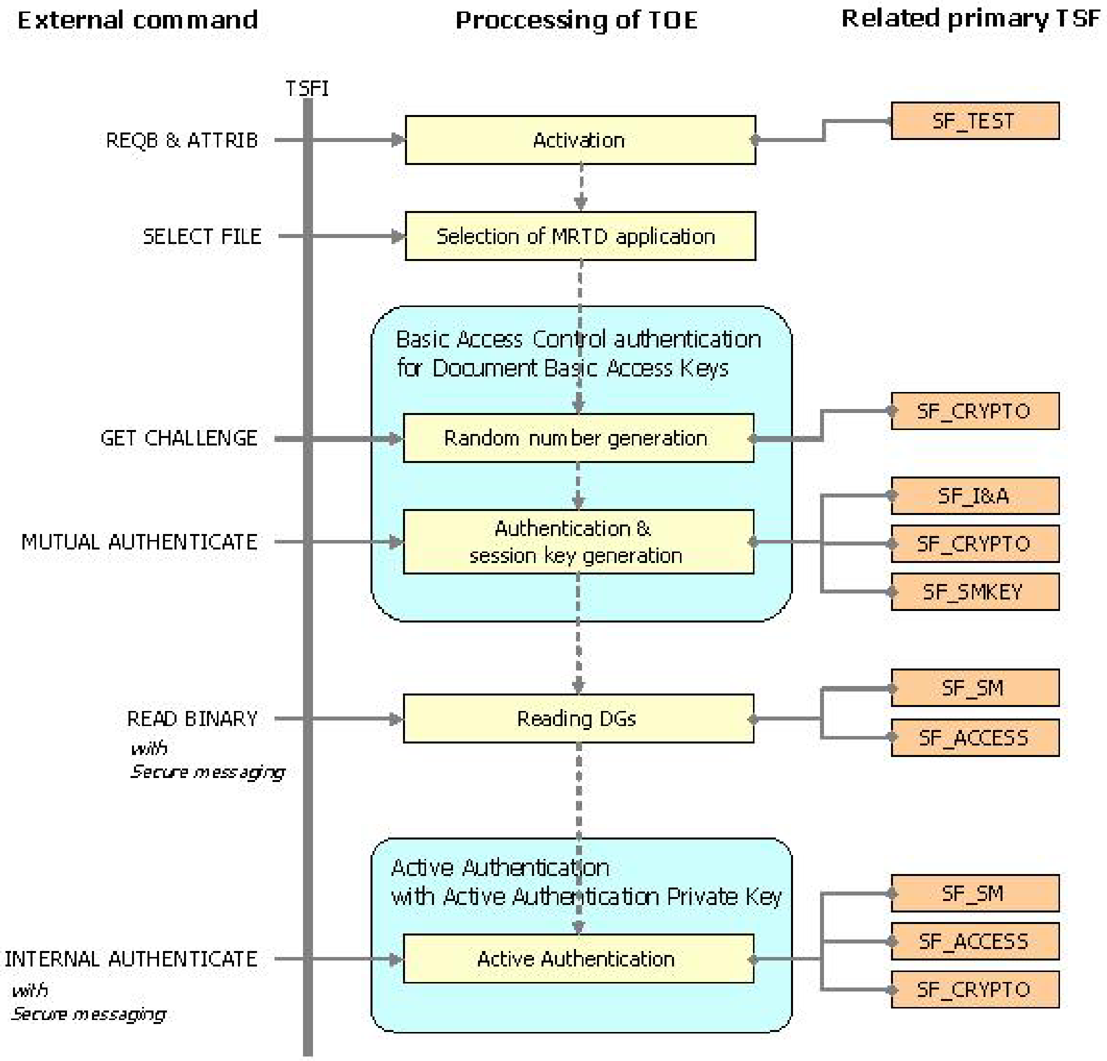
External command
Proccessing of TOE
Related primary TSF
TSFI
REQB & ATTRIB
Activation
SF_TEST
SELECT FILE
Selection of MRTD application
Basic Access Control authentication for Document Basic Access Keys
GET CHALLENGE
Random number generation
SF_CRYPTO
MUTUAL AUTHENTICATE
Authentication & session key generation
SF_I&A
SF_CRYPTO
SF_SMKEY
READ BINARY with Secure messaging
Reading DGs
SF_SM
SF_ACCESS
Active Authentication with Active Authentication Private Key
INTERNAL AUTHENTICATE with Secure messaging
Active Authentication
SF_SM
SF_ACCESS
SF_CRYPTO

Figure 7-2

7.2. Overview of TOE file structure

The file structure of TOE is described below.

