Security Target
Bundesdruckerei Document Application

Bundesdruckerei GmbH

Author: Bundesdruckerei GmbH

Version: 3.12

Date: 31.01.2014

Abstract

This document is the Security Target (ST) for the Common Criteria certification of the Document Application.

Keywords

CC, ST, Common Criteria, Security Target, Inspection System, nPA, eAT

This page intentionally left blank

Table of Contents

List of Tables

Page

List of Figures

Page

1 ST Introduction

This chapter presents Security Target (ST) and TOE identification information and a general overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3, Security Problem Definition)

b) A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (chapter 7, TOE Summary Specification).

1.1 ST and TOE Reference

This chapter provides information needed to identify and control this ST and its Target of Evaluation (TOE).

ST Title:	**Security Target – Bundesdruckerei Document Application**
ST Version:	3.12
Date:	31.01.2014
Author:	Bundesdruckerei GmbH
Certification-ID:	BSI-DSZ-CC-0932
TOE Identification:	Bundesdruckerei Document Application
TOE Version:	1.2.1129
TOE Platform:	VISOTEC® Änderungsterminal Firmware
Guidance Documents:	AGD - VISOTEC® Änderungsterminal; Handbuch - Installation und Bedienung (corresponding version to TOE as listed in certificate)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 as of September 2012.
Evaluation Assurance Level:	EAL 3
PP Conformance:	BSI-CC-PP-0064 (see [PP-IS])
Keywords:	CC, ST, Common Criteria, Security Target, Inspection System, nPA, eAT

1.2 TOE Overview

The Target of Evaluation (TOE) addressed by this Security Target (ST) is the Bundesdruckerei Document Application. In the following this application is called “Document Application”.

The Document Application is a library, which is used via a static link by an application running on an Inspection System (IS). The library is used to read and update the electronic data of the German identification card (“neuer Personalausweis (nPA)”) and electronic resident permit (“elektronischer Aufenthaltstitel (eAT)”) as well as to verify the document’s authenticity and the integrity of its data.

The TOE is applied in registration offices to allow card holders to verify that their nPA or eAT is working correctly. It is further possible to update the address information of the card holder, the card holder’s PIN for eID applications, and the community ID (“Gemeindeschlüssel”). In addition, the eID application functionality of the nPA or eAT can be activated or deactivated.

More details on the TOE Overview can be found in [PP-IS] section 1.2. The Document Application will be used as the main part of an IS as described in this section.

Necessary protocols for the communication of the TOE with the electronic Machine Readable Travel Documents (eMRTD) like the nPA or eAT are described in [ICAO_9303] and [TR-03110].

In comparison to the Security Target Bundesdruckerei Document Reading Application [ST_DRA] the TOE described in this Security Target can be used to modify data on the nPA and eAT.

1.3 TOE Description

This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration. The main purpose of this chapter is to bind the TOE in physical and logical terms.

The chapter starts with a description of the product type, the supported protocols and modes of operation. Afterwards it introduces the physical and logical scope of the TOE.

1.3.1 Product Type

The product type of the Target of Evaluation (TOE) described in this ST is an Inspection System (IS) used to read and modify data records on the electronic Machine Readable Travel Documents and to verify the integrity and authenticity of that data.

1.3.2 Supported protocols

The TOE implements the following protocols to communicate with eMRTDs:

Protocol Name	Specified in	Use Case
BAC	[ICAO_9303]	Confidentiality of submitted chip data, authentication and secure channels
Chip Authentication	[EAC2.10]	Authenticity of eMRTD chip, secure channels, confidentiality of submitted chip data
PACE	[EAC2.10]	Confidentiality of the submitted chip data, authentication and secure channels
Passive Authentication	[ICAO_9303]	Authenticity and integrity of the chip data

Table 1: implemented protocols

1.3.3 Modes of Operation

The TOE can be operated in different modes of operation depending on the user role that is logged in. The following table shows the actions that the TOE is able to perform in each mode.

Mode	User role	Actions
Idle	-	-
Admin	TOE Administrator	Management of configuration data Initiate firmware update View version number of the TOE
Operational	Operator	Read out/write data from/to eMRTD Verify date and time View version number of the TOE
Revision	Revisor	Audit data revision

Table 2: TOE modes of operation

1.3.4 Physical Scope and Boundary of the TOE

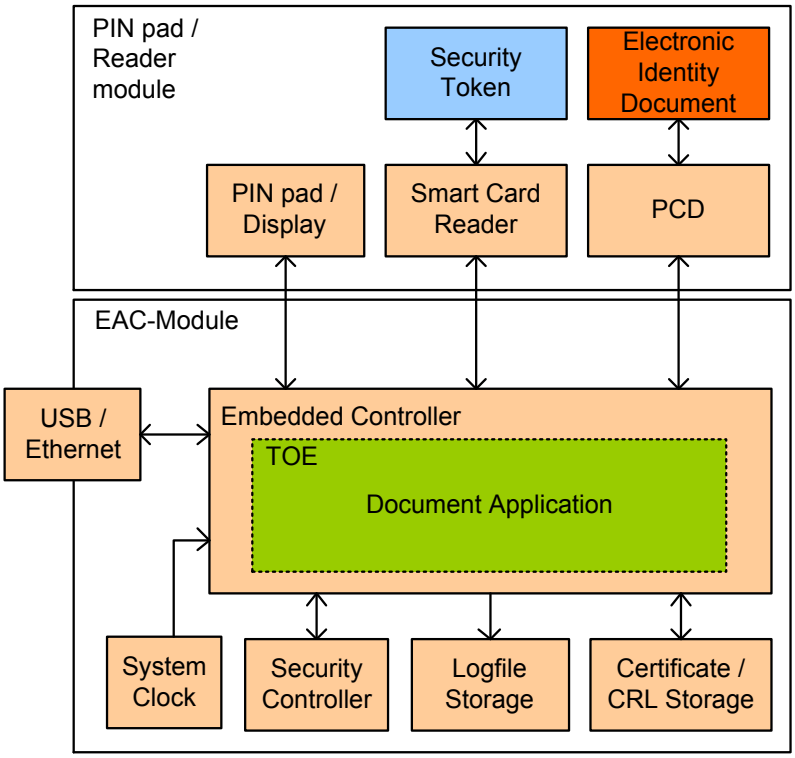

Figure 1: TOE demarcation

The physical scope and boundary of the TOE is depicted in Figure 1. The TOE is the document application of the product Inspection System and is therefore software only. It is accompanied by its dedicated guidance documentation.

The platform for the TOE is the VISOTEC® Änderungsterminal Firmware, which is based on a Linux Kernel of the 2.6 series and the GNU libc library. The underlying hardware is a 32 bit embedded controller.

