BUNDESDRUCKEREI

Security Target

Bundesdruckerei Document Application with tamper-evident casing

Author	Bundesdruckerei GmbH
Version	1.54
Date	11.09.2020
Certification-ID	BSI-DSZ-CC-1161
Target of Evaluation	Bundesdruckerei Document Application with tamper-evident casing
Evaluation Assurance Level	EAL 3
PP Conformance:	BSI-CC-PP-0064-V2-2018 (see [PP-DMT])

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, PA, eAT, ePass

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 with tamper-evident casing**
ST Version:	see Title Page
Date:	see Title Page
Author:	Bundesdruckerei GmbH
Certification-ID:	see Title Page
TOE Identification:	Bundesdruckerei Document Application with tamper-evident casing
TOE Version:	2.3.2
TOE Casing Version:	0
TOE Platform:	VISOTEC® V-Änderungsterminal Firmware
Guidance Documents:	AGD - VISOTEC® V-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 5 as of April 2017.
Evaluation Assurance Level:	EAL 3

PP Conformance:	BSI-CC-PP-0064-V2-2018 (see [PP-DMT])
Keywords:	CC, ST, Common Criteria, Security Target, Inspection System, PA, eAT, ePass

1.2 TOE Overview

The Target of Evaluation (TOE) addressed by this Security Target (ST) is the Bundesdruckerei Document Application with tamper-evident casing; also named "Document Application" in this document; together with components that are responsible for the secure communication to a control software running on an external PC and the physical enclosure of the TOE.

The Document Application is used by an application running on a Document Management Terminal (DMT) to read the German Passport (ePass), to read and update the electronic data of the German identification card ("Personalausweis (PA)") and electronic resident permit ("elektronischer Aufenthaltstitel (eAT)") as well as to verify the document's authenticity and the integrity of its data.

The following sections use the term Document Management Terminal, whenever the physical instantiation of the TOE and enclosure and components within the enclosure according to Figure 1: TOE demarcation is referenced.

The TOE is operated by governmental organisations, e.g. municipal office, police, government or other state approved agencies. The TOE is specifically applied in registration offices to allow card holders to verify that their ePass, PA or eAT is working correctly. In case of PA and eAT 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 PA or eAT can be activated or deactivated. Additionally the TOE ensures secure communication to an external control software and provides a tamper-evident enclosure.

Necessary protocols for the communication of the TOE with the electronic identity documents like the ePass, PA or eAT are described in [ICAO_9303] and [TR-03110-1], [TR-03110-2], [TR-03110-3].

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 part of a Document Management Terminal (DMT) used to

- read and modify data records on the electronic identity documents
- verify the integrity and authenticity of that eID data
- activate and deactivate the eID functionality.

1.3.2 Supported Protocols

The TOE implements the following protocols to communicate with electronic identity documents:

Protocol Name	Specified in	Use Case
BAC	[ICAO_9303]	Confidentiality of submitted chip data, authentication and secure channels
Chip Authentication	CAv1: [TR-03110-1] CAv2: [TR-03110-1]	Authenticity of document chip, secure channels, confidentiality of submitted chip data
PACE	[TR-03110-2] for eIDs [ICAO_9303] for eMRTDs	Confidentiality of the submitted chip data, authentication and secure channels, Confidentiality, authenticity and integrity of the secure channel to the Secure Access Module.
Passive Authentication	[ICAO_9303] and [TR-03110-1]	Authenticity and integrity of the chip data
Terminal Authentication	TAv1: [TR-03110-1] TAv2: [TR-03110-2]	Authenticity and authorisation of the Document Management Terminal (DMT).

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 Pairing between TOE and control software Initiate firmware update View version number of the TOE
Operational	Operator	Read out/write data from/to electronic identity document Check pairing 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

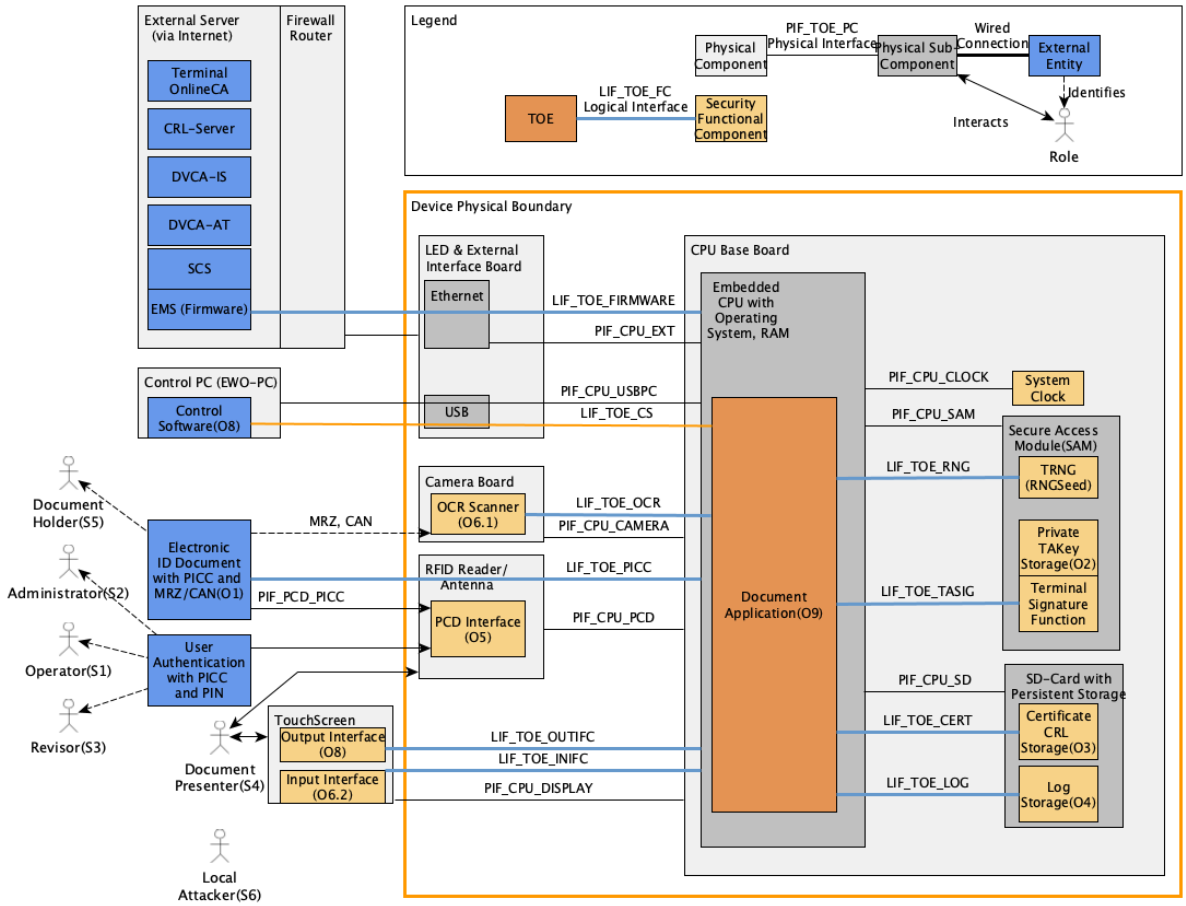

Figure 1: TOE demarcation

The physical scope and boundary of the TOE is depicted in Figure 1: TOE demarcation. The TOE is the document application of the product Document Management Terminal including additional functionality for secure communication with the external Control-PC plus the enclosure of the Base Unit. The TOE is accompanied by its dedicated guidance documentation.

Figure 1: TOE demarcation shows a user centric view onto the TOE and the TOE environment.

The platform for the TOE is the VISOTEC® V-Änderungsterminal Firmware, which is based on a special hardened Linux Kernel of the 4.1 series with secure boot and the GNU libc library. The underlying hardware is a 32-bit embedded controller.

All cryptographic operations related to Table 1 are performed in software by the TOE except for the signing operation needed for Terminal Authentication that is

performed by the SAM. Private keys that are used for other authentication mechanisms are stored temporarily in the volatile memory of the TOE.

The following list shows the components in the environment of the TOE that the TOE relies on (these components do not belong to the TOE):

- A touchscreen for user interaction
- Proximity coupling device (PCD) for communication with electronic identity documents and authentication of users with security tokens
- Camera with infrared document lighting (MRZ/CAN reader)
- Ethernet network interface for certificate and CRL download and firmware download.
- USB interface to Control-PC with Control-Software to read/write data groups of documents
- System Clock
- Flash Memory Storage for audit data and certificates/CRLs
- Secure Access Module
- Control PC
- External Server
- Firewall
- Router
- Operating System
- Electronic ID document with PICC
- User authentication with PICC (token)
- Other Hardware components (e.g. CPU, RAM, I/O)

The hardware components of the Document Management Terminal are physically separated into a base unit comprising CPU-Base Board, LED & IF Board, Camera Board and Reader & Antenna Board and the Touchscreen for user interaction. The base unit and touchscreen of the Document Management Terminal are connected by cable.

Physical Interfaces are implemented as follows:

- PIF_CPU_DISPLAY: The physical Interface between touchscreen and CPU-Base Board is realized by USB2.0 in Device-Mode.
- PIF_CPU_USBPC: The physical Interface between external Control-PC and CPU-Base-Board is realized by USB2.0 in Host-Mode.
- PIF_CPU_EXT: The physical Interface between external Network (Internet) and CPU-Base-Board is realized by Fast-Ethernet.

- PIF_CPU_CS: The physical Interface between Flash-Memory-SD-Card and CPU-Base-Board is realized by SD-Card-Interface.
- PIF_CPU_CLOCK: The Real-Time-Clock is physically soldered onto the CPU-Base-Board.
- PIF_CPU_SAM: The Secure Access Module Interface to the CPU-Base-Board is a SmartCard Using USB-Interface.
- PIF_CPU_OCR: The physical Interface between Camera Board and CPU-Base-Board is realized by USB with RGB video data transfer. The OCR is based on IR illumination and reading of the MRZ/CAN.
- PIF_PCD_PICC: The physical interface between PCD (RFID Transceiver) in the Terminal and PICC (RFID Chip in Electronic Document) is realized by ISO14443-1, ISO14443-2 (Type A, Type B), ISO14443-3, ISO14443-4.
- PIF_CPU_PCD: The physical interface between PCD (RFID Transceiver) and CPU-Base-Board is USB.

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 electronic identity documents,
- Protection of sensitive personal data from electronic identity documents and TSF data,
- Deterministic random number generation,
- Management including verification of firmware updates, secure pairing with control software running on a connected computer
- Secure storage and usage of private keys (except TA signer key),
- Generation of audit data, and
- Tamper evidence.