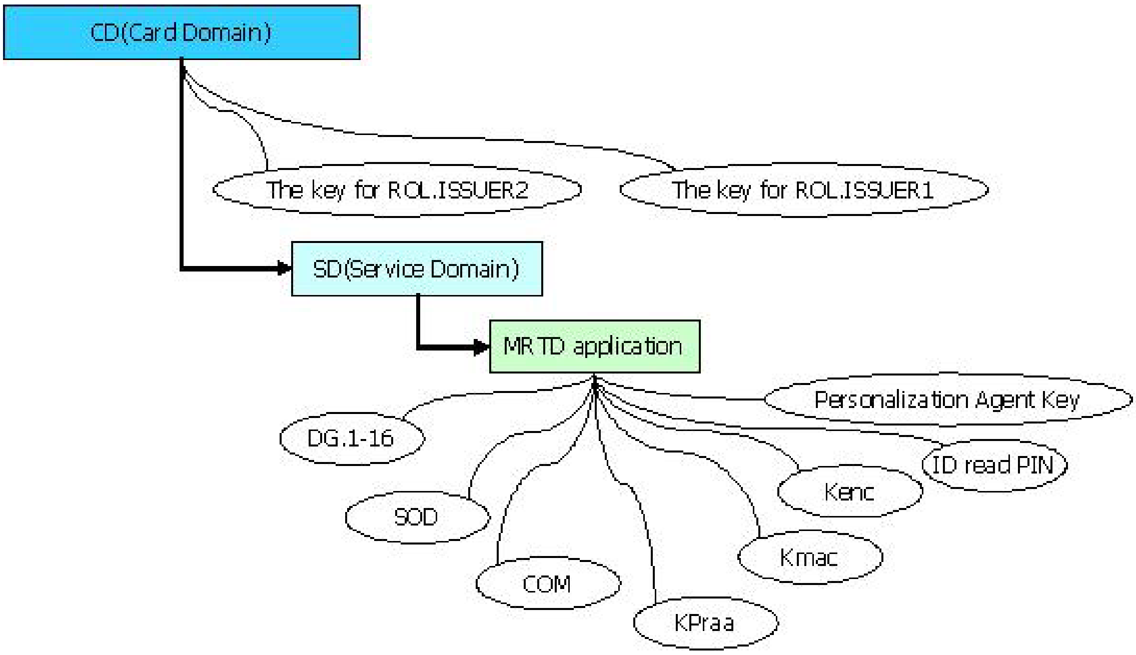

Figure 7-3

DF	No	componet	note
CD(Card Domain)			
	1	The key for ROL.ISSUER1	
	2	The key for ROL.ISSUER2	
SD(Service Domain)			
MRTD application			
	3	The key for ROL.EP.PersoPIN	Personalization Agent Key
	4	ID read PIN	for IC identification data
	5	Kenc	Document Basic Access Key(K_ENC)
	6	Kmac	Document Basic Access Key(K_MAC)
	7	KPraa	Active Authentication Private Key
	8	DG.1-16	Data group
	9	SOD	Document security object
	10	COM	common information

Table 7-2

7.3. TOE security functions

This chapter describes

- the specifications of TOE security functions and
- the traceability(linkage) between TOE security functions and TOE security functional requirements.

The TOE security functions related to Xaica-PF and MRTD application

7.3.1. SF_I&A

The outline of SF_I&A and the explanation of each function that SF_I&A provides are described below (Table 7-3).