The TOE relies on a security controller that performs the cryptographic operations for Terminal Authentication and that stores the necessary private key. All other cryptographic operations (e.g. for the other protocols) are performed in software by the TOE itself. Private keys that are used for other authentication mechanisms are stored temporarily in the volatile memory of the TOE.

The following list shows the other components in the environment of the TOE that the TOE relies on:

- A PIN pad and a display for user interaction
- Proximity coupling device (PCD) for communication with the eMRTDs
- Smartcard reader for authentication of users with security tokens
- Security Controller for cryptographic operations
- Ethernet network interface for certificate and CRL download

- USB interface to read/write data groups
- System Clock
- Storages for audit data and certificates/CRLs

The hardware components of the inspection system are physically separated into the EAC-Module and the PIN pad / Reader module.

1.3.5 Logical Scope and Boundary of the TOE

The logical scope of the TOE is best described by its main security functionality:

- Secure encrypted and authenticated communication with eMRTDs,
- Protection of sensitive personal data from eMRTDs and TSF data,
- Deterministic random number generation,
- Management including initiating secure firmware update, and
- Generation of audit data.

The TOE uses the following security functionality of the environment:

- Authentication of users,
- Installation of firmware update,
- Secure storage and usage of private keys,
- Entropy source for random number generation,
- Storage of audit data, and
- Physical protection.

1.4 Conventions

For this Security Target the following conventions are used:

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in chapter C.4 of Part 1 of the CC. Each of these operations is used in this ST.

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. If there is no refinement done, the placeholder is striked through.

Extensions on how the requirements in the underlying PP are interpreted in the actual context and implemented by the product are marked **bold,** too.

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 underlined text. Selections that have been made by the ST author appear in square brackets, and are *italicized* and underlined.

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. Assignments that have been made by the ST author appear in square brackets 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.

The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed ‘explicit requirements’ and are permitted if the CC does not offer suitable requirements to meet the authors’ needs. **Explicit requirements** must be identified and are required to use the CC class/family/component model in articulating the requirements.

An overview of keys and certificates used can be found in [PP-IS] chapter 6.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be

- **CC Part 2 (Version 3.1, Revision 4, September 2012) extended** as functional components as defined in part II of [CC] and also the extended functional components FCS_RND.1 and FIA_API.1 as defined in [PP-IS] have been used.
- **CC Part 3 (Version 3.1, Revision 4, September 2012) conformant** as only assurance components as defined in part III of [CC] have been used.

Further this Security Target claims to be conformant to the Security Assurance Requirements package EAL 3.

2.2 PP Conformance Claim

This Security Target claims conformance to the *Common Criteria Protection Profile for Inspection Systems (IS)* [PP-IS].

The Protection Profile requires a *demonstrable conformance* only. However, this Security Target claims strict conformance to the Protection Profile as it completely includes the statement of security problem definition of the PP.

3 Security Problem Definition

This chapter describes

- the assets that have to be protected by the TOE,
- assumptions about the environment of the TOE,
- threats against those assets, and
- organisational security policies that TOE shall comply with.

3.1 External entities

The following external entities interact with the TOE:

Operator (E1)

The Operator is the user of the TOE (e.g. employee of a governmental organization).

Administrator (E2)

The Administrator is a person who administrates the TOE and who is able to access the TOE on a dedicated service interface to change security attributes of the TOE Security Functionality (TSF).

Revisor (E3)

The Revisor is a person who is able to access the TOE on a dedicated service interface to inspect the log files of the TOE.

Attacker (E4)

A person who tries to manipulate the TOE in order to change its behaviour without being authorized or tries to provide the TOE with false information (this may be a forged certificate or a false software update, etc.) is an Attacker.

electronic Identity Document (E5)

An MRTD, ePass, nPA or eAT supporting cryptographic mechanisms which allows the Inspection System to check their Integrity and Authenticity. The Electronic Identity Document is presented to the Inspection System which then communicates with the TOE secured by cryptographic means.

electronic Identity Document presenter (E6)

Person presenting the electronic Identity Document to the inspection system and claiming the identity of the electronic Identity Document holder.

Private Key Storage (E7)

Storage of the Inspection System's Key Pairs. The Key Pairs are used for the Terminal Authentication Protocol. The Private Key Store is protected by further security measures in the environment of the TOE (security controller) to enforce the protection needs of the Inspection System's Key Pairs.

Certificate / CRL storage (E8)

The Certificate and CRL storage hold the certificates and CRLs representing the PKI for the Passive Authentication and Terminal Authentication. Furthermore the storage maintains specific certificates and/or specific public keys the Inspection System implicitly trusts in. These specific certificates and/or specific public keys are the root keys of the PKI. The Certificate and CRL storage is protected by further security measures to enforce the protection needs of the Certificates and CRLs.

Logfile storage (E9)

The Logfile storage holds the logfile entries generated by the TOE. The Logfile storage is protected by further security measures to enforce the protection needs of the Logfile entries.

Proximity Coupling Device (PCD) (E10)

The PCD realizes the interface between the electronic Identity Document and the TOE. The PCD consists of a contact-less interface and some further electronic components implementing appropriate transmission protocols allowing communication between the PCD and electronic Identity Documents. Furthermore the PCD provides an interface to the TOE finally allowing the communication between the TOE and electronic Identity Document.

PIN pad (E11)

The PIN pad provides necessary input data to the TOE. For example, it is used for entering the shared secret for PACE authentication.

Display (E12)

The display presents results of the Inspection Process as well as further information obtained during the process to the user of the TOE (E1 and/or E2). It is further used for general user interaction/feedback during management of the TOE.

Electronic Identity Document holder (E13)

The rightful/legitimated holder of the electronic Identity Document for whom the issuing authority personalised the electronic Identity Document.

3.2 Assets

The assets to be protected by the TOE and its environment are as follows:

Chip password (O1)

The chip password is used to get basic access to the chip data. In case of an eMRTD according to [ICAO_9303] this would be a part of the MRZ (Machine Readable Zone), for other electronic identity documents this could be e.g. another password printed on the document (as CAN in [EAC2.10]). Dependent upon the form of the chip password it can be read by an OCR Reader or must be typed in on a keyboard, etc.

Required Protection: Integrity, Confidentiality

Personal Chip Data (O2)

The Personal Chip Data (O2) is the data of a chip of an electronic identity document which is not secured by EAC according to [EAC2.10].

Required Protection: Integrity, Confidentiality

Sensitive Chip Data (O3)

The Sensitive Chip Data (O3) is the data of a chip (DG3, DG4) of an electronic identity document which can be read-out only by processing EAC according to [EAC2.10] successfully.

Required Protection: Integrity, Confidentiality

Private Key (O4)

The Private Key (O4) is the private key of the IS used for Terminal Authentication and is securely stored in the environment of the TOE (security controller).