The TOE uses the following security functionality of the environment:

- Authentication of users (by means of authentication tokens),
- Installation of firmware update,
- Storage of audit data
- Physical protection of the TOE,
- Physical protection by the surrounding building, and
- a SAM that generates seed (entropy) for the DRG in the TOE, and stores the private TA Signer key

Logical Interfaces are assigned to the following physical Interfaces:

- LIF_TOE_OUTIFC: Output Interface within the enclosure is realized via PIF_CPU_DISPLAY.
- LIF_TOE_INIFC: touchscreen within the enclosure is realized via PIF_CPU_DISPLAY.
- LIF_TOE_CS: The logical interface between Document Application and Control Software is realized via PIF_CPU_USBPC with the RNDIS protocol.
- LIF_TOE_OCR: The logical interface between Document Application and OCR Reader is realized via PIF_CPU_CAMERA
- LIF_TOE_PICC: The logical interface between Document Application and Chip in the Electronic ID Document is realized via PIF_CPU_RFID with the following protocols: [ISO7816-4], PACE [TR-03110-2], BAC [ICAO_9303], Terminal Authentication v1 [TR-03110-1] or Terminal Authentication v2 [TR-03110-2], Chip Authentication v1 [TR-03110-1] or Chip Authentication v2 [TR-03110-2], Passive Authentication [TR-03110-2].
- LIF_TOE_CERT: The logical interface between Document Application and Certificate/CRL Storage is realized via PIF_CPU_SD. The file system driver of the Document Terminal Operating System (Linux) encrypts data before and decrypts data after transfer over LIG_TOE_CERT.
- LIF_TOE_LOG: The logical interface between Document Application and Log Storage is realized via PIF_CPU_SD The file system driver of the Document Terminal Operating System (Linux) encrypts data before and decrypts data after transfer over LIF_TOE_LOG. The Log-Entries are additionally protected by hashes.
- LIF_TOE_TASIG: The logical interface between Document Application and Terminal Authentication (Signature Function and Private Key Storage) is realized via PIF_CPU_SAM with the following protocols: PACE Authentication according to [TR-03110-2] Sec.3.2, [ISO7816-4].
- LIF_TOE_FIRMWARE: The logical interface between Firmware-Download-Storage for the TOE and External Firmware Server is realized via PIF_EXT_ETH.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be

- **Common Criteria Part 1 (Version 3.1 Revision 5, April 2017)**.
- **Common Criteria Part 2 (Version 3.1, Revision 5, April 2017) extended** as functional components as defined in part II of [CC] and also the extended functional components FCS_RNG.1 and FIA_API.1 as defined in [PP-DMT] have been used.
- **Common Criteria Part 3 (Version 3.1, Revision 5, April 2017) 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 Document Management Terminal [PP-DMT].

This Security Target claims strict conformance to the Base-PP of [PP-DMT].

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.

Note from ST Editor: Sections in this chapter are copied from BSI-CC-PP-0064-V2-2018 (see [PP-DMT]). Changes from ST Editor are *italicized.* Beside the changes to the text, some additional headlines have been introduced to facilitate referencing parts of the document.

3.1 External entities

The following external entities interact with the TOE:

3.1.1 Subjects

3.1.1.1 Operator (S1)

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

3.1.1.2 Administrator (S2)

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).

3.1.1.3 Revisor (S3)

The Revisor is a person who is able to access the TOE on a dedicated service interface *using a Control Software on a local Control PC* to inspect the log files of the TOE.

3.1.1.4 Electronic Identity Document presenter (S4)

Person presenting the electronic Identity Document to the Document Management Terminal and claiming the identity of the electronic Identity Document holder.

3.1.1.5 Electronic identity document holder (S5)

The rightful/legitimated holder of the electronic identity document for whom the issuing authority personalised the electronic identity document.

3.1.1.6 Attacker (S6)

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. Hereby, electronic identity document presenter (S4) and holders (S5) may also be considered as potential attackers.

3.1.2 Objects

3.1.2.1 Electronic Identity Document (O1)

An eMRTD or eID Card supporting cryptographic mechanisms which allows the Document Management Terminal to check their Integrity and Authenticity. The Electronic Identity Document is presented to the Document Management Terminal which then communicates with the TOE secured by cryptographic means.

3.1.2.2 Private Key Storage (O2)

Storage of the Document Management Terminal's Key Pair. The Key Pair is used for the Terminal Authentication Protocol. The Private Key Store is protected by further security measures to enforce the protection needs of the Document Management Terminal's Key Pairs.

3.1.2.3 Certificate / CRL storage (O3)

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 Document Management Terminal 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.

3.1.2.4 Logfile storage (O4)

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.

3.1.2.5 Proximity Coupling Device (PCD) (O5)

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.

3.1.2.6 Camera (MRZ/CAN reader) (O6)

The camera provides necessary input data to the TOE by scanning the optically readable MRZ/CAN information on the electronic identity document.

3.1.2.7 Touchscreen (O7)

The touchscreen provides necessary input data to the TOE. For example, it is used for entering the PIN for user authentication or setting the eID PIN of the electronic identity document. It further presents results of the Inspection Process as well as further information obtained during the process to the user of the TOE (S1 and/or S2). It is further used for general user interaction/feedback during management of the TOE.

3.1.2.8 Control software (O8)

The control software is a software component that is executed on a *local Control PC* outside of the enclosure of the Document Management Terminal and may be used by the Operator (S1) to display data received from the Document Management Terminal or to send data to the Document Management Terminal.

3.1.2.9 Document Application (O9)

The Document Application is a software that is executed by the operating system running inside the base-unit of the Document Management Terminal. The Document Application is responsible for performing the cryptographic protocols required to communicate with the electronic identity document. Furthermore, it must enforce secured communication paths between itself and the control software (O8).

3.1.3 Other External Entities

Other External Entities support the Objects (O), communicate with the Document Management Terminal Base Unit, but do not directly communicate with the TOE.

3.1.3.1 EMS – EAC Box Management System (E1)

The EMS is contacted by the Document Management Terminal Base Unit (EMS Client) to download the TOE software. The Communication Channel is secured by TLS1.2.

3.1.3.2 CRL-Server (E2)

The CRL-Server is contacted by the base unit (Security Controller) to download the Certificate-Revocation Lists for User Authentication Tokens (e.g. SmartCards for Operator and Administrator Access) and CodeSigner. The Communication Channel is secured by TLS1.2.

3.1.3.3 DVCA-Inspection System (E3)

The DVCA-IS (Document Verifying Certificate Authority for Inspection Systems) is contacted by the Document Management Terminal. The Communication Channel is secured by TLS1.2.

3.1.3.4 DVCA-Authentication Terminal (E4)

The DVCA-AT is contacted by the Document Management Terminal. The Communication Channel is secured by TLS1.2.

3.1.3.5 Terminal OnlineCA (E5)

The Terminal OnlineCA is contacted by the Document Management Terminal. .The Communication Channel is secured by TLS1.2

3.1.3.6 SCS (Signer Certificate Store) (E6)

The SCS is contacted by the Document Management Terminal to read Country Signer Certificates and associated Certificate Revocation Lists. The Communication Channel is secured by TLS1.2.

Note from ST-Author: The Certificate Revocation Lists are implemented in form of defect lists which contain all the information of a classical revocation list but augmented by additional information.

3.2 Assets

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

3.2.1 R.ChipData

R.ChipData is any data which is stored on a chip of an electronic identity document.

Required Protection: Integrity, Confidentiality

3.2.2 R.ChipPassword

The chip password is used to get access to the chip data and is visible on the electronic identity document. 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 [TR-03110-1]). 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

3.2.3 R.PersonalChipPassword

The R.PersonalChipPassword is used to get access to the chip data and is known only to electronic identity document holder (S5). In general, this would be the PIN or PUK, which is verified in the PACE protocol (according to [TR-03110-2]). It must be typed in on a keyboard, etc.

Required Protection: Integrity, Confidentiality

3.2.4 R.AuthenticDocumentData

This asset reflects the genuineness of any data stored on the chip (R.ChipData) according to the governmental regulation of the electronic identity document. In particular, the stored identification data on the document owner must match the official governmental records of the person to whom the document belongs. Furthermore, the PIN (R.PersonalChipPassword) of the document must only be known to the owner.

Required Protection: Integrity

3.2.5 R.TerminalPrivateKey

R.TerminalPrivateKey is the private key of the Document Management Terminal used for Terminal Authentication.

Required Protection: Integrity, Confidentiality

3.2.6 R.SessionKeys

R.SessionKeys are any non-static session and ephemeral keys that are needed by the TOE to perform the protocols described in chapter 1.3.2 Supported Protocols.

Required Protection: Integrity, Confidentiality

3.2.7 R.RandomNumbers

R.RandomNumbers are those random numbers needed by the TOE to perform the protocols described in chapter 1.3.2 Supported Protocols.

Required Protection: Integrity, Confidentiality

3.2.8 R.Certificates

R.Certificates are needed for Passive Authentication and Terminal Authentication.

Required Protection: Integrity

3.2.9 R.CRL

R.CRL are the certificate revocation lists needed for Passive Authentication.

Required Protection: Integrity

3.2.10 R.ConfigurationData

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

Required Protection: Integrity

3.2.11 R.PairingData

The pairing data is used to configure a secure connection between the Document Application (O9) and the control software (O8) that ensures authenticity and confidentiality of the transferred data.

Required Protection: integrity, confidentiality

3.2.12 R.LogData

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

Required Protection: Integrity

3.2.13 R.SensitiveInputData

All further input data besides the R.ChipPassword and R.PersonalChipPassword received from an input interface are considered as R.SensitiveInputData.

Required Protection: Integrity, Confidentiality

3.2.14 R.ProtocolResults

R.ProtocolResults 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 Security Attributes

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

3.3.1 SecAttr.AccTerminalPrivateKey

The security attribute SecAttr.AccTerminalPrivateKey may be assigned to a user. Only users with the security attribute SecAttr.AccTerminalPrivateKey are authorised to enable access to or usage of any terminal private key (R.TerminalPrivateKey).

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.

3.4.1 T.AcceptForgedIdentity – Acceptance of forged electronic identity document

Adverse action: An attacker (S6) fraudulently manipulates or forges the data printed or stored electronically on an electronic identity document in order create a forged identity which deceives the Document Management Terminal.

Threat agent: An attacker (S6) having basic attack potential, being in possession of one or more legitimate electronic identity documents (O1).

Asset: R.ProtocolResults

3.4.2 T.MaliciousDataUpdate - Unauthorized modification of chip data

Adverse action: An attacker (S6) uses the Document Management Terminal and the TOE to modify R.ChipData from electronic identity documents (e.g. the PIN or the postal address) and hereby get in possession of an electronic identity document that does not belong to the attacker or does represent a non-existent person.

Threat agent: An attacker (S6) having basic attack potential, being in possession of a legitimate electronic identity documents (O1).

Asset: R.ChipData, R.AuthenticDocumentData, R.PersonalChipPassword

3.4.3 T.DataCompromise – Compromise of sensitive chip Data

Adverse action: An attacker (S6) uses the Document Management Terminal and the TOE to read sensitive data (R.ChipData) from electronic identity documents.

Threat agent: An attacker (S6) having basic attack potential, not knowing the optically readable MRZ data printed on the electronic

identity document data page in advance nor having access to the electronic identity document.

Asset: R.ChipData

3.4.4 T.FakedLogfileEntries - Spoofing of Logfile Information

Adverse action: An attacker (S6) tries to manipulate the logfiles (O4) to cover information about the TOE installation which might be changed maliciously.

Threat agent: An attacker (S6) having basic attack potential, having temporary physical access to the Document Management Terminal.

Asset: R.LogData

3.4.5 T.Eavesdropping Eavesdropping of sensitive chip data

Adverse action: An attacker (S6) eavesdrops chip data (R.ChipData) transmitted between the electronic identity document Chip, components of the Document Management Terminal, the control software and the TOE.

Threat agent: An attacker (S6) having basic attack potential.

Asset: R.ChipData, R.PersonalChipPassword, R.SensitiveInputData

3.4.6 T.TerminalManipulation – Manipulation of the terminal hardware

Adverse action: An attacker (S6) tries to manipulate hardware components of the Document Management Terminal, e.g. the touchscreen (O7). Hereby, the attacker can compromise the security functionality enforced by the TOE.

Threat agent: An attacker (S6) having basic attack potential, having temporary physical access to the Document Management Terminal.