Table 7-3

TOE security function	**SF_I&A**		
Outline	SF_I&A provides the functionality related to the authentication and the identification for the subjects. If authentication is succeeded, SF_I&A updates the security status for related key.		
No	**SFR**		**Note**
1	FIA_UID.1	Timing of identification	
2	FIA_UAU.1	Timing of authentication	
3	FIA_UAU.4/MRTD	Single-use authentication mechanisms	
4	FIA_UAU.5/MRTD	Multiple authentication mechanisms	
5	FPT_EMSEC.1	TOE Emanation	

7.3.2. SF_ACCESS

The outline of SF_ACCESS and the explanation of each function that SF_ ACCESS provides are described below (Table 7-4).

Table 7-4

TOE security function	SF_ACCESS
Outline	SF_ACCESS provides the functionality to allow only authorized user to access object with referring some statuses and attributes. And SF_ACCESS addresses two access control function. One is the generic access control function of Xaica-PF that can be commonly used by all application. The other is the dedicated access control function of MRTD application that be used by MRTD application only.

No	SFR		Note
1	FAU_SAS.1	Audit storage	
2	FDP_ACC.1/MRTD	Subset access control	
3	FDP_ACF.1/ MRTD	Security attribute based access control	
4	FMT_MOF.1	Management of functions in TSF	
5	FMT_MOF.1/Deactive	Management of functions in TSF	
6	FMT_SMR.1	Security roles	
7	FMT_LIM.1	Limited capabilities	
8	FMT_LIM.2	Limited availability	
9	FMT_MTD.1/INI_ENA	Management of TSF data	
10	FMT_MTD.1/INI_DIS	Management of TSF data	
11	FMT_MTD.1/KEY_WRITE	Management of TSF data	
12	FMT_MTD.1/KEY_READ	Management of TSF data	

7.3.3. SF_CRYPTO

The outline of SF_CRYPTO and the explanation of each function that SF_CRYPTO provides are described below (Table 7-5).

Table 7-5

TOE security function	SF_CRYPTO		
Outline	SF_CRYPTO provides the functionality related to the cryptographic functions with security features. T-DES(2Key), RSA1024bit(CRT), Random number generation and SHA-1 are provided as primary function.		
No	SFR		Note
1	FCS_COP.1/SHA_MRTD	Cryptographic operation	
2	FCS_COP.1/TDES_MRTD	Cryptographic operation	
3	FCS_COP.1/MAC_MRTD	Cryptographic operation	
4	FCS_COP.1/RSA_MRTD	Cryptographic operation	
5	FCS_RND.1/MRTD	MRTD Quality metric for random numbers	
6	FPT_EMSEC.1	TOE Emanation	
7	FPT_RVM.1	Non-bypassability of the TSP	

7.3.4. SF_LIFECYCLE

The outline of SF_LIFECYCLE and the explanation of each function that SF_LIFECYCLE provides are described below (Table 7-6).

Table 7-6

TOE security function	**SF_LIFECYCLE**		
Outline	SF_LIFECYCLE provides the functionality to manage the status of TOE itself (card-status). SF_LIFECYCLE depending on SF_ACCESS allows only authorized user to change card-status according to SFP.ACCESS.		
No	**SFR**		**Note**
1	FMT_SMF.1	Specification of Management Functions	
2	FMT_SMR.1	Security roles	

7.3.5. SF_SM

The outline of SF_SM and the explanation of each function that SF_SM provides are described below (Table 7-7).

Table 7-7

TOE security function	**SF_SM**		
Outline	SF_SM provides the functionality related to the secure messaging (of Basic Access Control mechanism) which has functions of encrypting/decrypting command and message authentication (retail MAC).		
No	**SFR**		**Note**
1	FIA_UAU.6/MRTD	Re-authenticating	
2	FDP_UCT.1/MRTD	Basic data exchange confidentiality	
3	FDP_UIT.1/MRTD	Data exchange integrity	

7.3.6. SF_SMKEY

The outline of SF_SMKEY and the explanation of each function that SF_SMKEY provides are described below (Table 7-8).