Required Protection: Integrity, Confidentiality

Session and Ephemeral Keys (O5)

The session and ephemeral keys (O5) are those non-static keys needed by the TOE to perform the protocols described in 1.3.2.

Required Protection: Integrity, Confidentiality

Random numbers (O6)

The random numbers (O6) are those random numbers needed by the TOE to perform the protocols described in 1.3.2.

Required Protection: Integrity, Confidentiality

Certificates (O7)

The certificates are needed for Passive Authentication and Terminal Authentication.

Required Protection: Integrity

CRLs (O8)

CRLs are needed for Passive Authentication.

Required Protection: Integrity including protection against unauthorised deletion

Configuration Data (O9)

TSF Data to configure the TOE. These data include security attributes of the TSF (e.g. address of Update Server for Revocation Lists, Software Update Public Key).

Required Protection: Integrity

Log Data (O10)

A document reading application can write Log Data to a permanent log file. These data can be used for revision purposes.

Required Protection: Integrity, Authenticity

Sensitive input data (O11)

All further input data besides the chip password (O1) received from the PIN pad is considered as sensitive input data.

Required Protection: Integrity, Confidentiality

Protocol results (O12)

Protocol results are the information about the processed protocols. This includes which protocols have been executed and if applicable what are the results of the process, e.g. the Integrity of the chip data has been proved by successful Passive Authentication.

Required Protection: Integrity

3.3 Assumptions

In the following the assumptions about the environment of the TOE are described:

A.SecureBoot

It is assumed that the environment provides mechanisms to boot the operating system containing the Document Application and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed. Furthermore it is assumed the secure boot process provides an integrity check of the TSF.

A.PhysicalTamper

It is assumed that the Inspection System is protected against physical tamper by placing additional devices on the Inspection System as e.g. key loggers or removing the whole terminal or parts of it concerning low level attacks.

A.SecureAdministration

It is assumed that the administration of the Inspection System as well as of the TOE installed at the Inspection System is maintained securely. This includes that only authorised personnel is allowed to administer the Inspection System respectively the TOE and that no Malware will be installed at the Inspection System.

A.TrainedUser

It is assumed that the authorised Users of the TOE, Operator (E1) and Administrator (E2), are well trained. This includes that no user will intentionally compromise the TOE installation as well as the assets secured by the TOE and the TOE environment.

A.SecureEnvironment

It is assumed that the TOE environment at the Inspection System is secure. This assumption includes that no other application - or also parts of the Operating System - installed at the inspection system compromise sensitive data, manipulate sensitive data or the results of the MRTD authentication, or even try to penetrate the TOE itself with the intention to affect the TOE's security functionality maliciously. Furthermore this includes also that components of the Inspection System the TOE relies on work properly as intended (e.g. the Output of the Inspection System prints the MRTD data as handed over by the TOE, the identification and authentication mechanism of Inspection System – provided by the operating environment – is effective, the security measures of the Certificate/ CRL, Private Key and Logfile storage are in place, etc.).

The firmware update is initiated by the TOE and securely performed by the environment. Therefore, the operating system and the firmware update component residing in the TOE environment are assumed to be trustworthy.

A.DisplayShield

It is assumed that the Inspection System is installed in such a way that the sensitive data printed at the output device are visible only to authorised persons.

A.ValidKeyAndCertificateData

It is assumed that all further data stored in TOE related components are securely maintained. This includes that they are generated and imported according to their protection requirements as defined in section 3.2.

A.PKI

It is assumed that the environment provides a Public Key infrastructure for EAC and Passive Authentication.

3.4 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.

T.ForgeMRTD – Acceptance of forged MRTD

Adverse action: An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive an inspection system by means of the changed MRTD holder's 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 another 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 MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveller into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder of this MRTD.

Threat agent: An attacker (E4) having basic attack potential, being in possession of one or more legitimate MRTDs

Asset: Protocol Results (O12)

T.DataCompromise – Compromise of sensitive MRTD Data

Adverse action: An attacker (E4) could pretend to be an operator (E1) using the IS and the TOE to read sensitive data (O2 and O3) from electronic identity documents.

Threat agent: An attacker (E4) having basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance nor having access to the MRTDs accessed.

Asset: Personal Chip Data (O2), Sensitive Chip Data (O3)

T.FakedLogfileEntries Spoofing of Logfile Information

Adverse action: An attacker (E4) could try to manipulate the logfiles (O10) to cover information about the TOE installation which might be changed maliciously.

Threat agent:	An attacker (E4) having basic attack potential, having physical access to the Inspection System.
Asset:	Log File entries (O9)

T.Eavesdropping Eavesdropping of sensitive chip data

Adverse action:	An attacker (E4) could eavesdrop sensitive and personal chip data (O2 and O3) transmitted between MRTD Chip and document reading application.
Threat agent:	An attacker (E4) having basic attack potential, having physical access to the Inspection System.
Asset:	Personal Chip Data (O2), Sensitive Chip Data (O3)

3.5 Organisational Security Policies

P.CheckTerminal

The integrity of the entire IS hardware shall be checked regularly by the Operator (E1).

The Case of the IS should be sealed in a manner that the Operator can verify at the beginning of his duty that the terminal is genuine. Therefore a unique label is necessary so that an exchange of the whole IS or manipulation on cable connections can be detected.

The stored log data shall be revised regularly to discover malfunctions or attacks. This shall be done by a revisor (E3) who is not the same person as the administrator (E2).

P.Date

The Operator (E1) must perform a daily check of the system date. Therefore he has to use a reliable reference (e.g. DCF-77 Clock, GPS Clock, etc.). Especially in the context of certificate validation it must be assured that the system date is correct.

P.ChipPassword

The Operator (E1) must ensure during a reading or updating operation that any person who is not authorised to know the chip password (O1) is not able to skim it. Therefore a special distance between the IS and waiting customers shall be enforced[3].

P.CertifiedPrivateKeyStore

It has to be assured that the Private Key Storage is a device certified according to minimum EAL4.

P.PrivateKeyStore

The Private Key Storage has to authenticate with the electronic Identity Document (E5) via the Terminal Authentication Protocol.

[3] The specific distance between the IS and waiting customers is defined in the guidance document.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. This chapter describes the security objectives for the TOE and its operational environment.

Aspects of the security objectives that are not stated in [PP-IS] but used in ST are marked bold.

4.1 Security Objectives for the TOE

O.AdminAuthorisation

The TOE must provide an administration interface. The TOE shall use the result of an Identification and Authentication mechanism to enforce that only authorised administrators are allowed to make use of the administration interface to change the TOE's configuration (including update of the TOE's current version). The TOE may use those Identification and Authentication mechanisms provided by the operating system.