Asset: R.ConfigurationData, R.PairingData

3.4.7 T.TheftOfTerminal – Theft of terminal

Adverse action: An attacker (S6) tries to steal the whole Document Management Terminal or parts of it and uses it to

	fraudulently readout or update electronic identity documents.
Threat agent:	An attacker (S6) having basic attack potential, having temporary physical access to the Document Management Terminal.
Asset:	R.ChipData, R.AuthenticDocumentData

3.5 Assumptions

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

3.5.1 A.SecureBoot

It is assumed that the the components in the TOE environment that are required for the operation of the Document Management Terminal (c.f. section 1.3.5) provide 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. If the Document Management Terminal implements an external user interface unit for input and output devices (O5+O6+O7), it is assumed that this unit is also protected by secure booting mechanisms so that an initial secure state without protection compromise for that unit is guaranteed. Furthermore, it is assumed the secure boot process provides an integrity check of the TSF.

3.5.2 A.SecureComponents

It is assumed that the components in the TOE environment that are required for the operation of the Document Management Terminal are secure. This assumption includes that no other application - or also parts of the operating system - installed inside the tamper-evident environment of the Document Management Terminal compromise sensitive data, manipulate sensitive data or the results of the electronic identity document 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 Document Management Terminal the TOE relies on work properly as intended (e.g. the output of the Document Management Terminal displays the electronic identity document data as handed over by the TOE, the identification and authentication mechanism of the Document Management Terminal – provided by the operating environment – is effective, the security measures of the certificate/ CRL, private key and logfile storage are in place, etc.).

3.5.3 A.TrainedUser

It is assumed that the authorised Users of the TOE, Operator (S1) and Administrator (S2) and Revisors (S3), 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.

3.5.4 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.

3.5.5 A.PKI

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

3.6 Organisational Security Policies

3.6.1 OSP.SecureAdministration

Only authenticated Administrators (S2) shall be able to perform administrative tasks. These must be performed in a secure manner. This includes that only authorised personnel is allowed to administer the Document Terminal respectively the TOE and that no malware will be installed at the Document Management Terminal. The Administrator has to be authenticated by the TOE before any administrative operations are performed. The Document Management Terminal must verify the authenticity of any software updates before installing them.

3.6.2 OSP.CheckTerminal

The integrity of the entire Document Management Terminal hardware shall be checked regularly by the Operator (S1), but at least at the beginning of his duty or if the terminal is returned from state "PKSDisabled" (c.f. OSP.TAKeyManagement).

The enclosure of the Document Management Terminal shall provide mechanisms that make any physical manipulation detectable.[3]

The Operator (S1) shall verify that the Document Management Terminal is authentic and has not been manipulated. Additionally, if the Document Management Terminal implements an external user interface unit, the Operator (S1) shall perform the same checks for that unit and shall check the pairing between the base unit and that unit.

If external in- or output devices are connected to the Document Management Terminal the Operator (S1) shall check their cable connection.

3.6.3 OSP.Date

The Operator (S1) must perform a daily check of the system date and time. Therefore, he has to use a reliable reference. Especially in the context of certificate validation it must be assured that the system date is correct.

[3] Please note that the following text from the original wording of the OSP has been removed as it does not apply to the current ST: "If the Document Management Terminal implements input and/or output devices in an external user interface unit according to PP-Module DMT-PP-UIU, that unit must be tamper evident too."

3.6.4 OSP.ChipPassword

The Operator (S1) must ensure during a reading or updating operation that any person who is not authorised to know the chip password (R.ChipPassword) is not able to skim it. Therefore, a special distance between the Document Management Terminal and any other person shall be enforced or the used input and output devices shall only be visible to the Operator (S1).

Note from ST-Author: Additionally, the touchscreen is protected against skimming by a privacy filter. Please refer to the guidance documentation for more information.

Note from ST-Author: The specific distance between the DMT and waiting customers is defined in the guidance documents. See also Application note 1 from [PP-DMT]).

3.6.5 OSP.PersonalChipPassword

During reading or updating operations that require entering the personal chip password (R.PersonalChipPassword) by the electronic identity document holder (S5) any other person shall not be able to skim the password. Therefore, a suffi cient distance between the input device of the Document Management Terminal used by the identity document owner (S5) to enter their PIN and any other person

must be enforced or other measures must be implemented to restrict the visibility of the personal password to the document holder (S5).

Note from ST-Author: Additionally, the touchscreen is protected against skimming by a privacy filter. Please refer to the guidance documentation for more information.

Note from ST-Author: The specific distance between the DMT and waiting customers is defined in the guidance document. See also Application Note 2 from [PP-DMT]).

3.6.6 OSP.PrivateKeyStore

The Document Management Terminal shall provide a private key storage (O2) to store the private key (R.TerminalPrivateKey) used for Terminal Authentication (TA).The Private Key Storage (O2) has to perform the signature operation using the terminal private key (R.TerminalPrivateKey) during the Terminal

Authentication protocol in order to authenticate the terminal towards the electronic identity document (O1).

It has to be assured that the private key storage is a device certified according to common criteria assurance package EAL4+ or higher, whereby augmentation results from AVA_VAN.5.

3.6.7 OSP.TAKeyManagement

Organisational measures have to be taken to ensure that access to the private key of the terminal (R.TerminalPrivateKey) is restricted as hereafter specified.

The private key of the terminal (R.TerminalPrivateKey) used for Terminal Authentication (TA) may only be stored in the private key storage (O2) of the terminal.

The access to or usage of (generate, renew and perform signing operation) any terminal private key (R.TerminalPrivateKey) can be either enabled or disabled.

The group of users that is authorised to enable access to or usage of any terminal private key (R.TerminalPrivateKey) must be restricted to users with the security attribute SecAttr.AccTerminalPrivateKey.

The security attribute SecAttr.AccTerminalPrivateKey may only be assigned to Operators (S1).

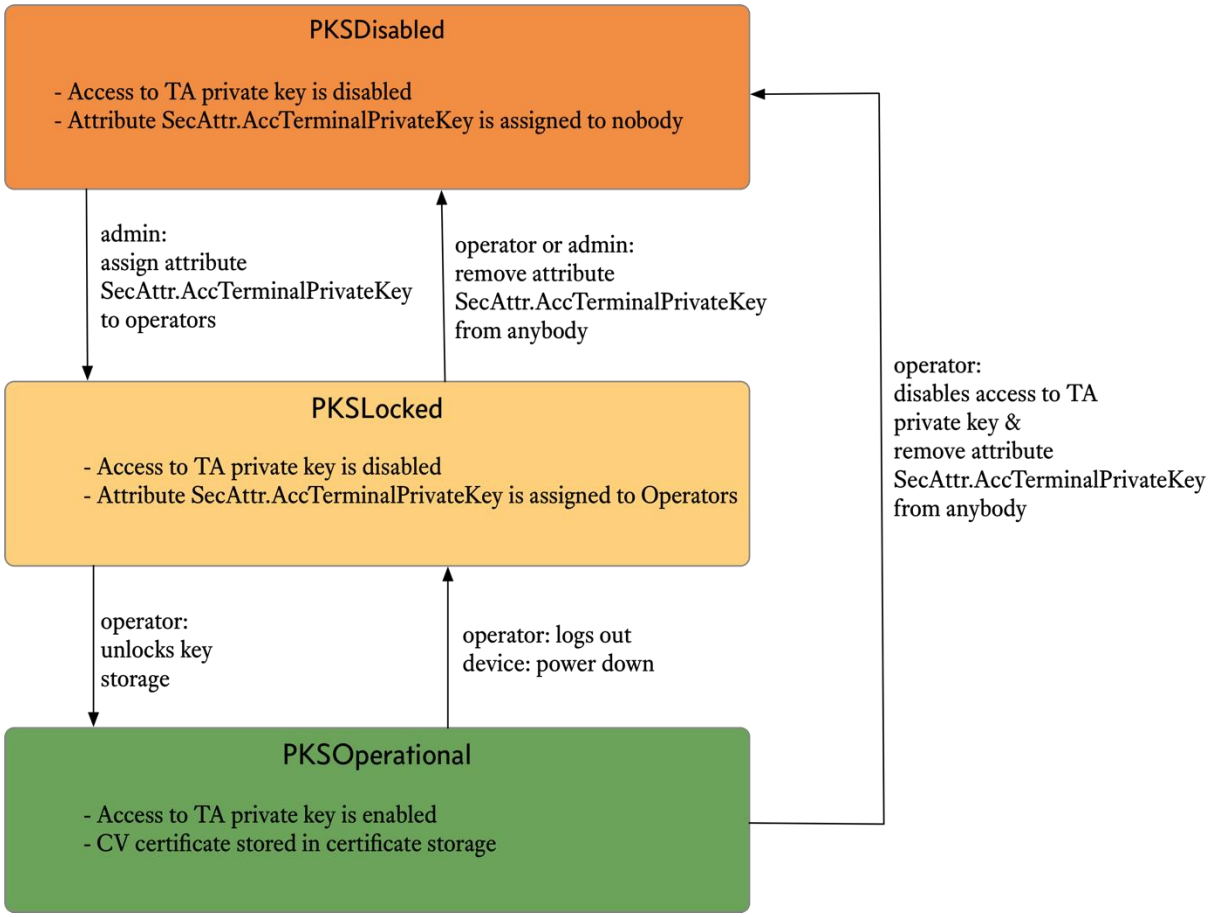

Figure 2: State diagram for Terminal Authentication keys

The security attribute SecAttr.AccTerminalPrivateKey may only be assigned by Administrators (S2), but may be removed by Administrators (S2) and Operators (S1).

The Document Management Terminal supports the following three states[4]:

- State **PKSDisabled**:
  - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is disabled.
  - Attribute SecAttr.AccTerminalPrivateKey is assigned to nobody.
- State **PKSLocked**:
  - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is disabled.
  - SecAttr.AccTerminalPrivateKey authorises Operators (S1) to enable access to or usage of R.TerminalPrivateKey.

[4] Please note that the text of this OSP has been adopted here to reflect the concrete situation of the TOE (while the PP was more generic there).

- State **PKSOperationa**l:
    - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is enabled and a valid terminal authentication certificate is associated to the terminal private key (R.TerminalPrivateKey) and stored in the certificate storage (O3) of the terminal.
    - SecAttr.AccTerminalPrivateKey authorises Operators (S1) to enable access to or usage of R.TerminalPrivateKey.

Application Note 3: A terminal authentication certificate contains the public key linked to the Terminal Authentication private key and is signed by a DV. The certificate is considered valid during the validity period specified in the certificate.

Only an Administrator (S2) shall be allowed to switch the terminal from state "PKSDisabled" to state "PKSLocked".

Operators (O1) and Administrators (O2) must be allowed to return the terminal to state “PKSDisabled”.

Only an Operator (S1) shall be allowed to switch the terminal from state "PKSLocked to state "PKSOperational".

The terminal may only remain in state "PKSOperational" as long as the terminal is under direct supervision by the Operator (S1) and must be returned to state "PKSLocked" or state "PKSDisabled" otherwise.

The terminal must return to state “PKSLocked” if it is powered down in state "PKSOperational".

The terminal may only remain in the state "PKSLocked" if one of the following conditions is fulfilled and must be returned to state "PKSDisabled" otherwise:

1. In case of stationary use, the Document Management Terminal must be installed permanently at its intended environment (e.g. at the working places of a municipal office).
2. In case of mobile use, the terminal may remain in the state "PKSLocked" if the terminal is left unattended by the Operator (S1) for a short time period or if the terminal is stored in a secure environment. The environment is considered secure if physical and remote access to that environment is restricted to the Operator (S1). The terminal must be returned to state "PKSDisabled" if the Document Management Terminal shall be left unattended and cannot be stored in a secure environment.

The necessary transition between the states are depicted in figure 2.

3.6.8 OSP.Logging

The TOE is required to generate a log of security-relevant events, recording the event details and the subjects associated with the event.