Table 7-8

TOE security function	SF_SMKEY		
Outline	SF_SMKEY provides the functionality to manage the session keys generated by MUTUAL AUTHENTICATE command (of Basic Access Control mechanism), which has functions of session key generation(distribution) and session key destruction(erasing).		
No	SFR		Note
1	FCS_CKM.1/BAC_MRTD	Cryptographic key generation	
2	FCS_CKM.4	Cryptographic key destruction	

7.3.7. SF_KEYPW

The outline of SF_KEYPW and the explanation of each function that SF_KEYPW provides are described below (Table 7-9).

Table 7-9

TOE security function	SF_KEYPW	
Outline	SF_KEYPW provides the functionality to manage the key stored on TOE. SF_KEYPW depending on SF_ACCESS allows only authorized user to set the key according to SFP.ACCESS.	
No	SFR	Note

1	FMT_MOF.1	Management of functions in TSF	
2	FMT_SMF.1	Specification of Management Function	
3	FMT_SMR.1	Security roles	
4	FMT_MTD.1/KEY_WRITE	Management of TSF data	

7.3.8. SF_MASEC

The outline of SF_MASEC and the explanation of each function that SF_MASEC provides are described below (Table 7-10).

Table 7-10

TOE security function	SF_MASEC		
Outline	SF_MASEC provides the functionality to manage the security policy configuration for TOE. The security policy configurations primarily consist of application downloading policy, cryptographic usage policy and test features usage policy, which could be changed by SET CONFIGURATION command if needed.		
No	SFR		Note
1	FMT_MOF.1/Deactive	Management of functions in TSF	
2	FMT_SMF.1	Specification of Management Function	
3	FMT_SMR.1	Security roles	
4	FMT_LIM.1	Limited capabilities	
5	FMT_LIM.2	Limited availability	

7.3.9. SF_TEST

The outline of SF_TEST and the explanation of each function that SF_TEST provides are described below (Table 7-11).

Table 7-11

TOE security function	**SF_TEST**		
Outline	SF_TEST provides the functionality to self-test hardware, operations and integrity of data and change its state to secure state.		
No	**SFR**		**Note**
1	FPT_TST.1	TSF testing	
2	FPT_RVM.1	Non-bypassability of the TSP	
3	FPT_FLS.1	Failure with preservation of secure state	

The TOE security functions related to the chip by STMicroelectronics

7.3.10. SF_CONFIG_A: TOE configuration switching and control

In TEST, ISSUER and USER configurations, this functionality ensures the switching and the control of TOE configuration.

This functionality ensures that the TOE is either in TEST, ISSUER or USER configuration.

The only auhorised TOE configuration modifications are:

- TEST to ISSUER configuration by TEST administrator.
- ISSUER to USER configuration by ISSUER administrator.

This functionality is responsible for the TOE configuration detection and notification to the other resources of theTOE.

7.3.11. SF_INIT_A: Hardware Initialisation & TOE attribute initialisation

In TEST, ISSUER and USER configurations, this functionality ensures he following:

- he TOE starts running in a secure slate,
- he TOE is securely initialised,
- he reset operation is correctly managed.

7.3.12. SF_INT_A: TOE logical integrity

This functionality is responsible for the following operations, performed according to actual TOE configuration:

- NVM, USR-ROM and ST-ROM integrity content verifications in TEST and ISSUER configurations,
- valid CPU usage and stack overflow verification in TEST, ISSUER and USER configurations.
- for correcting single bit fails upon a read operation,
- other actions are not described here.

This functionality is responsible for reporting to SF_ADMINIS_A detected errors on

CPU usage, stack overflow and EEPROM.

7.3.13. SF_FWL_A: Storage and Function Access Firewall

TOE memories are partitioned. This portioning is partially defined by the TOE user and partially by STM:

- ST-ROM mapping is STM defined,
- USR_ROM mapping is user defined,
- RAM and NVM mappings are partly STM defined and partly user defined.

In TEST, ISSUER and USER configurations, this security functionality monitors:

- access from memory locations to other locations for ROM. PAM and NVM,
- NVM use,
- register access,

and is responsible for the notification of violation attempts to SF_ADMINIS_A.

An access can be:

- a read, to registers, ROM, RAM or NVM,
- a write, to registers or RAM,
- a program, to NVM,
- an erase, to NVM.