O.OperatorAuthorisation

If personal chip data (O2) and/or sensitive chip data (O3) shall be read the TOE must enforce the authentication of the operator (E1) as an authorised person. The TOE shall use the result of an Identification and Authentication mechanism to enforce the operator's authorisation. The TOE may use those Identification and Authentication mechanisms provided by the operating system.

O.UpdatingSoftware

The TOE shall only accept signed updates with a version number that is higher than or equal to the current version.

O.DisplayVersion

The TSF must be able to maintain version information about the TOE itself and must be able to present this evidence to external entities allowing those entities to verify the version of the TSF itself.

O.Logdata

The TOE shall write log data at least about every change in configuration or software updates.

O.DeletionEphemeralData

The TOE shall delete ephemeral data after every completed or aborted reading/updating process in a secure way (data shall be overwritten). This includes all data read from the chip

(O1, O2, O3), every generated random number (O6), ephemeral key and session key (O5) and sensitive input data (O11).

O.ProtocolMRTD

The TOE shall implement the protocol according to the specifications **[EAC2.10]** in realisation of an inspection system. This includes the Security Mechanisms Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE), Chip Authentication and Passive Authentication.

The TOE shall enforce the establishment of secure messaging between the electronic identity document's chip and Document Application in dependency on the protocols (see [PP-IS, 1.2.4]) supported by the chip.

4.2 Security Objectives for the operational Environment

OE.SecureBoot
The environment must provide mechanisms to boot the Inspection System OS and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed.

OE.SignedCertsAndCRLs

The environment shall make sure that only certificates, certificate-lists and CRLs (O7, O8) from the certificate storage are provided to the TOE which are signed by the CSCA or a key signed by the CSCA of the operating state.

OE.PKI

The environment must provide Public Key Infrastructures for EAC and Passive Authentication according to the specifications in [ICAO_9303], **[EAC2.10]** depending on the used protocols.

Each PKI environment must provide a Certificate Policy.

OE.TA

The environment of the TOE shall implement the cryptographic mechanism Terminal Authentication as part of EAC. This includes maintaining of the Terminal's Private Key and the implementation of the security protocol Terminal Authentication.

OE.SecureAdministration

The administration of the Inspection System as well as the TOE itself shall be maintained securely. Only authorised personnel shall be allowed to administer the Inspection System and the TOE. The administration personnel will not install any malicious soft- or hardware at the inspection system.

OE.TrainedUser

The Users – Operators and Administrators – of the Inspection System shall be well trained in a sense not to intentionally compromise neither the TOE installation itself nor the assets secured by the TOE and the TOE environment.

OE.SecureEnvironment

The TOE environment shall be secure. **For example, the firmware update is initiated by the TOE and securely performed by the environment. Therefore, the operating system and the firmware update component residing in the TOE environment shall be trustworthy.** Other applications installed at the Inspection System as well as the Operating System itself shall not compromise and/or manipulate sensitive data and shall not penetrate

the TOE. The Secure Environment shall ensure that the results of the MRTD authentication are displayed to the Operator unaltered. Further components of the Inspection System the TOE relies on, the Certificate and CRL Store respectively, the private Key Storage and the identification/authentication mechanism of the operational environment shall work properly as intended:

– The identification/authentication mechanism of the operating system shall be effective and shall provide information to the TOE which allows the TOE to assign roles to identities.

– The Security Measures of the Certificate and CRL Storage respectively and the Private Key Storage shall be in place.

– The operational environment shall provide a secure storage for logfiles which enforces access control and provides secure messaging.[4]

The Private Key Store shall be certified according to the Common Criteria at least with the assurance level EAL4.

OE.ComponentCommunication

The communication between the TOE and the logfile storage, the private key storage and the certificate / CRL storage shall be secured for the assets transferred according to the the required protection as defined in chapter 3.2.

E.g. the communication between TOE and the Private Key Store shall be secured against attacks on the confidentiality, authenticity and integrity of the exchanged messages. The communication between the TOE and the log file storage shall be secured against attacks on authenticity and integrity.

OE.DisplayShield

The Display of the Inspection System shall be installed in a manner that the output of sensitive data can't be observed by unauthorised persons.

OE.CheckTerminalIntegrity

The integrity of the entire IS hardware shall be checked regularly by Operator (E1) .The housing of the IS should be sealed in a manner that the operator can verify at the beginning of his duty that the terminal is authentic. Therefore a unique label is necessary so that an exchange of the whole IS or manipulation on cable connections can be detected. The stored log data shall be revised regularly to discover malfunctions or attacks. This shall be done by a revisor (E3) who is not the same person as the administrator (E2).

OE.Date

[4] The log file storage will be implemented within the chassis of the Inspection System, which provides physical security measures. Logical access to the log file storage will be limited to the Revisor role only.

The operator (E1) shall check the correctness of the current date and time of the TOE at the beginning of his duty. For this the Operator has to use a reliable reference (e.g. DCF-77 Clock, GPS Clock).

OE.ChipPassword

The environment must enable the Operator (E1) to ensure during a reading or updating operation that any person who is not authorised to know the chip password (O1) is not able to skim it. Therefore a special distance between the IS and waiting customers shall be enforced.

OE.ValidKeyAndCertificateData

The TOE environment shall provide adequate measures to ensure the security of the further key and certificate data – including the CRLs – during the generation and the import of such data. In more detail the authenticity and integrity of the Private Key and the Certificates as well as Certificate Revocation Lists shall be ensured. Furthermore for the Private Key the confidentiality has to be ensured.

4.3 Security Objectives Rationale

The following table provides an overview of the security objectives' coverage (bold **X**s are not from [PP-IS]):

	O.AdminAuthorisation	O.OperatorAuthorisation	**O.UpdatingSoftware**	O.DisplayVersion	O.Logdata	O.DeletionEphemeralData	O.ProtocolMRTD	OE.SignedCertsAndCRLs	OE.ComponentCommunication	OE.SecureBoot	OE.PKI	OE.TA	OE.SecureAdministration	OE.TrainedUser	OE.SecureEnvironment	OE.DisplayShield	OE.CheckTerminalIntegrity	OE.Date	OE.ChipPassword	OE.ValidKeyandCertificateData
T.ForgeMRTD	X		**X**				X	X				X								
T.DataCompromise	X	X	**X**	X		X			X					X		X				
T.FakedLogFileEntries					X				X				X		X					
T.Eavesdropping							X													
A.SecureBoot										X										
A.PhysicalTamper																	X			
A.SecureAdministration													X							
A.TrainedUser														X						
A.SecureEnvironment									X						X					
A.DisplayShield																X				
A.ValidKeyAndCertificateData																				X
A.PKI											X									
P.CheckTerminal																	X			
P.Date																		X		
P.ChipPassword																			X	
P.CertifiedPrivateKeyStore															X					
P.PrivateKeyStore												X								

Table 3: Security Objective Rationale

4.3.1 Considerations about Threats

T.ForgeMRTD

This threat is covered by the following combination of objectives:

O.AdminAuthorisation makes sure that only authorised administrators can change the configuration of the TOE. Therefore attackers cannot change the configuration in any way which might bypass the functionality used to authenticate an MRTD.