In particular, the TOE shall log any updates of the TOE software or configuration (R.ConfigurationData) and any changes of the pairing between the TOE and the control software (R.PairingData).

The stored log data shall be revised regularly to discover malfunctions or attacks. This shall be done by a Revisor (S3) who is not the same person as the Administrator (S2).

3.6.9 OSP.RNG

The TOE is required to generate random numbers that meet a specified quality metric, for use by client applications. These random numbers shall be suitable for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes.

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-DMT] but used in ST are marked bold.

Note from ST-Author: This chapter is copied from [PP-DMT]. Modifications by the ST-Author are *italicized*. Beside the changes to the text, some additional headlines have been introduced to facilitate referencing parts of the document.

4.1 Security Objectives for the TOE

4.1.1 OT.PrivilegedRoleAuthorisation

The TOE must provide an interface to identify and authenticate Administrators (S2) or Revisors (S3). The TOE shall use the result of an Identification and Authentication mechanism to enforce that:

1.) Only authorised Administrators (S2) are allowed to change the TOE's configuration (including update of the TOE's current version).

2.) Only authorised Administrator (S2) shall be allowed to assign the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) and hereby switch the *Document Management Terminal* from state "PKSDisabled" to state "PKSLocked".

3.) Authorised Administrators (S2) shall be allowed to remove the security attribute SecAttr.AccTerminalPrivateKey.

4.) Only authorised Revisors (S3) are allowed to readout the logfile storage or to inspect the log files.

The TOE may use those Identification and Authentication mechanisms provided by the operating system.

Application Note 4: The identification and authentication (I&A) mechanism has to be provided by the environment according to OE.SecureComponents.

Note from ST-Author: The mechanism for Identification and Authentication of (S2), (S3) is implemented by the environment. The interface for Identification and Authentication of Administrators and Revisors is the Interface between TOE and Touchscreen plus the Interface between TOE and PCD (Two-Factor Authentication). See also Application Note 4 from [PP-DMT]).

4.1.2 OT.OperatorAuthorisation

Before chip data (R.ChipData) is read or modified the TOE must enforce the authentication of the Operator (S1) 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.

Only authorised Operators (S1) with the security attribute SecAttr.AccTerminalPrivateKey shall be allowed to retrieve a Terminal Authentication CV certificate from the DV and to enable access to or usage (generation, renewal and signing operation) of a terminal private key (R.TerminalPrivateKey) stored in the terminal private key storage (O2).

Authorised Operators (*S1*) shall be allowed to remove the security attribute SecAttr.AccTerminalPrivateKey.

Application Note 5: If sensitive chip data shall be read on a self-service terminal this could be made possible by giving the document holder the authorisation only for reading his/her own data and this would be proved by a secret password known by the holder and the document's chip.

Application Note 6: The identification and authentication (I&A) mechanism has to be provided by the environment according to OE.SecureComponents. The ST Author may decide to implement the I&A mechanism in the TOE. In this case the objective for the environment to provide an I&A mechanism may be replaced by an objective for the TOE. Requirements on the authentication means are given in OE.AuthenticationMeans.

Note from ST-Author (in response to application note 5): The TOE does not support a self-service mode. So, this kind of authorisation is not required.

Note from ST-Author (in response to application note 6) The mechanism for Identification and Authentication of (S1) is realized by the environment of the TOE. The interface for Identification and Authentication of Operators is the Interface between TOE and Touchscreen plus the Interface between TOE and PCD (Two-Factor Authentication).

4.1.3 OT.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.

4.1.4 OT.Logdata

The TOE shall write log data at least about every change in configuration or software updates or any changes of the pairing between the TOE and the control software (R.PairingData).

4.1.5 OT.VerifySoftwareUpdateSignature

The TOE shall verify the authenticity of any software updates installed at the document management terminal by checking the signature of any update. Only successful verified updates are allowed to be installed.

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

4.1.6 OT.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 (R.ChipData, R.ChipPassword), every generated random number (R.RandomNumbers), ephemeral key and session key (R.SessionKeys) and sensitive input data (R.SensitiveInputData).

4.1.7 OT.Protocols

The TOE shall implement the:

1. Basic Access Control (BAC) protocol according to the specifications [ICAO 9303] Sect. 4.3 (Basic Access Control)

2. Password Authenticated Connection Establishment (PACE) protocol according to [ICAO 9303], Sec 4.4 (PACE) or [TR-03110-2], Sec. A.3.2 (PACE)

3. Passive Authentication protocol according to [ICAO 9303], Part 11, Section 5.1 and [TR-03110-1], Sec. 1.1

4. Terminal Authentication protocol according to [TR-03110-1] Sec. 3.5 (Terminal Authentication Version 1) or [[TR-03110-2], Sec. 3.3 (Terminal Authentication Version 2)

5. Chip Authentication protocol according to [TR-03110-1] Sec. 3.4 (Chip Authentication Version 1) or [[TR-03110-2], Sec. 3.4 and 3.5 (Chip Authentication Version 2 and 3)

The TOE shall enforce the establishment of secure messaging between the electronic identity document's chip and Document Application in dependency on the protocols supported by the chip.

Application Note 7: As part of the terminal authentication protocol a signing operation using the terminal private key (R.TerminalPrivateKey) is required. Since that private key may only be stored in the private key storage (O2) of the Document Management Terminal, also the signing operation has to be performed by the key storage. Therefore, the TOE does not need to implement that operation itself but has to rely on the private key storage for the signing operation (c.f. OE.SecureComponents).

Note from ST-Author: The signing operation using the terminal private key (R.TerminalPrivateKey) is perfomed by the Secure Access Module (SAM) which contains the private key storage (O2) of the Document Management Terminal. The SAM is not part of the TOE.

4.1.8 OT.TamperEvidence - Tamper Detection

The TOE shall provide measures to protect its security functions and its environment inside the enclosure of the Document Management Terminal against tampering. In particular, the TOE shall make any physical manipulation within the scope of the intended environment detectable for the Operators (S1) and Administrators (S2) of the TOE.

4.1.9 OT.ControlSoftwareSecureComm – Secure communication between the Document Management Terminal and the control software

The TOE must provide a secure channel for communication with the control software executed on an external computer, providing integrity, authenticity and confidentiality of the transmitted data. The secure channel shall mutually authenticate the control software and the terminal. The terminal shall provide identification data to the control software that allows to unambiguously identify the terminal.

4.1.10 OT.RandomNumberGenerator - Random number quality

Random numbers generated and provided to client applications for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes shall meet a defined quality metric in order to ensure that random numbers are not predictable and have sufficient entropy.

4.2 Security Objectives for the operational Environment

4.2.1 OE.AuthenticationMeans

Operators (S1), Administrators (S2) and Revisors (S3) must be authenticated by at least two authentication factors from different categories, whereby at least the categories possession-based authentication factor and knowledge-based authentication factor must be taken into account.

4.2.2 OE.SecureBoot

The components in the TOE environment that are required for the operation of the Document Management Terminal (c.f. section 1.3.5) must provide mechanisms to boot the Document Management Terminal's OS and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed.

The devices drivers of any external input and output device (O5+O6+O7) must also be protected by secure booting mechanisms.

Application Note 8: If the software and the device drivers of an external component are not updatable by any means secure booting mechanisms can be assumed for that component.

Note from ST-Author: No User Interface Unit is connected to the base unit. The software of the SAM is not updateable. The base unit supports a secure boot.

4.2.3 OE.SecureComponents

Any private key storage (O2), certificate and CRL storage (O3), logfile storage (O4) input and output device (O5+O6+O7) and any other component that is part of the Document Management Terminal shall be secure. Other applications installed at the Document Management Terminal as well as the operating system itself shall not compromise and/or manipulate sensitive data and shall not penetrate the TOE. The components shall ensure that any data transferred from the components to the TOE or vice versa are transmitted unaltered. Further components of the Document Management Terminal the TOE relies on, the certificate and CRL store respectively, the private key storage and the identification/authentication mechanism of the operating environment shall work properly as intended:

- An effective identification/authentication mechanism shall be implemented by the Document Management Terminal in the environment of the TOE. This identification/authentication mechanism shall provide information to the TOE which allows the TOE to assign roles to identities. Such an identification/authentication mechanism may be provided by the operating system.
- The private key storage (O2) shall be certified according to the Common Criteria at least with the assurance level EAL4+, whereby augmentation results from AVA_VAN.5. The storage shall provide the required functionality to perform the signing operation necessary for the Terminal Authentication protocol.
- The security measures of the certificate and CRL storage (O3) and the private key storage (O2) shall be in place.
- A secure storage for logfiles (O4) shall be implemented which enforces access control.
- Input devices (O5+O6) shall ensure that any data that is entered is transferred to the TOE unaltered.
- Output devices (O7) shall ensure that any data received by the TOE is presented unaltered.
- If any input and/or output device (O5+O6+O7) necessary for the operation of the Document Management Terminal is situated outside of the tamper-evident environment according to OT.TamperEvidence, they must be directly connected to the base unit by cable. In particular, no hubs or active cables are allowed in the connection between the base-unit and the

input and/or output device. The devices must remain in close proximity to the base unit during operation, i.e. they must remain in sight of the Operator (S1).

4.2.4 OE.TrainedUser

The Users – Operators (S1), Administrators (S2) and Revisors (S3) – of the Document Management Terminal shall be well-trained and trustworthy in a sense not to compromise the TOE installation itself or the assets secured by the TOE and the TOE environment.

4.2.5 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 Keys and the Certificates as well as Certificate Revocation Lists shall be ensured. Furthermore, for the Private Key the confidentiality has to be ensured.

4.2.6 OE.PKI

The environment must provide Public Key Infrastructures for EAC and Passive Authentication according to the specifications in [ICAO_9303], [TR-03110-1] Sec 1.1 depending on the used protocols.

Each PKI environment must provide a Certificate Policy.

4.2.7 OE.SignedCertsAndCRLs

The environment shall make sure that only certificates, certificate-lists and CRLs (R.Certificates, R.CRL) from the certificate storage (O3) are provided to the TOE which are signed by the CSCA or a key signed by the CSCA of the operating state.

4.2.8 OE.SecureAdministration

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

4.2.9 OE.CheckTerminalIntegrity

The integrity of the entire Document Management Terminal hardware shall be checked regularly by Operator (S1), but at least at the beginning of his duty or if the terminal is returned from state "PKSDisabled" (c.f. OE.TAKeyManagement).

The Operator (S1) shall verify that the Document Management Terminal is authentic and has not been manipulated.

If external in- or output devices are connected to the Document Management Terminal the Operator (S1) shall check their cable connection.

4.2.10 OE.Date

The Operator (S1) 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).

4.2.11 OE.ChipPassword

The environment must enable the Operator (S1) or the Electronic identity document holder (S5) to ensure during entering or updating *the chip password (R.ChipPassword) or* the personal chip password (R.PersonalChipPassword) that any person who is not authorised to know that password is not able to skim it. Therefore, a special distance between the Document Management Terminal and any other person shall be enforced. Additionally, the touchscreen is protected against skimming by a privacy filter.

4.2.12 OE.TAKeyManagement

The private key of the terminal (R.TerminalPrivateKey) used for Terminal Authentication (TA) may only be stored in the private key storage (O2) of the terminal.

The access to or usage of (generate, renew and perform signing operation) any terminal private key (R.TerminalPrivateKey) can be either enabled or disabled.

The group of users that is authorised to enable access to or usage of any terminal private key (R.TerminalPrivateKey) must be restricted to users with the security attribute SecAttr.AccTerminalPrivateKey.

The security attribute SecAttr.AccTerminalPrivateKey may only be assigned to Operators (S1).