Executability, Read, Write, Program and Erase right classes are defined by the user and STM for ROM, RAM and NVM.

7.3.14. SF_PHT_A: Physical tampering security function

In TEST, ISSUER and USER configurations, this functionality ensures the following:

- the TOE detects clock and voltage supply operating changes by the environment,
- the TOE detects attempts to violate its physical integrity,
- the TOE is always clocked with shape and timing within specified operating conditions.

7.3.15. SF_ADMINIS_A: Security violation administrator

In TEST, ISSUER and USER configurations, this functionality ensures the management of security violations attempts.

The security violations attempts which are managed are:

- access to unavailable or reserved memory locations,
- unauthorised access to user memories,
- unauthorised access to STM memories,
- bad CPU usage,
- bad NVM use,
- EEPROM single bit fails,
- clock and voltage supply operating changes,
- TOE physical integrity abuse

7.3.16. SF_SKCS_A: Symmetric Key Cryptography Support

In USER configuration, this security function implements the following standard symmetric key cryptography algorithms:

- Data Encryption Standard (DES) with 64 bits long keys (56 effective bits).
- This functionality supports the following standard modes of operation, both for encryption and for decryption:
- DES by itself,
- Triple DES, chaining two DES encryption and one DES decryption.

Each of these modes of operation can be changed in the standard Cipher Block Chaining mode (CBC). In the encryption operation mode, this function can compute either a 64 bits long Message Authentication Code (MAC) or the encrypted data.

This functionality implements the following standard symmetric key cryptography algorithms:

- Advanced Encryption Standard (AES) with 128 bits long keys, 128 bits long blocks, 10 rounds, providing cipher, Inverse cipher and key expansion operations.

When provided, this SF implements software and hardware counter-measures to limit or eliminate information leakage.

7.3.17. SF_AKCS_A: Asymmetric Key Cryptography Support

In USER configuration, this security function implements the following standard asymmetric key cryptography algorithms:

- RSA verification (encryption) with an RSA modulo up to 1088 bits,
- RSA verification (encryption) with an RSA modulo up to 2176 bits,
- RSA signature (decryption) without the Chinese Remainder Theorem (CRT), with an RSA modulo up to 1088 bits,
- RSA signature (decryption) with the Chinese Remainder Theorem (CRT), with an RSA modulo up to 2176 bits,
- RSA secret and public keys computation with an RSA modulo up to 2176 bits,
- Prime number and RSA prime number generation up to 1088 bits, with Rabin Miller primality tests.

In USER configuration, this security function implements the following standard hash function:

- SHA-I hash function chaining blocks of 512 bits to get a 160 bits result

When provided, this SF implements software and hardware counter-measures to limit or eliminate information leakage.

7.3.18. SF_ALEAS_A: Unpredictable Number Generation Support

In all configurations, this securily function provides two unpredictable and unrelated 8 bits numbers..

In ISSUER and USER configurations, this security function supports the prevention of information leakage.

This security function ensures the generation of unpredictable numbers of 1088 bits, in USER configuration.

This security function can be qualified, with:

- the test metrics required by he NlST FlPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module (statistical test upon demand),
- the test metrics required by the BSI-AIS31 standard for a P2 class device.

8. PP claims

This security target does not claim any protection profile.

This security target references the Protection Profile Machine Readable Travel Document with ICAO Application and Basic Access Control, Version 1.0, BSI-PP-0017 [21a].

9. Rationale

The whole the description of Rationale is omitted to keep NTTDATA Corporation property confidential.

10. Glossary and Acronyms

Glossary and acronyms are described in this chapter.

10.1. Glossary

The glossary based on BSI-PP0017[21a] is described in Table 10-1.