OE.SignedCertsAndCRLs makes sure that only legitimate public keys are accepted for the verification of signatures or certificates provided by an MRTD and/or used by the TOE.

O.ProtocolMRTD makes sure that the TOE uses the specified cryptographic protocols to verify the authenticity of data provided by an MRTD.

O.UpdatingSoftware makes sure that only legitimate software is used for the TOE, which also mitigates the threat of bypassing the functionality used to authenticate an MRTD.

OE.TA makes sure that the environment supports the advanced cryptographic mechanism necessary for Terminal Authentication according to the respective specifications.

T.DataCompromise

This threat is covered by the following combination of objectives:

O.AdminAuthorisation, **O.OperatorAuthorisation** and **OE.TrainedUser** together make sure that only authorised and trained users can operate the TOE. This prevents compromising MRTD data by operators.

OE.ComponentCommunication, OE.DisplayShield and **O.DeletionEphemeralData** make sure that attackers cannot see secret data during transport between components of the Terminal, during Display of Data or by finding old secret data in the storage of the Terminal.

O.DisplayVersion again supports this by making sure that only legitimate software is used.

O.UpdatingSoftware supports that attackers are not able to see secret data.

T.FakedLogFileEntries

This threat is covered as follows:

O.Logdata makes sure that log entries are written, whenever the TOE configuration is changed or updates are installed.

OE.ComponentCommunication prevents manipulation of log file entries during their transport between TOE and storage.

OE.SecureAdministration and OE.SecureEnvironment make sure that the log files are not manipulated during their storage.

T.Eavesdropping

O.ProtocolMRTD makes sure that the specified cryptographic protocols are used for communication between TOE and MRTD. In particular this prevents unauthorised reading of secret data on this interface.

4.3.2 Considerations about Assumptions and OSPs

4.3.2.1 Assumptions

A.SecureBoot

OE.SecureBoot addresses this assumption directly as a requirement for the environment of the TOE.

A.PhysicalTamper

OE.CheckTerminalIntegrity addresses this assumption directly as a requirement for the environment of the TOE.

A.SecureEnvironment

The identically named Security Objective for the Environment **OE.SecureEnvironment** together with the Security Objective for the Environment **OE.ComponentCommunication** address this assumption to ensure the secure environment for the TOE.

A.SecureAdministration, A.TrainedUser, A.DisplayShield, A.PKI and A.ValidKeyAndCertificateData are also directly addressed by security objectives for the environment of the corresponding names.

4.3.2.2 OSP

P.CheckTerminal

OE.CheckTerminalIntegrity addresses this Organisational security policy directly as a requirement for the environment of the TOE.

P.Date

OE.Date addresses this Organisational security policy directly as a requirement for the environment of the TOE.

P.ChipPassword

OE.ChipPassword addresses this Organisational security policy directly as a requirement for the environment of the TOE.

P.CertifiedPrivateKeyStore

OE.SecureEnvironment addresses this in one of its paragraphs.

P.PrivateKeyStore

OE.TA addresses this Organisational security policy as a requirement for implementation of the Terminal Authentication Protocol by the environment of the TOE.

5 Extended Component Definition

See the extended component definition in [PP-IS]. There are no further extended components defined in this ST.

6 Security Requirements

This chapter defines the security requirements that shall be satisfied by the TOE or its environment:

Common Criteria divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subchapters.

6.1 TOE Security Functional Requirements

The TOE satisfies the SFRs described in the following chapter.

6.1.1 Class Security Audit (FAU)

FAU_GEN.1/Audit Audit data generation - Audit

FAU_GEN.1.1/Audit	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [*not specified*] level of audit; and c) every change of TOE configuration, or software updates and [*auditable events defined by Table 4*].
FAU_GEN.1.2/Audit	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*audit relevant information defined in Table 4*].

Refinement: The TOE supports the storage of audit records by the TOE environment (cf. OE.SecureEnvironment) by providing the respective information and by sending that information to the secure audit storage.

Application Note: The TOE makes use of the time stamps provided by the TOE environment (cf. OE.SecureEnvironment and OE.Date).

Auditable event	**Audit relevant information (in addition to those of FAU_GEN.1.2 a))**
Start-up and shutdown of the audit functions	-
Every change of TOE configuration	The modified configuration element
Firmware update	In case of software update: firmware version of new firmware

Table 4: List of auditable events and audit relevant information

FAU_GEN.1/PA Audit data generation – Passive Authentication

FAU_GEN.1.1/PA	The TSF shall be able to generate **information** of the following auditable events: • announcement of having processed the Passive

Authentication Protocol including the result of the process

- announcement of having processed the Chip Authentication Protocol including the result of the process.

FAU_GEN.1.2/PA	The TSF shall **export** within **the Passive and Chip Authentication Result Status Output** at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, Passive and Chip Authentication carried out and [*none*].

Refinement: The TSF shall implement the Passive Authentication and Chip Authentication Protocol (cf. FCS_COP.1/CER). The TSF shall present the result of the Passive Authentication Protocol and the Chip Authentication Protocol to the operator.

Application Note: The TOE makes use of the time stamps provided of the TOE environment (cf. OE.SecureEnvironment and OE.Date).

6.1.2 Class Cryptographic Support (FCS)

FCS_CKM.1/KDF Cryptographic key generation – Document Basic Access Key

FCS_CKM.1.1/KDF The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Document Basic Access Key Derivation Algorithm* and specified cryptographic key sizes *112 bit* that meet the following: [*[ICAO_PKI]*].

Application Note: The assigned list of standards shall ensure that the Inspection System derives the same document basic access key as loaded by the personalization agent into the MRTD and used by the TOE for FIA_UAU.4. The [ICAO_9303], Annex A5.1, referenced by [EAC2.10], describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the document basic access keys for Basic Access Control from the second line of the printed MRZ data.

FCS_CKM.1/PACE Cryptographic key generation – Diffie-Hellmann PACE Keys

FCS_CKM.1.1/PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Password authenticated Diffie-Hellman key agreement* and specified cryptographic key sizes [*128 bit (to be used with AES)*] that meet the following: **[EAC2.10]**, *A.2.3 and A.3.*

Application Note: The [EAC2.10] describes the Key Agreement Protocol for PACE in Annex A.2.3. Annex A.3. of [EAC2.10] lists the standards for symmetric keys agreed by PACE. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAO_9303], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC

FCS_CKM.1/DH Cryptographic key generation – Diffie-Hellmann Chip Authentication Keys

FCS_CKM.1.1/DH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Diffie-Hellman key agreement*] and specified cryptographic key sizes [*128 bit (to be used with AES)*] that meet the following: **[EAC2.10]**, Annex A.1.