The security attribute SecAttr.AccTerminalPrivateKey may only be assigned by Admininstrator (S2), but may be removed by any authenticated user.

The Document Management Terminal has to support following three states. Additional states may exist as long as they do not violate or relax the requirements of the three mandatory states:

- State PKSDisabled:
  - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is disabled.
  - *Security* Attribute SecAttr.AccTerminalPrivateKey is assigned to nobody.
- State PKSLocked:
  - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is disabled.
  - SecAttr.AccTerminalPrivateKey authorises Operators (S1) to enable access to or usage of R.TerminalPrivateKey.
- State PKSOperational:
  - Access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) is enabled and a valid terminal authentication certificate is associated to the terminal private key (R.TerminalPrivateKey) and stored in the certificate storage (O3) of the terminal.
  - SecAttr.AccTerminalPrivateKey authorises Operators (S1) to enable access to or usage of R.TerminalPrivateKey.

The terminal may only remain in state "PKSOperational" as long as the terminal is under direct supervision by the Operator (S1) and must be returned to state "PKSLocked" or state "PKSDisabled" otherwise.

The terminal must return to state “PKSLocked” if it is powered down in state "PKSOperational".

The terminal may only remain in the state "PKSLocked" if one of the following conditions is fulfilled and must be returned to state "PKSDisabled" otherwise:

1. In case of stationary use, the Document Management Terminal must be installed permanently at its intended environment (e.g. at the working places of a municipal office).
2. In case of mobile use, the terminal may remain in the state "PKSLocked" if the terminal is left unattended by the Operator (S1) for a short time period or if the terminal is stored in a secure environment. The environment is considered secure if physical and remote access to that environment is restricted to the Operator (S1). The terminal must be returned to state "PKSDisabled" if the Document Management Terminal shall be left unattended and cannot be stored in a secure environment.

4.2.13 OE.CheckLogData

The stored log data (R.LogData) shall be revised regularly to discover malfunctions or attacks. This shall be done by a Revisor (S3) who is not the same person as the Administrator (S2).

4.3 Security Objectives Rationale

The following table provides an overview of the security objectives' coverage:

	OT.PrivilegedRoleAuthorisation	OT.OperatorAuthorisation	OT.DisplayVersion	OT.LogData	OT.VerifySoftwareUpdateSignatur	OT.DeletionEphemeralData	OT.Protocols	OT.TamperEvidence	OT.ControlSoftwareSecureComm	OT.RandomNumberGenerator	OE.AuthenticationMeans	OE.SecureBoot	OE.SecureComponents	OE.TrainedUser	OE.ValidKeyandCertificateData	OE.PKI	OE.SignedCertsAndCRLs	OE.SecureAdministration	OE.CheckTerminalIntegrity	OE.Date	OE.ChipPassword	OE.TAKeyManagement	OE.CheckLogData
T.AcceptForgedIdentity	X		X				X				X						X						
T.MaliciousDataUpdate		X	X								X		X	X								X	
T.DataCompromise		X	X			X	X	X	X		X												
T.FakedLogFileEntries	X			X				X			X		X	X									
T.Eavesdropping						X	X	X	X														
T.TerminalManipulation								X											X				
T.TheftOfTerminal									X														
A.SecureBoot												X											
A.SecureComponents													X										
A.TrainedUser														X									
A.ValidKeyAndCertificateData															X								
A.PKI																X							
OSP.SecureAdministration	X				X													X					
OSP.CheckTerminal								X											X				
OSP.Date																				X			
OSP.ChipPassword																					X		
OSP.PersonalChipPassword																					X		
OSP.PrivateKeyStore							X						X										
OSP.TAKeyManagement	X	X																				X	
OSP.Logging				X																			X
OSP.RNG										X													

Table 3: Security Objectives Rationale

4.3.1 Considerations about Threats

4.3.1.1 T.AcceptForgedIdentity

This threat is covered by the following combination of objectives:

- **OT.PrivilegedRoleAuthorisation** and **OE.AuthenticationMeans** make sure that only authorised Administrators (S2) 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 electronic identity document (O1).
- **OE.SignedCertsAndCRLs** makes sure that only legitimate public keys are accepted for the verification of signatures or certificates provided by an electronic identity documentand/or used by the TOE.
- **OT.Protocols** makes sure that the TOE uses the specified cryptographic protocols to verify the authenticity of data provided by an electronic identity document.
- **OT.DisplayVersion** supports this by making sure that only legitimate software is used.

Application Note 9: All security objectives for the environment and all objectives that mitigate T.Eavesdropping and T.TerminalManipulation also help to address this threat, because they prevent modification or bypass of the TOE. However, this holds for all threats in general, because a TOE, which could be modified by unauthorised persons cannot guarantee any security function. Therefore, this basic support isn't mentioned in the following discussions any more.

4.3.1.2 T.MaliciousDataUpdate

This threat is covered by the following combination of objectives:

- **OT.OperatorAuthorisation** and **OE.AuthenticationMeans** make sure that only authorised Operators (S1) are allowed to use the TOE to update data stored on the chip of the electronic identity document.
- **OE.TrainedUser** makes sure that the Operator (S1) only stores legitimate data (R.AuthenticDocumentData) on the chip of the electronic identity document (O1).
- **OE.SecureComponents** ensures that the input device (O6) transfers the personal chip password (R.PersonalChipPassword) to the TOE unaltered.
- **OE.TAKeyManagement** ensures that the terminal private key (R.TerminalPrivateKey) necessary to get access to an electronic identity document (O1)present in the private key storage (O2) of the Document Management Terminal is only accessible and usable if the Document Management Terminal is situated in a secure environment.

- **OT.DisplayVersion** supports this by making sure that only legitimate software is used.

4.3.1.3 T.DataCompromise

This threat is covered by the combination of the following objectives:

- **OT.OperatorAuthorization** and **OE.AuthenticationMeans** make sure that only authorized Operators (S1) are allowed to use the TOE to read data (R.ChipData) stored on the chip of the electronic identity document (O1).
- **OT.Protocols** and **OT.DeletionEphemeralData** ensure that any sensitive chip data (R.ChipData) transferred between the electronic identity document and the Document Management Terminal is protected in integrity and confidentiality.
- All objective mitigating **T.Eavesdropping** make sure that attackers cannot see secret data during transport between components of the terminal or by finding old secret data in the storage of the terminal.
- **OT.DisplayVersion** supports this by making sure that only legitimate software is used.

4.3.1.4 T.FakedLogFileEntries

This threat is covered as follows:

- **OT.PrivilegedRoleAuthorization** and **OE.AuthenticationMeans** make sure that only authorised Revisors (S3) can readout logfiles from the log storage.
- **OT.LogData** makes sure that log entries (R.LogData) are written, whenever the TOE configuration is changed or updates are installed.
- **OT.TamperEvidence** prevents manipulation of log file entries (R.LogData) during their transport between TOE and storage.
- **OE.SecureComponents** makes sure that the log files are not manipulated during their storage in the logfile storage (O4).

4.3.1.5 T.Eavesdropping

This threat is covered by the combination of the following objectives:

- **OT.Protocols** makes sure that the specified cryptographic protocols are used for communication between TOE and electronic identity document (O1) . In particular this prevents unauthorised reading of secret data (R.ChipData, R.PersonalChipPassword, R.SensitiveInputData) on this interface by establishing secure messaging.

- **OT.DeletionEphemeralData** and **OT.TamperEvidence** make sure that attackers cannot eavesdrop secret data during transport between components of the Document Management Terminal and the TOE.
- **OT.ControlSoftwareSecureComm** makes sure that attackers cannot eavesdrop secret data during transport between the control software and the TOE.

4.3.1.6 T.TerminalManipulation

This threat is covered by the combination of the following objectives:

- **OT.TamperEvidence** prevents tampering of the components the TOE relies on, by embedding them into tamper-evident enclosures.
- **OE.CheckTerminalIntegrity** ensures that any attempted tampering of the Document Management Terminal may be detected by the Operator (S1).

4.3.1.7 T.TheftOfTerminal

This threat is covered by the following objective:

- **OT.ControlSoftwareSecureComm** makes sure that the Document Management Terminal can only communicate with the control software (O8) that has been authorized by an Administrator (S2).

4.3.2 Assumptions

4.3.2.1 A.SecureBoot

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

4.3.2.2 A.SecureComponents

- The identically named security objective for the environment **OE.SecureComponents** addresses this assumption to ensure the secure environment for the TOE.

4.3.2.3 A.TrainedUser,

- **OE.TrainedUser** directly addresses that assumption.

4.3.2.4 A.ValidKeyAndCertificateData

- **OE.ValidKeyAndCertificateData** directly addresses that assumption

4.3.2.5 A.PKI

- **OE.PKI** directly addresses that assumption.

4.3.3 Organizational Security Policies

4.3.3.1 OSP.SecureAdministration

The policy is enforced by the following combination of objectives:

- **OT.PrivilegedRoleAuthorization** makes sure that only authorised Administrators (S2) can change the configuration of the TOE.
- **OT.VerifySoftwareUpdateSignature** ensures that only authenticated software updates may be installed at the Document Management Terminal.
- **OE.SecureAdministration** ensures that only authorised personnel may act in the role of an Administrator (S2) and thus is able to administrate the Document Management Terminal including the TOE.

4.3.3.2 OSP.CheckTerminal

The policy is enforced by the following combination of objectives:

- **OT.TamperEvidence** allows the Operator (S1) to detect modification of the components of the Document Management Terminal.
- **OE.CheckTerminalIntegrity** instructs the Operator (S1) to check the integrity of the Document Management Terminal on a regular basis.

4.3.3.3 OSP.Date

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

4.3.3.4 OSP.ChipPassword

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

4.3.3.5 OSP.PersonalChipPassword

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

4.3.3.6 OSP.PrivateKeyStore

The policy is enforced by the following combination of objectives:

- **OT.Protocols** makes sure that the TOE implements the functionality to perform the Terminal Authentication protocol.
- **OE.SecureComponents** ensures that the private key storage can perform the required signing operation during the Terminal Authentication protocol and that it is certified as required.

4.3.3.7 OSP.TAKeyManagement

The combination of the following objectives ensures that access to or usage of the private key of the terminal (R.TerminalPrivateKey) is restricted appropriately:

- **OE.TAKeyManagement** makes sure that
  - the Document Management Terminal is set up in an environment that can be considered as secure,
  - the terminal provides the required states for securing the private key of the terminal (R.TerminalPrivateKey),
  - the conditions for storing the private key of the terminal (R.TerminalPrivateKey) at the private key storage (O2) of the terminal are fulfilled,
  - the conditions for performing signing operations using the private key of the terminal (R.TerminalPrivateKey) are fulfilled.
- **OT.PrivilegedRoleAuthorization** makes sure that only an Administrator (S2) is allowed to assign the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) and hereby to switch the terminal from state "PKSDisabled" to state "PKSLocked".
- **OT.OperatorAuthorization** makes sure that only an Operator (S1) with the security attribute SecAttr.AccTerminalPrivateKey is allowed to unlock the private key storage (O2) in order to enable the necessary signing operations for Terminal Authentication.

4.3.3.8 OSP.RNG

- **OT.RandomNumberGenerator** addresses this organisational security policy directly as a requirement for the TOE.

4.3.3.9 OSP.Logging

The policy is enforced by the following combination of objectives:

- **OT.LogData** enforces the TOE to write events to a logfile (R.LogData) inside the log storage (O4).
- **OE.CheckLogData** instructs the Revisor (S3) to check the logfiles (R.LogData) stored in the log storage (O4) on a regular basis.

5 Extended Component Definition

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

Note from ST-Author: Application Note 10 of [PP-DMT] was taken into account. No changes to RNG are necessary.