Table 10-1

Term	Definition
Active Authentication	Security mechanism defined in [7] option by which means the MTRD ' s chip proves and the inspection system verifies the identity and authenticity of the MTRD ' s chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD ' s chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [7] by which means the MTRD ' s chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Inspection System	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD ' s chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD and the terminals part of the Active Authentication Mechanism and verificates signature from MRTD using the Active Authentication Public key of MRTD.
~~*Basic Inspection System (BIS)*~~	~~An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD ' s chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.~~
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [8]
biometric reference	Data stored for biometric authentication of the MRTD holder in the MRTD ' s chip as (i) digital portrait and (ii) optional biometric reference

data	data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [8]
Country Signing CA Certificate (CCSCA)	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD ' s chip and the inspection system [7]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SOD)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD ' s chip. It may carry the Document Signer Certificate (CDS). [7]
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD 's chip and the inspection system to gain the data on the MRTD ' s chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [9]
Extended Access Control	Security mechanism identified in [7] by which means the MTRD ' s chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [8]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [9]
IC Dedicated	That part of the IC Dedicated Software (refer to above) which provides

Support Software	functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person ' s document. [8]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else ' s travel document or visa; or (d) no travel document or visa, if required. [9]
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD ' s material (IC identification data).
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity. [9]
Inspection system (IS)	A 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.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD ' s chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD ' s chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [6]
Issuing State	The Country issuing the MRTD. [6]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [6]. The capacity expansion technology used is the MRTD ' s chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, DG1), (3) the digitized portraits (DG2), (4) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (5) the other data according to LDS (DG5 to DG16).

Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	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. [6]
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [6]
Machine readable zone (MRZ)	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. [6]
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [8]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD ' s chip. It includes - the file structure implementing the LDS [6], - the definition of the User Data, but does not include the User Data itself (i.e. content of DG1 to DG14 and DG 16) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD ' s chip based on MRZ information as key seed and access condition to data stored on MRTD ' s chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD ' s Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAOT, [10], p. 14.
MRTD ' s chip Embedded Software	Software embedded in a MRTD 's chip and not being developed by the IC Designer. The MRTD ' s chip Embedded Software is designed in Phase 1 and embedded into the MRTD ' s chip in Phase 2 of the TOE life-cycle.
Optional biometric	Data stored for biometric authentication of the MRTD holder in the

reference data	MRTD ' s chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document. [8]
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/~~SYM~~PIN_PT and (ii) by the MRTD ' s chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD 's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Keys.
Pre-personalized MRTD ' s chip	MRTD ' s chip equipped with an unique identifier and an unique asymmetric Active Authentication Key Pair of the chip.
Primary Inspection System (PIS)	A inspection system that contains a terminal for the contactless communication with the MRTD ' s chip and does not implement the terminals part of the Basic Access Control Mechanism.
Receiving State	The Country to which the MRTD holder is applying for entry. [6]
reference data	Data enrolled for a known identity and used by the verifier to check the

	verification data provided by an entity to prove this identity in an authentication attempt.
secondary image	A repeat image of the holder ' s portrait reproduced elsewhere in the document by whatever means. [8]
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Travel document	A passport or other official document of identity issued by a State or organi-zation, which may be used by the rightful holder for international travel. [9]
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD ' s chip.
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee ' s template. [9]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

The glossary in addition to BSI-PP0017[21a] is described in Table 10-2.

Table 10-2

Term	Definition
Chip Configuration	The lifecycle of ST19WR66. It takes 'ISSUER' , 'TEST' or 'USER'. However, it is fixed as 'USER configuration' after the delivery of TOE from IC chip manufacturer. Therefore , it is always regarded as 'USER configuration' in software programmer by chip manufacturer.
(External) command	Communication data sent from external terminal to TOE on Logical interface (APDU).
External terminal	Device or computer PC connected with smartcard reader writer. It can communicate with smartcard via reader writer

10.2. Acronym

The glossary based on BSI-PP0017[21a] is described in Table 10-3.

Table 10-3

Acronym	Term
SFR	Security functional requirement
TOE	Target of Evaluation
SAR	Security assurance requirements
TSF	TOE security functions
CC	Common Criteria
OSP	Organisational security policy
~~*PIS*~~	~~Primary Inspection System~~
~~*BIS*~~	~~Basic Inspection System~~
PT	Personalization Terminal
n.a.	Not applicable

The glossary in addition to BSI-PP0017[21a] is described inTable 10-4.