Application Note: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol, see [EAC2.10], sec. 3.1 and Annex A.1. The shared secret value is used to derive the AES or Triple-DES key for encryption and the Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [ICAO_9303], normative appendix 5, A5.1, for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with other values or the new key that meets the following: none.

Refinement: The TOE shall destroy the BAC Session Keys and PACE Session Keys (i) after detection of an error in a received command by verification of the MAC, or (ii) after successful run of the Chip Authentication Protocol. The TOE shall destroy the Chip Session Keys as well as the Chip Authentication Ephemeral Key Pair after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys as well as ephemeral keys after ending a session and therefore before starting the communication with the MRTD in a new session.

FCS_COP.1/SHA Cryptographic operation – Hash for Key Derivation and Passive Authentication

FCS_COP.1.1/ SHA	The TSF shall perform hashing in accordance with a specified cryptographic algorithm [*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*] and cryptographic key sizes none that meet the following: [*FIPS 180-4*].

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

FCS_COP.1.1/ SYM	The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm [*3DES CBC and AES CBC*] and cryptographic key sizes [*3DES: 112 bit, AES: 128 Bit*] that meet the following: 'TR-03110', [EAC2.10].

Application Note: This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the MRTD during the execution of the Basic Access Control Authentication Mechanism, the Password Authenticated Connection Establishment or as part of the Chip Authentication Protocol according to the FCS_CKM.1.

FCS_COP.1/MAC Cryptographic operation – MAC

FCS_COP.1.1/ MAC	The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm [*3DES CBC MAC and AES CMAC*] and cryptographic key sizes [*3DES 112 Bit, AES: 128 Bit*] that meet the following: 'TR-03110', [EAC2.10].

Application Note: 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 during the execution of the Basic Access Control Authentication Mechanism, the Password Authenticated Connection Establishment or the Chip Authentication Protocol according to the FCS_CKM.1.

FCS_COP.1/CER Cryptographic operation – Signature check

FCS_COP.1.1/CER	The TSF shall perform signature check using CRLs and the whole certificate chain in accordance with a specified cryptographic algorithm [*ECDSA/SHA-1, ECDSA/SHA-224, ECDSA/SHA-256, ECDSA/SHA-384, ECDSA/SHA-512*] and cryptographic key sizes [*ECDSA: 256 bit*] that meet the following: [*[ICAO_9303]*].

Application Note: The TSF shall perform signature check using CRLs and the whole certificate chain in the context of performing the security protocol Passive Authentication as described in [EAC2.10] and [ICAO_9303], respectively.

FCS_COP.1/SW Cryptographic operation – Software Update

FCS_COP.1.1/SW	The TSF shall perform signature check[5] in accordance with a specified cryptographic algorithm [*RSA/SHA-256*] and cryptographic key sizes [*RSA: 2048 bit*] that meet the following: [*[PKCS#1] and [FIPS180-4]*]

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet the functionality class K4 as defined in [AIS20] with at least 64 bit entropy for the seed.

Application Note: This SFR requires the TOE to generate random numbers used for the authentication protocols as requested by the requirements of FCS_CKM.1 and FIA_UAU.5 respectively.

[5] Please note that other checks like the check for certification revocation list (CRL) are not performed by the TOE. The requirement only addresses signature verification with a public key according to the used cryptographic algorithm.

6.1.3 Class User Data Protection (FDP)

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [*Firmware Update SFP*] on [

- *Subjects (TOE, firmware update component (environment))*
- *Information (firmware update)*
- *Operation (initiate firmware update)*

].

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [*Firmware Update SFP*] based on the following types of subject and information security attributes: [

- *Firmware update (signature and version number of firmware update)*
- *TOE (authentication state of the TOE administrator)*

].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

The TOE shall initiate the TOE firmware update by calling the firmware update component in the environment only if

- *the TOE administrator is authenticated,*
- *the version number of the firmware to be installed is higher than or equal to the version number of the installed firmware, and*
- *the signature of the firmware update is valid according to the trust anchor[6].*

].

FDP_IFF.1.3 **Refinement:** The TSF shall enforce ~~**the**~~ [*no additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

[6] The trust anchor is a root CA stored in the hardware (security controller) of the TOE.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: Chip Password, Personal Chip Data, Sensitive Chip Data, sensitive Input Data.

Refinement: The TSF shall delete the information after every completed or aborted reading/updating process at least by an overwriting mechanism.

Application Note: The objects requested to be deleted by this requirement have to be deleted by the TSF only if they have been produced during the Inspection Process.

6.1.4 Class Identification and Authentication (FIA)

FIA_API.1/BAC Authentication Proof of Identity

FIA_API.1.1/BAC	The TSF shall provide a Basic Access Control Authentication Mechanism according to **[EAC2.10]** to prove the identity of the electronic Identity Document presenter.

Application Note: This SFR requires the TOE to implement the Basic Access Control Authentication Mechanism specified in [EAC2.10].

FIA_API.1/PACE Password Authenticated Connection Establishment

FIA_API.1.1/PACE	The TSF shall provide a Password Authenticated Connection Establishment according to **[EAC2.10]** to prove the identity of the electronic Identity Document presenter.

Application Note: This SFR requires the TOE to implement the Password Authenticated Connection Establishment specified in [EAC2.10].

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to 1 Basic Access Control Authentication Mechanism 2 Password Authenticated Connection Establishment.

Application Note: The Basic Access Control Authentication Mechanism [ICAO_9303] and the Password Authenticated Connection Establishment [EAC2.10] use a challenge RND.IFD freshly and randomly generated by the terminal to prevent reuse of a response generated by an MRTD's chip and of the session keys from a successful run of the authentication protocol.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide 1 Basic Access Control Authentication Mechanism 2 Password Authenticated Connection Establishment

3 Passive Authentication

4 Chip Authentication Protocol

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 MRTD by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys or by means of the Password Authenticated Connection Establishment Authentication Mechanism.

2 After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the TOE accepts only response codes with correct message authentication code sent by means of secure messaging with keys agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism or by means of the Password Authenticated Connection Establishment Authentication Mechanism.

3 The TOE accepts the authenticity and integrity of the MRTD Data by means of the Passive Authentication Mechanism after successful authentication by Basic Access Control or Password Authenticated Connection Establishment Authentication Mechanism.