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 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 ~~stricken 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. For the sake of better readability, the iteration operation may also be applied to a non-repeated single component in

order to indicate that such component belongs to a certain functional cluster. In such a case, the iteration operation is applied to only one single component.

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.

6.2 TOE Security Functional Requirements

The TOE satisfies the SFRs described in the following chapter.

6.2.1 Class (FAU) - Logging

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 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 modification of the TOE configuration data (R.ConfigurationData); and

d) software updates; and

e) announcement of having processed the Passive Authentication protocol including the result of the process; and

f) announcement of having processed the Chip Authentication protocol including the result of the process; and

g) [*audit relevant information defined in Table 4*].

FAU_GEN.1.2 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 TSF supports the storage of audit records by the TOE environment (cf. OE.SecureComponents) by poviding the audit records according to FAU_GEN.1.1 c), and d) and by sending these records to the Logfile Storage (O4).

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 according to FAU_GEN.1.1 e) and f) to the Operator (S1).

Application note 12: The TOE makes use of the time stamps provided by the TOE environment (cf. OE.SecureComponents 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
Control Software pairing	When the TOE is paired with the control software, the corresponding log entry will also contain the SHA-256 value of the certificate chain used for pairing
Firmware update	In case of software update: firmware version of new firmware

Table 4: List of auditable events and audit relevant information

Note from ST-Author: The aforementioned table has been added compared to the PP.

Class FCS - Cryptographic Protocols

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

FCS_CKM.1.1/KDF_BAC 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 9303], Part 11, Sect 4.3 (Basic Access Control)]*.

Application Note 13: The ST writer shall perform the open operation in the element FCS_CKM.1.1/KDF_BAC. The cryptographic key generation algorithm and the cryptographic key sizes depend on the protocol which shall be used by the Document Management Terminal. 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 electronic identity document and used by the TOE for FIA_UAU.4. The [ICAO 9303], Part 11, Sect. 4.3 (Basic Access Control), 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.

Note from ST-Author: Application Note 13 was considered.

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

FCS_CKM.1.1/DH_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: *[ICAO 9303] , Part 11, Sec 4.4 (PACE), TR-03110-2, Sec 3.2(PACE)].*

Application Note 14 The cryptographic key generation algorithm and the cryptographic key sizes depend on the protocol which shall be used by the Document Management Terminal for PACE. [TR-03110-2], Sec. 3.2 (PACE) describes the key agreement protocol for PACE. [TR-03110-3], Sec. A.3 (PACE) 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 Key Derivation Algorithm described in [TR-03110-3], A.2.3 (Key Derivation Function), for the TSF required by FCS_COP.1/SYM and FCS_COP.1/MAC

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

FCS_CKM.1.1/DH_CA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Diffie-Hellman key agreement*] and specified cryptographic key sizes [*112 bit (to be used with Triple-DES)*, *128 bit (to be used with AES), 256 bit (to be used with EC DH)*] that meet the following: that meet the following: *[[TR-03110-1] Sec 3.4 (Chip Authentication Version 1), [TR-03110-2] Sec 3.4 (Chip Authentication Version 2)]*.

Application Note 15 The TOE generates a shared secret value with the terminal during the Chip Authentication protocol, see [TR-03110-1] Sec. 3.4 (Chip Authentication Version 1) and [TR-03110-2], Sec. 3.4 and 3.5 (Chip Authentication Version 2) for a protocol description. [TR-03110-3] Sec. A.4.1.2 and Sec. A.4.1.3 (both CAv1 & CAv2) lists the standards for symmetric keys agreed by Chip authentication. 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 Key Derivation Algorithm described in [TR-03110-3], A.2.3 (Key Derivation Function), 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 **as well as the Terminal Authentication (v2) 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 electronic identity document in a new session.

FCS_COP.1/SHA Cryptographic operation – Hash

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

Application note 16: The ST writer shall perform the missing selection operation. The TOE shall implement the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control authentication mechanism (cf. [ICAO 9303], Part 11, Sect. 4.3 (Basic Access Control)). For the Passive Authentication mechanism the TOE must implement at least SHA-1 and SHA-256. The TOE may implement additionally the SHA-224, the SHA-384 and/or the SHA-512 algorithm. The Chip Authentication protocol and the Password Authenticated Connection Establishment protocol may use SHA-1 for session key derivation (cf. [ICAO 9303], Part 11, Sec 9.7.4 (Secure Messaging Keys) or [TR-03110-3], A.2.3 (Key Derivation Function)).

Note from ST-Author: Application Note 16 was considered.

Note from ST-Author: SHA-1 may also be used as a hint for identifying certificates (Subject Key Identifier). This usage is considered not SFR-enforcing.

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: *[[ICAO 9303], Part 11, Sec 9.8 (Secure Messaging), [TR-03110-3] Sec.F (Secure Messaging)*].

Application Note 17 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 electronic identity document 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: [*[ICAO_9303], Part 11, Sec 9.8 (Secure Messaging), [TR-03110-3] Sec. F (Secure Messaging)*].

Application Note 18: 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.

Note from ST-Author: [ICAO_9303] Sec 9.8 requires "Retail-MAC" (ISO9797-1 Mode 3), [TR-03110-3] Section F requires AES-CMAC.

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-224 (brainpoolP224r1), ECDSA/SHA-256 (brainpoolP256r1), ECDSA/SHA-384 (brainpoolP384r1), ECDSA/SHA-512 (brainpoolP512r1)*] and cryptographic key sizes [224 bit, *256 bit, 384 bit, 512 bit*] that meet the following: [*[ICAO_PKI] Section 6.2 (Certificate/CRL Validation and Revocation Checking), [TR-03110-3] Section 2.5 (Certificate Validation), [RFC5280]*].

Application Note 19: 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 [TR-03110-1] Sec 1.1 and [ICAO_9303] Section 5.1, respectively.

Application Note 20: The ST writer shall perform the missing operation for the assignment of the signature algorithm and key sizes as well as the appropriate list of standards supported by the TOE.

Note from ST-Author: Application Note 20 was considered.

FCS_COP.1/UpdateSig Cryptographic operation – Signature Verification of Updates

FCS_COP.1.1/UpdateSig	The TSF shall perform digital signature verification of software update in accordance with a specified cryptographic algorithm *[[ECDSA/SHA-256 (secp384r1, secp256r1)]* and cryptographic key sizes *[256 Bit, 384Bit]* that meet the following: [*[FIPS186-4] and [FIPS180-4]*]

FCS_RNG.1 Generation of random numbers

FCS_RNG.1.1	The TSF shall provide a [*deterministic*] random number generator that implements: [• *(DRG.3.1) If initialized with a random seed by a PTG.2 during start-up the internal state of the RNG shall have at least 255 bit entropy.* • *(DRG.3.2) The RNG provides forward secrecy.* • *(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.*].
FCS_RNG.1.2	The TSF shall provide [*octets of bits*] that meet [*(DRG.3.4) The RNG, initialized with a random seed by the DRG.4 RNG of the SAM which is seeded by a PTG.2, generates output for which 2^{14} strings of bit length 128 are mutually different with probability >1-2^{-8}.* *(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A from AIS31*].

Application Note 10: A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses an random seed to produce a pseudorandom output.

A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

Note from ST-Author: The TOE uses a variant of the hash based random number generator as described in [FIPS186-2, Appendix 3, Section 3.1 - "ALGORITHM FOR COMPUTING m VALUES OF x"] , with the extension for SHA-256 instead of SHA-1.

6.2.2 Class FDP - User Data Protection

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 (R.ChipPassword), Personal Chip Password (R.PersonalChipPassword), Personal Chip Data (R.ChipData), sensitive Input Data (R.SensitiveInputData).

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

6.2.3 Class Identification and Authentication (FIA)

Application note 11: Other families of the class FIA describe only the authentication verifi cation of user's identity performed by the TOE and do not describe the functionality of the TOE to prove its own identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter 'Extended components definition (APE_ECD)') from a TOE point of view.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a Terminal Authentication protocol according to *[[TR-03110-1] Sec. 3.5 (Terminal Authentication Version 1) and [TR-03110-2] Sec. 3.3 (Terminal Authentication Version 2)*] to prove the identity of the TOE.

Application Note 21: This SFR requires the TOE to implement the Terminal Authentication Protocol according to [TR-03110-1] Sec. 3.5 (Terminal Authentication Version 1) and/or [[TR-03110-2], Sec. 3.3 (Terminal Authentication Version 2).

Application Note 22: As part of the terminal authentication protocol a signing operation using the terminal private key (R.TerminalPrivateKey) is required. Since that private key may only be stored in the private key storage (O2) of the Document Management Terminal, also the signing operation has to be performed by the key storage.

Therefore, the TOE shall not implement that operation itself but shall rely on the private key storage for the signing operation (c.f. OE.SecureComponents).

FIA_UAU.2 User authentication before any action

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

Note from ST-Author: In accordance with PP-Application Note 23 FIA_UAU.1 is replaced by FIA_UAU.2.

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.SecureComponents).

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

a) Basic Access Control Authentication Mechanism

b) Password Authenticated Connection Establishment.

Application Note 24: The Basic Access Control Authentication Mechanism [ICAO_9303] Part 11, Sect 4.3 (BAC) and the Password Authenticated Connection Establishment [TR-03110-2] Sec 3.2 (PACE) use a challenge freshly and randomly generated by the terminal to prevent reuse of a response generated by an electronic identity document'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

a. Basic Access Control Authentication Mechanism;

b. Password Authenticated Connection Establishment;

c. Passive Authentication;

d. 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:

a. The TOE accepts the authentication attempt as electronic identity document's 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.

b. After successful authentication as electronic identity document 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 electronic identity document by means of the Basic Access Control Authentication Mechanism or by means of the Password Authenticated Connection Establishment Authentication Mechanism.

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

d. 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 25: 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 electronic identity document. 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 electronic identity document shall use the secure messaging with the keys generated by the Chip Authentication Mechanism after the mutual authentication.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

a. Each response sent to the TOE after successful authentication of the electronic identity document 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 (BAC) Authentication or by the Password Authenticated Connection Establishment (PACE) Mechanism

b. 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.

Application Note 26: The Basic Access Control Mechanism, the Password Authenticated Connection Establishment mechanism and the Chip Authentication Protocol 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 electronic identity document (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

Note from ST-Author: Analog to the approach for FIA_UAU.1, FIA_UID.1 has been replaced by FIA_UID.2 as the assignment in FIA_UID.1 would have been empty.

6.2.4 Class Security Management (FMT)

FMT_MTD.1/TOE-Config Management of TSF data – Update TOE configuration

FMT_MTD.1.1/TOE-Config	The TSF shall restrict the ability to modify the 1.) TOE configuration data (Modify R.ConfigurationData) 2.) Pairing between the TOE and the control software (Modify R.PairingData) 3.) the further TSF data: *[none]* to Administrators (S2).

FMT_MTD.1/EnableOpAccKeyStore Management of TSF data – Enable Operator Access to key store

FMT_MTD.1.1/ EnableOpAccKeyStore	The TSF shall restrict the ability to assign the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) to Administrators (S2).

FMT_MTD.1/UnlockKeyStore Management of TSF data – Unlock key store

FMT_MTD.1.1/ UnlockKeyStore	The TSF shall restrict the ability to enable the access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) stored in the private key storage (O2) to Operators (S1) with the security attribute SecAttr.AccTerminalPrivateKey.

FMT_MTD.1/ReadLog Management of TSF data – Read log data

FMT_MTD.1.1/ReadLog	The TSF shall restrict the ability to query the TOE log data (R.LogData) to Revisors (S3).

Note from ST-Author: Revisor is not underlined in PP, but should be according to PP operator style conventions.

FMT_MTD.1/ReadVersion – Management of TSF data – Read TOE version

FMT_MTD.1.1/ ReadVersion	The TSF shall restrict the ability to query the TOE version and further TSF data: *[date and time]* to Operators (S1), Administrators (S2) and Revisors (S3).

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: 1. Update the TOE configuration data (Modify R.ConfigurationData), 2. Update the pairing between the TOE and the control software (Modify R.PairingData), 3. Read the TOE version, 4. Revise the log data (Read R.LogData), 5. Assign or remove the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) (see Application Note), 6. Enable and disable access to or usage (generation, renewal and signing operation) of a terminal private key (R.TerminalPrivateKey) stored in the terminal private key storage (O2), and *7. [Verify date and time,* 8. *Initiate firmware update]*

Application Note 27: After assigning the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) access to or usage (generation, renewal and signing operation) of a terminal private key (R.TerminalPrivateKey) stored in the terminal private key storage (O2) must still be disabled and may not be enabled by Administrators (S2).

FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles Operators (S1), Administrators (S2), Revisors (S3) and [*none*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.5 Class TSF Physical Protection (FPT)

FPT_PHP.1/BaseUnit Passive detection of physical attack

FPT_PHP.1.1/BaseUnit	The TSF shall provide unambiguous detection of physical tampering of the enclosure of the base unit that might compromise the TSF.
FPT_PHP.1.2/BaseUnit	The TSF shall provide the capability to determine

	whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application note 28: The protection against tampering shall be enforced by the enclosure of the Document Management Terminal.

6.2.6 Class Trusted Paths (FTP)

FTP_TRP.1/ControlSoftware Trusted path – Control Software

FTP_TRP.1.1/ ControlSoftware	The TSF shall provide a communication path between itself and ~~users~~ local control software (O8) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure, *[none]*.
FTP_TRP.1.2/ ControlSoftware	The TSF shall permit *[local users]* to initiate communication via the trusted path.
FTP_TRP.1.3/ ControlSoftware	The TSF shall require the use of the trusted path for transferring chip data (R.ChipData) or presenting if the electronic identity document is genuine (R.ProtocolResults) or receiving updated chip data (R.ChipData) or transferring non-personal chip passwords (R.ChipPassword) or transferring sensitive input data (R.SensitiveInputData) or *[none]*.

Application Note 29: The pairing between the control software and the Document Management Terminal is configured in R.PairingData and may only be modified by an Administrator (S2).

Note by ST-Author: The communication between control software and TOE is secured by a trusted channel. This trusted channel is implemented as a mutually authenticated TLS 1.2 channel. Please refer to chapter 7.4 for an overview of the supported cipher suites.

Application Note 30: The terminal shall provide identification data to the control software that allows the Operator (S1) to unambiguously identify the connected terminal.

Application Note 31: The control software is treated as a local user in FTP_TRP.1.2.

6.3 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).

6.4 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-DMT].

	OT.PrivilegedRoleAuthorisation	OT.OperatorAuthorisation	OT.DisplayVersion	OT.LogData	OT.VerifySoftwareUpdateSignatur e	OT.DeletionEphemeralData	OT.Protocols	OT.TamperEvidence	OT.ControlSoftwareSecureComm	OT.RandomNumberGenerator
FAU_GEN.1 – Audit data generation				X			X			
FCS_CKM.1/KDF_BAC – Cryptographic key generation							X			
FCS_CKM.1/DH_PACE – Cryptographic key generation							X			
FCS_CKM.1/DH_CA – Cryptographic key generation							X			
FCS_CKM.4 – Cryptographic key destruction						X	X			
FCS_COP.1/SHA – Cryptographic operation							X			
FCS_COP.1/SYM – Cryptographic operation							X			
FCS_COP.1/MAC – Cryptographic operation							X			
FCS_COP.1/CER – Cryptographic operation							X			
FCS_COP.1/UpdateSig – Cryptographic operation					X					
FCS_RNG.1 – Generation of random numbers							X			X
FDP_RIP.1 – Subset residual information protection						X				
FIA_API.1 – Authentication Proof of Identity							X			
~~FIA_UAU.1 – Timing of authentication~~	~~X~~	~~X~~								
FIA_UAU.2 - User authentication before any action	**X**	**X**								
FIA_UAU.4 – Single-use authentication mechanisms							X			
FIA_UAU.5 – Multiple authentication mechanisms							X			
FIA_UAU.6 – Re-authenticating							X			
FIA_UID.2 – User Identification before any action	X	X								
FMT_MTD.1/TOE-Config – Management of TSF data	X									
FMT_MTD.1/EnableOpAccKeyStore – Management of TSF data	X									
FMT_MTD.1/UnlockKeyStore – Management of TSF data		X								
FMT_MTD.1/ReadLog – Management of TSF data	X									

	OT.PrivilegedRoleAuthorisation	OT.OperatorAuthorisation	OT.DisplayVersion	OT.LogData	OT.VerifySoftwareUpdateSignatur e	OT.DeletionEphemeralData	OT.Protocols	OT.TamperEvidence	OT.ControlSoftwareSecureComm	OT.RandomNumberGenerator
FMT_MTD.1/ReadVersion – Management of TSF data			X							
FMT_SMF.1 - Specification of Management Functions	X	X	X							
FMT_SMR.1 – Security Roles	X	X								
FPT_PHP.1/BaseUnit - Passive detection of physical attack								X		
FTP_TRP.1/Control Software - Trusted path – Control Software									X	

Table 5: Security functional requirements rationale

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

6.4.1 OT.PrivilegedRoleAuthorisation

This objective is covered by the combination of the following SFRs:

- FMT_SMF.1 specifies the actions that the TOE must be capable to perform.
- FMT_SMR.1 specifies the user roles the TOE must support.
- FMT_MTD.1/TOE-Config and FMT_MTD.1/ReadLog specify the actions that are restricted to Administrators (S2) and Revisors (S3).
- FMT_MTD.1/EnableOpAccKeyStore specifies that only Administrators (S2) may assign the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1).
- FIA_UAU.2 makes sure that any user must be authenticated to the TOE before performing any of the actions listed in FMT_SMF.1.
- FIA_UID.2 makes sure that users can be identified as Administrators (S2) or Revisors (S3) by the TOE.

6.4.2 OT.OperatorAuthorisation

This objective is covered by the combination of the following SFRs:

- FMT_SMF.1 specifies the actions that the TOE must be capable to perform.
- FMT_SMR.1 specifies the user roles the TOE must support.
- FMT_MTD.1/UnlockKeyStore specifies that only Operators (S1) with the security attribute SecAttr.AccTerminalPrivateKey may enable access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) stored in the private key storage (O2).
- FIA_UAU.2 makes sure that any user must be authenticated to the TOE before performing any actions.
- FIA_UID.2 makes sure that users can be identified as Operators (S1) by the TOE.

6.4.3 OT.DisplayVersion

The objective is directly addressed by FMT_SMF.1 and FMT_MTD.1/ReadVersion.

6.4.4 OT.LogData

This objective is addressed by FAU_GEN.1, which requires suitable log data to be generated.

6.4.5 OT.VerifySoftwareUpdateSignature

This objective is addressed by FCS_COP.1/UpdateSig which requires a verification of the signature of each software update.

6.4.6 OT.DeletionEphemeralData

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

6.4.7 OT.Protocols

This objective is covered by the combination of the following SFR's concerning cryptographic operation:

- FCS_COP.1/SHA, FCS_COP.1/SYM and FCS_COP.1/MAC provide the required cryptographic functions to perform secure messaging;
- FCS_CKM.1/KDF_BAC provides the required cryptographic functions to perform key derivation according to the Basic Access Control (BAC) protocol;
- FCS_CKM.1/DH_PACE provides the required cryptographic functions to establish session keys according to the Password Authenticated Connection Establishment (PACE) protocol;

- FCS_COP.1/CER provides the required cryptographic functions to perform Passive Authentication;
- FCS_COP.1/SHA provides the required cryptographic functions to perform Terminal Authentication. (The required signing operation has to be implemented by the private key storage (O2) (c.f. OE.SecureComponents));
- FCS_CKM.1/DH_CA provides the required cryptographic functions to establish session keys according to the Chip Authentication (CA) protocol;
- FCS_CKM.4 provides the required functions to destroy cryptographic key material;
- FCS_RNG.1 provides the capability to generate random numbers required for any protocol;

and the following SFR's that describe the properties of the authentication protocols used between the TOE and an electronic identity document:

- FIA_API.1, FIA_UAU.4, FIA_UAU.5 and FIA_UAU.6

The FAU_GEN.1 requires the TOE to present the enforcement and the result of the Passive Authentication to the Operator (S1) of the Document Management Terminal.

6.4.8 OT.TamperEvidence - Tamper Detection

This objective is directly addressed by the SFR FPT_PHP.1/BaseUnit.

6.4.9 OT.ControlSoftwareSecureComm – Secure communication between the Document Management Terminal and the control software

This objective is addressed by the SFR FTP_TRP.1/ControlSoftware that enforces one-to-one relationship by providing a trusted path to the control software that provides protection in integrity and confidentiality.

6.4.10 OT.RandomNumberGenerator - Random number quality

This objective is directly addressed by the SFR FCS_RNG.1

6.5 Security Functional Requirements Dependency rationale

The dependency rationale for all SFRs from [PP-DMT] is provided in [PP-DMT, 6.2,1].

6.6 Security Assurance Requirements

The minimum Evaluation Assurance Level for this Protection Profile is EAL 3. The following table lists the assurance components which are therefore applicable to this PP.

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Life-Cycle Support	ALC_CMC.3
	ALC_CMS.3
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

Table 6: Assurance Requirements

6.7 Security Assurance Requirement Rationale

The assurance level was taken from [PP-DMT]. Please see [PP-DMT, 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 electronic identity documents are enforced according to [TR-03110-1], [TR-03110-2], [TR-03110-3] and [ICAO_9303] (**FIA_UAU.4, FIA_UAU.5, FIA_UAU.6 and FIA_API.1**):

Function	**Algorithm**	**Key-Length (Bit)**	**SFR**	**Reference**
BAC ChallengeGen	RNG DRG.3	112	(FCS_RNG.1) FCS_CKM.1 / KDF_BAC	[ICAO_9303]#4.3.1
BAC Encryption of Challenge/Response	3DES-CBC IV=0, No Padding	112	FCS_COP.1 /SYM	[ICAO_9303]#4.3.3.1 [ICAO_9303]#9.7.1.2
BAC Key Derivation	SHA1	128	FCS_CKM.1 / KDF_BAC FCS_COP.1 /SHA	[ICAO_9303]#9.7.1.1
BAC Authentication(MAC)	Retail-MAC (DES-CBC) IV=0, Padding Method 2 MAClen=8Bytes	112	FCS_COP.1 / MAC	[ICAO_9303]#4.3.3.2 ISO9797-1 Mode 3
PACE KeyGen (Ephemeral)	RNG DRG.3	256 (brainpool P256r1)	(FCS_RNG.1) FCS_CKM.1 / DH_PACE	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116-2]
PACE Nonce	RNG DRG.3		(FCS_RNG.1)	[TR-03110-2] [ICAO_9303]#4.4
PACE	AES-CBC	~~112~~	FCS_COP.1	[TR-03116-2]

Function	**Algorithm**	**Key-Length (Bit)**	**SFR**	**Reference**
Encryption/ Decryption		128	/SYM	[TR-03110-2] [ICAO_9303]#4.4
PACE KeyAgreement PACE Mapping	ECKA/ECKA-GM(ECDH)	-	FCS_CKM.1 / DH_PACE	- [TR-03110-2] [ICAO_9303]#4.4 [TR-03116-2]
PACE MAC	~~3DES-CBC~~ AES-CMAC	~~112~~ 128	FCS_COP.1 / MAC	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116-2]
PACE Key Derivation	AES-CBC SHA-1	128	FCS_CKM.1 / FCS_CKM.1 /DH_PACE FCS_CKM.1 /KDF_BAC FCS_COP.1 /SHA	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116-2] [TR-03111]#4.3.3.2
TAv2 KeyGen (Ephemeral)	(RNG DRG.3)	256 (brainpoolP256r1)		[TR-03110-2]#3.3 [TR-03116-2]
TAv1/TAv2 Sign	ECDSA-SHA256	~~224~~ 256 (StaticKey: brainpoolP256r1) -	FCS_COP.1 /SHA FIA_API.1	[TR-03116-2] [TR-03110-2]#3.3 [TR-03110-1]#3.5
PKI Passive Authentication (CSCA)	ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512	256 384 512	FCS_COP.1 /SHA FCS_COP.1 /CER	[TR-03116-2] [ICAO_9303]#5.1 [TR-03110-1]#1.1
Passive Authentication Document	ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384	224 256 384	FCS_COP.1 /SHA FCS_COP.1	[TR-03116-2] [ICAO_9303]#5.1 [TR-03110-1]#1.1

Function	Algorithm	Key-Length (Bit)	SFR	Reference
Signer			/CER	
PKI Passive Authentication DG-Hash	~~SHA1~~ SHA256 SHA384	~~160~~ 256 384	FCS_COP.1 /SHA	[TR-03116-2] [ICAO_9303]#5.1 [TR-03110-1]#1.1
PKI Terminal Authentication CVCA	ECDSA-SHA2	~~224~~ 256	FCS_COP.1 /SHA FCS_COP.1 /CER	[TR-03116-2] [TR-03110-1]#3.5 [TR-03110-2]#3.3
CAv1 KeyGen	(ECC: RNG DRG.3)	256 (brainpool P256r1) -	FCS_CKM.1 / DH_CA	[TR-03116-2] [TR-03110-1]#3.4
CAv2 KeyGen (Generated during TAv2)	(ECC: RNG DRG.3)	(From TAv2)	(FCS_CKM. 1/DH_CA)	[TR-03116-2] [TR-03110-2]#3.4
CAv1/CAv2 KeyAgreement	ECKA(ECDH) ~~DH~~	256 -	FCS_CKM.1 / DH_CA	[TR-03116-2] [TR-03110-1]#3.4 [TR-03110-2]#3.4
CAv1 Encryption	3DES-CBC AES-CBC	112 128	FCS_COP.1 /SYM	EUCOM (2006) 2909 [TR-03116-2] [TR-03110-1]#3.4
CAv1 Authentication(MAC)	3DES RetailMAC AES-CMAC	112 128	FCS_COP.1 / MAC	EUCOM (2006) 2909 [TR-03116-2] [TR-03110-1]#3.4
CAv2 Encryption	AES-CBC	~~112~~ 128	FCS_COP.1 /SYM	- [TR-03116-2] [TR-03110-2]#3.4
CAv2 Authentication(MAC)	AES-CMAC	~~112~~ 128	FCS_COP.1 / MAC	[TR-03116-2] [TR-03110-2]#3.4
Firmware	ECDSA	256	FCS_COP.1.	[FIPS186-4]#Kap 6

Function	Algorithm	Key-Length (Bit)	SFR	Reference
Signature Verification		(secp256r1 =NIST P-256), 384 (secp384r1 , NIST P-384)	1/ UpdateSig	
Firmware Signature Hash	SHA256		FCS_COP.1 /SHA	[FIPS180-4]

Table 7: Cryptographic Protocols of the TOE

It should be noted that the aforementioned table is a more detailed version of table 1 from [PP-DMT].

Function	Algorithm	Key-Length	SFR	Reference
SAM-Access/ Authentication PACE	ECKA/ECDH	384 (brainpoolP384r1)	(FCS_COP.1/ MAC)	[TR-03111]
SAM-SecureMessaging	AES-CBC AES-CMAC	128	(FCS_COP.1/ SYM)	AES: [FIPS197] CBC: [SP800-38A] CMAC: [SP800-38B]

Table 8: Cryptographic Protocols with Interface to the TOE

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_RNG.1**), key generation/derivation (**FCS_CKM.1/KDF_BAC, FCS_CKM.1/DH_PACE, FCS_CKM.1/DH_CA, FCS_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/**).

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_UAU.2, FIA_UID.2 FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/TOE-Config, FMT_MTD.1/EnableOpAccKeyStore and FMT_MTD.1/ReadVersion**):

- Modification of configuration data of the TOE
- Update of the pairing between TOE and control software
- Initiate firmware update
- View the version number of the TOE
- Verify date and time

For firmware update the TOE ensures that the update is only performed, if the authenticity of the firmware to be installed could be verified using signature verification (**FCS_COP.1/UpdateSig**).

It further enforces that only Operators with the security attribute SecAttr.AccTerminalPrivateKey are allowed to access the private key used for Terminal Authentication (**FMT_MTD.1/UnlockKeyStore)** and to view the version number of the TOE and verify date and time (**FMT_MTD.1/ReadVersion**).

Revisors are allowed to view the version number of the TOE, verify date and time (**FMT_MTD.1/ReadVersion**) and read TOE log data (**FMT_MTD.1/ReadLog**).

7.3 SF.AUDIT

The TOE generates audit data (**FAU_GEN.1**) which is then stored by the environment. Table 4 lists the events and further audit relevant information that will be logged.

The following information is logged for every event:

- A unique number,
- date and time of the event,
- Type of the event,
- outcome of the event,
- a hash value.

The hash value (SHA-256) ensures the authenticity of the event. It is not only calculated over the current event but also over the hash value of the preceding event. This way, all events in a log file are combined to a list.

After a predefined number of events has been written to an audit file, the TOE will add a signature to the file and start a new audit file.

7.4 SF.PROTECTION

SF.PROTECTION allows the user to detect physical tampering of the base unit (**FPT_PHP.1/BaseUnit)** and provides a trusted communication path between TOE and control software (**FTP_TRP.1/ControlSoftware**).

Detection of physical tampering is realized by a seal that is carried by the base unit. This seal will be broken and therewith indicated physical tampering of the base unit.

The communication between Control Software and TOE is secured by a trusted channel. This trusted channel is implemented as a mutually authenticated TLS 1.2 channel. The TOE supports the following cipher suites:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256

With the following curves[5]:

- prime256v1
- secp384r1
- secp521r1
- brainpoolP256r1
- brainpoolP384r1
- brainpoolP512r1

[5] It should be noted that while the TOE is generally able to support these curves, only the curves prime256v1 and secp384r1 are used as the certificates are issued for these curves.

8 References

The following documentation was used to prepare this ST:

[AIS31] A proposal for: Functionality classes for random number generators, Version 2.0, 18.9.2011

[CC] Common Criteria for Information Technology Security Evaluation –

Part 1: Introduction and general model,
dated April 2017, version 3.1, R5

Part 2: Security functional requirements,
dated April 2017, version 3.1, R5

Part 3: Security assurance requirements,
dated April 2017, version 3.1, R5

[CEM] Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated April 2017, version 3.1, R5

[PP-DMT] Common Criteria Protection Profile for Document Management Terminal, BSI-CC-PP-0064-V2-2018

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents - Part 11: Security Mechanisms for MRTDs, ICAO, 7th edition, September 2015

[ICAO_PKI] ICAO Doc 9303, Machine Readable Travel Documents – Part 12, Public Key Infrastructure for Machine Readable Travel Documents for MRTDs, ICOA 7th edition, September 2015.

[FIPS180-4] FIPS 180-4; FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015.

[TR-03110-1] BSI TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, Part 1: eMRTDs with BAC/PACEv2 and EACv1 - Version 2.20, 2015

[TR-03110-2] BSI TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, Part 2: Protocols for electronic IDentification, Authentication and Trust Services (eIDAS) - Version 2.21, 2016

[TR-03110-3] BSI TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, Part 3: Common Specifications - Version 2.21, 2016

[TR-03111] BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, Juni 2018

[TR-03116-2] BSI TR-03116-2: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2: Hoheitliche Ausweisdokumente, Stand Februar 2019

[FIPS186-2] FIPS 186-2 – Digital Signature Standard (DSS), National Institute of Standards and Technology, 27.01.2000

[FIPS186-4] FIPS 186-4 – Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013

[FIPS197] FIPS PUB 197 – Announcing the ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, November 2001

[SP800-38A] Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology, December 2001

[SP800-38B] Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, National Institute of Standards and Technology, May 2005

9 Glossary and Abbreviations

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 ELECTRONIC IDENTITY DOCUMENT and its data elements on the electronic identity document's chip were created by the issuing State or Organization
Basic Access Control (BAC)	Security mechanism defined in [ICAO_9303] by which means the electronic identity document'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 electronic identity document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical electronic identity document.
Biographical data (biodata).	The personalized details of the electronic identity document 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 electronic identity document holder in the electronic identity document'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).

Term	Definition
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]
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 electronic identity document.
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 electronic identity document'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.

Term	Definition
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 electronic identity document'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 electronic identity document in the limits provided by the issuing States or Organizations
Eavesdropper	A threat agent with Enhanced-Basic attack potential reading the communication between the electronic identity document's chip and the inspection system to gain the data on the electronic identity document'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).*
eRA	Look at the term *Machine readable travel document (MRTD).*
Extended Access Control	Security mechanism identified in [ICAO_9303] by means of which the electronic identity document'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 electronic identity document 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.

Term	Definition
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 electronic identity documents. [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.
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 electronic identity document material during the IC manufacturing and the delivery process to the electronic identity document manufacturer.

Term	Definition
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 electronic identity document presented to it by a traveller (the electronic identity document 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 electronic identity document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as electronic identity document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The electronic identity document's chip is an integrated circuit.
Integrity	Ability to confirm that the electronic identity document and its data elements on the electronic identity document'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 electronic identity document. [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 electronic identity document's chip.

Term	Definition
Logical electronic identity document	Data of the electronic identity document 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 electronic identity document 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]

Term	Definition
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the electronic identity document or MRP Data Page or, in the case of the TD1, the back of the electronic identity document, 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]
electronic identity document application	Non-executable data defining the functionality of the operating system on the IC as the electronic identity document'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.
electronic identity document Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the electronic identity document's chip based on MRZ information as key seed and access condition to data stored on electronic identity document's chip according to LDS.
electronic identity document holder	The rightful holder of the electronic identity document for whom the issuing State or Organization personalized the electronic identity document.
electronic identity document'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].
electronic identity document's chip Embedded Software	Software embedded in an electronic identity document's chip and not being developed by the IC Designer. The electronic identity document's chip Embedded Software is designed in Phase 1 and embedded into the electronic identity document's chip in Phase 2 of the TOE life-cycle.
MRZ	Machine Readable Zone (on an electronic identity document)

Term	Definition
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 electronic identity document holder in the electronic identity document'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.
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 electronic identity document or parts of it via the contact-less communication channel of the TOE without knowledge of the printed MRZ data.

Term	Definition
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]
Traveler	Person presenting the electronic identity document to the inspection system and claiming the identity of the electronic identity document 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 electronic identity document	The electronic identity document that contains the electronic identity document 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 enrolee whose identity is being claimed, to determine whether it matches the enrolee’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
CAN	Card Access Number
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
MRZ	Machine Readable Zone
nPA	Neuer Personalausweis
OS	Operating System
OSP	Organisational Security Policy
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
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