Table 10-4

Acronym	Term
AID	Application ID. Before executing an application on smartcard it must be selected with AID by using SELECT command.
APDU	Application Protocol Data Unit defined in ISO7816 [31]
CCS	Optional function for secure messaging, which gives the authentication code in the secure messaging APDU for the purpose of ensuring the integrity of APDU
CD	Card domain created by card manufacture in ‘init’ mode of card-status.
CLA/INS	Class and instruction defined in ISO7816. It is the header of APDU, which indicates some attributes of external command.
DF	Dedicated File (ISO7816 [31])
DFA	Differential fault analysis It is one of the side channel attacks against IC chip which deliberately cause the fault state while IC chip is computing. DFA includes an illegal voltage attacks or electrical noise,

	and so on.
DPA	Differential power analysis. Attack method to get some power consuming waves and analyze the difference of them in order to know the cryptographic key.
EEPROM	Non volatile memory on IC chip. it is used for storing data or keys of the smartcard platform.
EFID	Unique ID assigned in IEF or WEF.
EMA	Electromagnetic analysis
ENC	Optional function for secure messaging which enciphers APDU for the purpose of the confidentiality of APDU.
GUN	The generator of unpredictable number.
IEF	Internal Elementary File. Normally it is used for storing keys.
RAM	Volatile memory equipped in the IC chip of smartcard.
RDF	Root dedicated file used for file-based application.
ROM	Read only memory equipped in the IC chip of smartcard. Normally it is used for storing the programs of libraries, basic OS, smartcard platform software and embedded applications.
STM	STMicroelectronics Corporation
SPA	Simple power analysis. It is one of side channel attacks method to analyze the power consuming waves in order to know the cryptographic key.
WEF	Working Elementary File. Normally it is used for storing user data.

11. References

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.3, August 2005

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.3, August 2005

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.3, August 2005

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

[5] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

[5a]/[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20; Bundesamt für Sicherheit in der Informationstechnik, Version 1.0, 2.12.199

ICAO

[6] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[7] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[8] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[9] BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, Version 1.9, ICAO TAG MRTD/NTWG, 19 May 2003

[10] INTERNATIONAL CIVIL AVIATION ORGANIZATION FACILITATION (FAL)

DIVISION, twelfth session (Cairo, Egypt, 22 March – 1 April 2004)

[11] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version – 0.42 - Draft, August, 2004, Dr. Kügler, BSI

Cryptography

[12] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, Bonn, 10.8.2004 (Zieldatum der Veröffentlichung ist Januar 2005)

[13] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[14] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[15] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[16] Federal Information Processing Standards Publication 186-2 DIGITAL SIGNATURE STANDARD (DSS) (+ Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

[17] Certicom Research: SEC 1: Elliptic Curve Cryptography, September 20, 2000, Version 1.0

[18] AMERICAN NATIONAL STANDARD X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)©, September 20, 1998

[19] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

Protection Profiles

[20] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[21] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

[21a]/[PP0017]Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control, Version 1.0, 18.08.2005, BSI-PP-0017, Bundesamt für Sicherheit in der Informationstechnik

Other

[22] Technical Report Advanced Security Mechanisms for Machine Readable Travel Documents, Version 0.8 (final), BSI,

[23] ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, FDIS 2004
Page 74 of 74 Bundesamt für Sicherheit in der Informationstechnik

The glossary in addition to BSI-PP0017 [21a] is described below.

[30] Security Target for ST19WR66, SMD_ST19WR66_05_001_V01.02, STMicroelectronics

[31] ISO/IEC 7816 - Identification Cards - Integrated Circuit Cards with Contacts

[32] ISO/IEC 14443 - Contactless Integrated Circuit Cards, Proximity Cards

[33] E-passport: Adaptation and interpretation of E-passport Protection Profiles, Revision 0.1. Public document, published on DCSSI Internet website (www.ssi.gouv.fr)

[34] E-passport : Intrinsic resistance of the BAC mechanism – Entropy of the MRZ data, Revision 0.1. Public document, published on DCSSI Internet website (www.ssi.gouv.fr)

Deliverables of Xaica-ALPHA64K

[35] AGD_OMP: Operator Manual for Personalization Agent, Version 1.30, NTTDATA Corporation