4 After run of the Chip Authentication Mechanism the TOE accepts only response codes with correct message authentication codes sent by means of secure messaging with keys agreed with the terminal by means of the Chip Authentication Mechanism

Application Note: Basic Access Control Mechanism or the Password Authenticated Connection Establishment Authentication Mechanism includes the secure messaging for all commands and response codes exchanged after successful mutual authentication between the inspection system and the MRTD. The inspection system shall use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys or the Password Authenticated Connection Establishment Authentication Mechanism drawn from the second, optical readable MRZ line and the secure messaging after the mutual authentication. The Inspection System and the MRTD shall use the secure messaging with the keys generated by the Chip Authentication Mechanism after the mutual authentication.

FIA_UAU.6/BT Re-authentication – BAC/PACE

FIA_UAU.6.1/BT The TOE shall re-authenticate the user under the conditions

1 Each response sent to the TOE after successful

authentication of the MRTD with Basic Access Control or Password Authenticated Connection Establishment Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication or by the Password Authenticated Connection Establishment Mechanism

2 Each response sent to the TOE after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol.[1]

Application Note: The Basic Access Control Mechanism, the Password Authenticated Connection Establishment mechanism and the Chip Authentication Protocol specified in [EAC2.10] include secure messaging for all commands and responses exchanged after successful authentication of the TOE. The TOE checks by secure messaging in MAC_ENC mode each response based on Retail-MAC whether it was sent by the successfully authenticated MRTD (see FCS_COP.1/MAC for further details). The TOE does not accept any response with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those responses received from the authenticated user.

FIA_UID.2 User identification before any action

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: The TOE verifies the result of the identification/authentication system of the environment by only respecting the roles supported by the TOE (see OE.SecureEnvironment). The SFR FIA_UID.1 of [PP-IS] was replaced by FIA_UID.2 according to application note 27 in [PP-IS].

6.1.5 Class Security Management (FMT)

FMT_MTD.1/Admin – Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to modify the

- configuration data of the TOE and
- the further TSF data: [*none*]

to the Administrator.

FMT_MTD.1/Version – Management of TSF data

FMT_MTD.1.1/Version	The TSF shall restrict the ability to read the TOE version and further TSF data: [*date and time*] to the Operator and the Administrator.

FMT_SMF.1 - Specification of management functions

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: - modification of configuration data of the TOE - read the TOE version - [*Verify date and time* - *Initiate firmware update*]

FMT_SMR.1 – Security roles

FMT_SMR.1.1	The TSF shall maintain the roles: - Administrator - Operator - and the further authorised roles [*Revisor*]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application Note: The identification/authentication mechanism is implemented by the TOE environment (see OE.SecureEnvironment). The TOE reuses the result of the identification/authentication mechanism by the determination of the user's role.

6.2 Security Assurance Requirements for the TOE

The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 3 (EAL3).

6.3 Security Functional Requirements Rationale

The following table provides an overview for the security functional requirements' coverage. Bold text indicates requirements which are not present in the [PP-IS].

	O.AdminAuthorisation	O.OperatorAuthorisation	**O.UpdatingSoftware**	O.DisplayVersion	O.Logdata	O.DeletionEphemeralData	O.ProtocolMRTD
FAU_GEN.1/Audit					X		
FAU_GEN.1/PA							X
FCS_CKM.1/KDF							X
FCS_CKM.1/PACE							X
FCS_CKM.1/DH							X
FCS_CKM.4						X	X
FCS_COP.1/SHA							X
FCS_COP.1/SYM							X
FCS_COP.1/MAC							X
FCS_COP.1/CER							X
FCS_COP.1/SW			**X**				
FCS_RND.1							X
FDP_IFC.1			**X**				
FDP_IFF.1			**X**				
FDP_RIP.1						X	
FIA_API.1/BAC							X
FIA_API.1/PACE							X
FIA_UAU.4							X
FIA_UAU.5							X
FIA_UAU.6							X
FIA_UID.2	X	X					
FMT_MTD.1/Admin	X		**X**				
FMT_MTD.1/Version	X	X					
FMT_SMF.1	X	X	**X**	X			
FMT_SMR.1	X	X	**X**				

Table 5: Security functional requirements rationale

The Security Objectives for the TOE are covered by the SFRs as follows:

O.AdminAuthorisation is addressed by FIA_UID.2, because this SFR makes sure that only authorised persons can act as administrators. In addition FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/Version and FMT_MTD.1/Admin specify the actions allowed for the administrator.

O.OperatorAuthorisation is also addressed by FIA_UID.2, because this SFR makes sure that only authorised persons can act as operators. In addition FMT_SMR.1, FMT_SMF.1 and FMT_MTD.1/Version specify the actions allowed for the operators.

O.DisplayVersion is addressed by FMT_SMF.1, which specifies a requirement to output the TOE's version number on request of the Operator and Administrator.

O.LogData is addressed by FAU_GEN.1/Audit, which require suitable log data to be generated.

O.DeletionEphemeralData is addressed by FDP_RIP.1 and FCS_CKM.4, which require deletion of security relevant data after their use.

O.ProtocolMRTD is realised by several SFRs as follows: The SFRs FCS_CKM.1/*, FCS_CKM.4, FCS_COP.1/* and FCS_RND.1 from class FCS provide the various cryptographic functions and protocols used for the MRTD protocols (including the generation of keys, where applicable). The SFRs FIA_API.1/*, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6/BT from class FIA describe properties of the authentication protocols used between TOE and MRTDs. FAU_GEN.1/PA requires the TOE to present the enforcement and the result of the Passive Authentication to the Operator of the Inspection System.

O.UpdatingSoftware is realized by FDP_IFF.1, FDP_IFC.1, and FCS_COP.1/SW, which make sure that only authentic software is accepted and moreover, that only newer software is accepted. FMT_SMF.1, FMT_SMR.1 and FMT_MTD.1/Admin make sure that only the administrator is able to initiate a firmware update thereby changing the TOE configuration.

6.4 Dependency rationale for SFRs

The dependency rationale for all SFRs from [PP-IS] is provided in [PP-IS, 6.3.2]. For the additional SFR FCS_COP.1/SW the following dependency rationale is provided:

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/SW	[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	Not fulfilled formally, but FMT_SMF.1 and FMT_MTD.1/Admin allow the administrator to manage this public key Not fulfilled: For a public key there is no security requirement for key destruction.
FDP_IFC.1	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1 The dependency FMT_MSA.3 is not fulfilled as there are no static attributes to be initialized by the TOE.

Table 6: Dependency rationale for SFRs

6.5 Security Assurance Requirement Rationale

The assurance level was taken from [PP-IS]. Please see [PP-IS, 6.3.3] for a rationale for SARs.

7 TOE Summary Specification

This chapter presents a short overview of the security functions implemented by the TOE.

7.1 SF.PROTOCOLS

SF.PROTOCOLS ensures that the following protocols for communication between itself and eMRTDs are enforced according to [EAC2.10], and [ICAO_9303] (**FIA_API.1/BAC, FIA_API.1/PACE, FIA_UAU.4, FIA_UAU.5, and FIA_UAU.6**):

- BAC
- Chip Authentication
- PACE
- Passive Authentication

It also ensures that the necessary cryptographic operations for encryption/decryption (**FCS_COP.1/SYM**), signature verification (**FCS_COP.1/CER**), random number generation (**FCS_RND.1**), key generation/derivation (**FCS_CKM.1/KDF, FCS_CKM.1/DH, FCS_CKM.1/PACE, FSC_COP.1/SHA, FCS_COP.1/MAC**) and key destruction (**FCS_CKM.4**) are performed in a secure manner.

The TOE also presents the status for Passive Authentication and Chip Authentication to the operator (**FAU_GEN.1/PA**).

Further, all sensitive data including chip data and passwords will be wiped upon deallocation (**FDP_RIP.1**).

7.2 SF.MANAGEMENT

SF.MANAGEMENT enforces that the following management functions are accessible to the administrator of the TOE (**FIA_UID.2, FMT_SMR.1, FMT_SMF.1, and FMT_MTD.1/Admin**):

- Modification of configuration data of the TOE
- Initiate firmware update
- View the version number of the TOE
- Verify date and time

For firmware update the SF ensures that the update is only performed if the version number of the firmware to be installed is higher than or equal to the version number of the installed firmware and authenticity of the firmware to be installed could be verified using signature verification (**FCS_COP.1/SW, FDP_IFC.1, FDP_IFF.1**).

It further enforces that operators are allowed to view the version number of the TOE and verify date and time (**FMT_MTD.1/Version**).

7.3 SF.AUDIT

The TOE generates audit data (**FAU_GEN.1/Audit**) which is then stored by the environment. Table 4 lists the events and further audit relevant information that will be logged. At least the date and time of the event, the type of the event, and the outcome of the event are part of the generated audit log.

8 References

The following documentation was used to prepare this ST:

[CC] Common Criteria for Information Technology Security Evaluation –
Part 1: Introduction and general model,
dated September 2012, version 3.1 R4
Part 2: Security functional requirements,
dated September 2012, version 3.1, R4
Part 3: Security assurance requirements,
dated September 2012, version 3.1, R4

[CEM] Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated September 2012, version 3.1 R4

[PP-IS] Common Criteria Protection Profile for Inspection Systems (IS), BSI-CC-PP-0064, Version 1.01, 2010

[ST_DRA] Security Target Bundesdruckerei Document Reading Application, Version 1.2.12, Bundesdruckerei GmbH, 18.10.2013.

[ICAO_9303] ICAO Doc 9303, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents - Part 1: Machine Readable Passport, volume 2, ICAO, 6th edition, 2006

[ICAO_PKI] ICAO. Technical Report: PKI for Machine Readable Travel Documents offering ICC read-only access. V1.1. International Civil Aviation Organization, 2004-10.

[EAC2.10] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents; Version 2.10; 20. March 2012.

[FIPS180-4] FIPS 180-4; FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), March 2012.

[PKCS#1] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003.

9 Glossary and Abbreviations

Glossary:

Term	Definition
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Audit entries generated by the TOE and stored in the TOE environment
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 (BAC)	Security mechanism defined in [ICAO_9303] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminal's part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the MRTD holder 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. [ICAO_9303]
Biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).
Complete Inspection System	A complete inspection system is a terminal providing respective services to a human user. E.g. such a terminal can be an attended terminal operated by an border control officer or also an self-service terminal operated by the electronic identity document holder itself. In this sense the TOE described in this protection profile is a major internal part of an complete inspection system.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [ICAO_9303]

Term	Definition
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used to validate card verifiable certificates.
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [ICAO_9303], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
Document Basic Access Keys	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [ICAO_9303]. 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 (SO_D)	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 (C_{DS}). [ICAO_9303]
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
Eavesdropper	A threat agent with Enhanced-Basic 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. [ICAO_9303]
ePass	Look at the term *Machine readable travel document (MRTD).*

Term	Definition
eRA	Look at the term *Machine readable travel document (MRTD).*
Extended Access Control	Security mechanism identified in [ICAO_9303] by means of which the MRTD'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 itself with Personalization Agent Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference 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 terminal's part of the Extended Access Control Authentication Mechanism.
Firmware update	The Firmware update is a secure mechanism to install a new version of the Inspection System's Firmware, including the TOE.
Firmware update component	The Firmware update component is a part of the TOE environment, which realizes access to the storage media during validation of the Firmware update
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [ICAO_9303]
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
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. [ICAO_9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

Term	Definition
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.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer.
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. [ICAO_9303]
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. [ICAO_9303]
Inspection or Inspection Process	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [ICAO_9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is an integrated circuit.
Integrity	Ability to confirm that 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). [ICAO_9303]
Issuing State	The Country issuing the MRTD. [ICAO_9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO_9303]. The capacity expansion technology used is the MRTD's chip.

Term	Definition
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [ICAO_9303] as specified by ICAO on the contact-less integrated circuit. It presents contact-less readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (3) the digitized portraits (EF.DG2), (4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (5) the other data according to LDS (EF.DG5 to EF.DG16). (6) EF.COM and EF.SOD
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contact-less 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. [ICAO_9303]
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. [ICAO_9303]
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. [ICAO_9303]
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. [ICAO_9303]

Term	Definition
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 [ICAO_9303], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) 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 ICAO, [ICAO_9303].
MRTD's chip Embedded Software	Software embedded in an 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.
MRZ	Machine Readable Zone (on an eMRTD)
nPA	The contactless smart card integrated into the plastic, optical readable cover and providing the following applications: ePassport, eID and eSign (optionally).
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint 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.
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.

Term	Definition
Receiving State	The Country to which the Traveller is applying for entry. [ICAO_9303]
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. [ICAO_9303]
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 contact-less communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall all be valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel. [ICAO_9303]
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
Trust anchor	The trust anchor is a root CA stored in the hardware (security controller) of the TOE
TSF data	Data created by and for the TOE that might affect the operation of the TOE ([CC] part 1).
Unpersonalized MRTD	The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.
User data	Data created by and for the user that does not affect the operation of the TSF ([CC] part 1).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [ICAO_9303]
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 following abbreviations are used in this Security Target:

Abbreviation	Definition
ACL	Access Control List
BAC	Basic Access Control
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CIM	Consistency Instruction Manual
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
eAT	Elektronischer Aufenthaltstitel (electronic resident permit)
eID	Electronic Identification
eMRTD	Electronic Machine Readable Travel Document
ePass	Elektronischer Reisepass (electronic passport)
eRA	Elektronischer Reiseausweis (electronic travel document)
IS	Inspection System
IT	Information Technology
nPA	Neuer Personalausweis
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality