Federal Office
for Information Security

Common Criteria Protection Profile for Document Management Terminal DMT-PP

BSI-CC-PP-0064-V2-2018

Version 2.0

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 PP Introduction 5
1.1 PP Reference 5
1.2 Terminology 5
1.3 TOE Overview 5
1.3.1 Major security features of a TOE 7
1.3.2 TOE Type 7
1.3.3 Required non-TOE hardware/software 7
1.3.4 Location of input or output-devices 8
1.3.5 Protocol overview 9
2 Conformance Claim 10
2.1 CC Conformance Claim 10
2.2 PP Claim 10
2.3 Package Claim 10
2.4 Conformance Claim Rationale 10
2.5 Conformance Statement 10
3 Security Problem Definition 11
3.1 TOE security policy 11
3.1.1 Subjects 11
3.1.2 Objects 11
3.2 Assets 12
3.3 Security Attributes 14
3.4 Threats 14
3.5 Assumptions 15
3.6 Organizational Security Policies (OSP) 16
4 Security Objectives 20
4.1 Security Objectives for the TOE 20
4.2 Security Objectives for the Operational Environment 22
4.3 Security Objectives Rationale 25
4.3.1 Threats and objectives 25
4.3.2 Assumptions 27
4.3.3 Organizational Security Policies 27
5 Extended Component Definitions 30
5.1 Family: Generation of random numbers (FCS_RNG) 30
5.2 Family: Authentication Proof of Identity (FIA_API) 31
6 Security Requirements 32
6.1 Security functional requirements 32
6.1.1 Class FAU - Logging 32
6.1.2 Class FCS - Cryptographic Protocols 33
6.1.3 Class FDP – User Data Protection 37
6.1.4 Class FIA – Identification and Authentication 37
6.1.5 Class FMT – Security Management 39
6.1.6 Class FPT - TSF physical protection 41
6.1.7 Class FTP - Trusted Paths 42

6.2 Security Assurance Requirements ... 42
6.3 Security Requirements Rationale ... 42
6.3.1 Security Functional Requirements Rationale ... 42
6.3.2 Security Functional Requirements Dependency Rationale ... 45
6.3.3 Security Assurance Requirements Rationale ... 47
6.3.4 Security Requirements – Mutual Support and Internal Consistency ... 47
A PP-Module – User Interface Unit DMT-PP-UIU ... 49
A.1 PP-Module introduction ... 49
A.1.1 PP-Module reference ... 49
A.1.2 Base-PP identification ... 49
A.1.3 TOE overview ... 49
A.2 Consistency Rationale ... 49
A.3 Conformance Claim ... 50
A.3.1 CC Conformance Claim ... 50
A.3.2 Conformance Statement ... 50
A.4 Security Problem Definition ... 50
A.5 Security Objectives ... 50
A.5.1 Security Objectives for the TOE ... 50
A.5.2 Security Objectives for the Operational Environment ... 51
A.5.3 Security Objectives Rationale ... 51
A.6 Security Functional Requirements ... 52
A.6.1 Class FPT - Tamper Resistance ... 52
A.6.2 Class FTP - Trusted Paths ... 52
A.6.3 Security Functional Requirements Rationale ... 53
A.6.4 Security Functional Requirements Dependency Rationale ... 53
B PP-Configuration DMT-with-UIU ... 54
B.1 PP-Configuration reference ... 54
B.2 Components statements ... 54
B.3 Conformance statement ... 54
B.4 Security Assurance Requirements (SAR) statement ... 54
C Appendix ... 55
C.1 Glossary ... 55
C.2 Acronyms ... 57
Reference Documentation ... 58

Figures

Figure 1: General overview of the TOE and the related components ... 6
Figure 2: State diagram for Terminal Authentication keys ... 18

Tables

Table 1: Overview of the protocols to be supported by the TOE ... 9
Table 2: Security Objectives Rationale ... 25
Table 3: Coverage of Security Objectives for the TOE by SFRs ... 43
Table 4: Dependencies between the SFR for the TOE ... 47
Table 5: Security Objectives Rationale – Package DMT-PP-UIU ... 51
Table 6: Coverage of Security Objectives for the TOE by SFRs – Package DMT-PP-UIU ... 53

1 PP Introduction

1.1 PP Reference

Title:	Common Criteria Protection Profile – Document Management Terminal
Abbreviation:	DMT-PP
CC version:	v3.1 release 5
PP version:	2.0
Authors:	Federal Office for Information Security
Publication Date:	6th June 2018
Keywords:	ICAO, inspection system, machine readable travel document, extended access control
Registration:	BSI-CC-PP-0064-V2-2018

1.2 Terminology

Electronic Identity Document

The term “Electronic Identity Document” denotes a document which allows the owner of the document to prove their identity and which supports cryptographic mechanisms to check the integrity and authenticity of the document, as well as restricting access to all or some of the stored data to authenticated terminals. In general, this will be an eMRTD (electronic Machine Readable Travel Document) compliant to [ICAO 9303] and [TR-03110-1], or an eID Card (e.g. national identity card or a residence permit) compliant to [TR-03110-2].

Chip data

The term chip data denotes any electronic data which is stored on the chip of an electronic identity document.

Document Management Terminal

The Document Management Terminal is a device which is used to read or update data stored in electronic identity documents. It includes the document application, which is the actual TOE of this PP, as well as several interfaces, input/output-devices and storage components, which are required for the operability of the device. The device could be operated by the issuing authority as part of the issuance and change management process for Electronic Identity Documents for example.

A more detailed description is given in section 1.3.

1.3 TOE Overview

The Target of Evaluation (TOE) addressed by this Protection Profile (PP) is an application, and its interfaces which are part of a Document Management Terminal. The TOE is used to read, and where applicable update, the electronic data of an electronic identity document and verify its integrity and authenticity. In the following this application is called “document application”.

In order to get access to the chip data the TOE must be able to perform several cryptographic protocols. An overview of these protocols is given in section 1.3.5.

The Document Management Terminal regarded in this PP is operated by governmental organisations, e.g. municipal office, police, government or other state approved agencies.

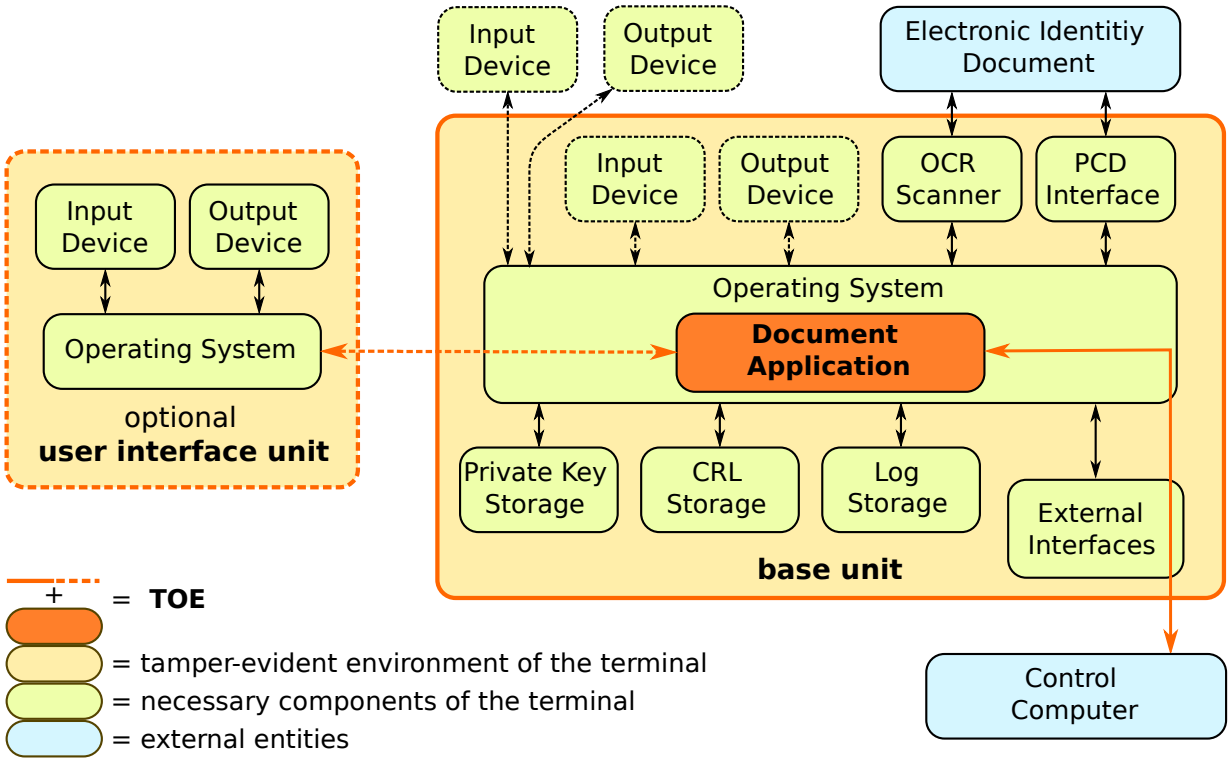


Figure 1: General overview of the TOE and the related components (Dashed lines indicate optional components)

Usage and major security features of a Document Management Terminal are described in section 1.3.1. Document Management Terminals can have different configurations. The TOE is the main item of a Document Management Terminal, but there are several additional components necessary to get a fully functional device. For this reason, a description of the required and optional non-TOE hardware/software is given in section 1.3.3.

A general overview of the TOE and its related components is given in Figure 1.

Figure 1 shows the components necessary for a Document Management Terminal as regarded in this PP. The document application shall be the Target of Evaluation (TOE) and is marked red. The connection of the document application to the control software is also part of the TOE and is also marked red. Furthermore, the enclosure of the Document Management Terminal, which provides a tamper-evident environment to the document application and additional components is subject of the evaluation, which is depicted by the red frames and that provides the capability to determine whether physical tampering of the enclosure has occurred.

The operating system as base of the document application, the input and output devices, the key and certificate/CRL storages, the logfile storage and the PCD (Proximity Coupling Device, see also chap. 1.2.2) are marked light-green as being not part of the TOE but necessary for the functionality of the Document Management Terminal.

For each input or output-device there are different options for implementing them, which is indicated by dashed lines in Figure 1. These options are described in section 1.3.4, respectively.

1.3.1 Major security features of the TOE

There are two main security features for the TOE. The first is the protection of sensitive personal data read from or written to the electronic identity document right from the beginning of the reading/writing process as long as the data are in the scope of the TOE.

The document chip defines how sensitive the different chip data are. The TOE is not required to protect the data on a higher level than the chip itself does.

The other main security feature is the correct execution of the access control protocols listed in section 1.3.5. For this purpose the correct implementation and the generation of strong random numbers, as well as the reliable connection to the storages needed for Passive Authentication and Terminal Authentication is important.

In addition, the TOE provides protection against manipulations of the TOE application itself, as well as the components required for the TOE operation.

1.3.2 TOE Type

First of all, the TOE is a software which is capable of reading or updating electronic identity documents. The electronic identity documents have protected data and have to prove their authenticity and integrity by the protocols defined in [ICAO 9303], [TR-03110-1] and/or [TR-03110-2] to the TOE.

Furthermore, the TOE includes a tamper-evident environment that protects the software of the TOE itself as well as the required components for the operation of the TOE listed in section 1.3.3. In- or output-devices may be situated outside of the tamper-evident environment under conditions described in section 1.3.4.

1.3.3 Required non-TOE hardware/software

In order to read out or update the personal data from the electronic identity document's chip and to verify its authenticity and integrity the following components are necessary additionally to the document application:

1. The document application is running on an **operating system**.
2. The **PCD (Proximity Coupling Device)** is featured with a RF (Radio Frequency) reading module and an antenna. It is used for the wireless communication with the electronic identity document's chip in order to establish a connection based on the [ISO/IEC 14443] and [ISO/IEC 7816] protocols.
3. Most types of electronic identity documents demand some kind of password to get access to the electronic identity document's chip. Therefore, an **input device** is necessary to record these passwords. It is conditional to the business case of the Document Management Terminal which type of input devices are needed:
    1. *OCR Reader:* In case of an ICAO compliant electronic identity document this “password” is one part of the MRZ (Machine Readable Zone) and it can be read with an OCR-Reader (Optical Character Recognition).
    2. *Keyboard*: With consideration of the electronic identity documents where the password is not meant to be read optically like the Card Access Number (CAN) or cases in which the MRZ, etc. is difficult to be read due to a damaged or polluted document, an input device should be usable to type in a password. Furthermore, a kind of keyboard etc. is needed when personal chip data (e.g. the address) shall be updated.
    3. *Cameras or Scanners*: The Input device may provide also capturing features for biometric attributes like fingerprint or images of the electronic identity document holder's face[1].
4. In order to communicate information about the authenticity and integrity of the electronic identity document and the chip data to the Document Management Terminal user[2] at least one **output device** is needed. The Document Management Terminal can provide more than one output device, e.g. one for the

1 Advanced matching mechanisms between the biometric information captured from the electronic identity document holders and the respective information stored at the electronic identity document are not addressed by this document.

2 This could be the border control officer, the employee of a local municipal office or any other person who is authorised to operate the Document Management Terminal.

operator and one for the document presenter. Hereby, the document owner can enter his current document PIN or enter a new one to update the document PIN.

5. The **private key storage** contains the private key of the Document Management Terminal used for Terminal Authentication in the context of EAC and is a device certified according to minimum common criteria assurance package EAL4, augmented with at least AVA_VAN.5.
6. The **certificate and CRL (Certificate Revocation List) storages** contain the CSCA-Certificates and the corresponding CRLs needed for Passive Authentication and may also contain the corresponding DS-Certificates. The certificate chain needed for Terminal Authentication may be stored in the same storage or in a different one.
7. The **logfile storage** contains the logfile written by the TOE for revision purposes. There shall be a logfile to retrace the changes in the TOE's configuration made by the administrator.

1.3.4 Location of input or output-devices

A Document Management Terminal may implement input or output-device in three different ways, that are described in the following. The option used may be different for each input or output-device.

1. An input or output-device may be implemented inside the tamper-evident enclosure of the base unit that houses the document application.
2. An input or output-device may be located outside the tamper-evident enclosure of the base unit that houses the document application, if it is directly connected to the base unit by a wired connection and if the device does not run its own operating system.
3. One or more input or output-device may be implemented in an external user interface unit running a dedicated operation system that can be detached from the base unit that hosts the document application. However, the third option is not covered by the Base-PP itself but by the PP-Module DMT-PP-UIU instead.

Note: *Wireless connection between an input or output-device and the base unit are not directly allowed. However, an input or output-device may be implemented inside an external user interface according to option 3, which in turn may be connected wireless to the base-unit.*

1.3.5 Protocol overview

The following table provides an overview of the protocols that have to be supported by the TOE in order to communicate with the chip of an electronic identity document.

protocol name	specified in	keys/certificates/randoms needed by the IS	use case
BAC	[ICAO 9303], Part 11	rnd_{BAC} = random nonce created by the terminal K_{BAC} = random key created by the terminal	confidentiality of the submitted chip data, authentication & secure channels Is provided by the TOE
PACE	[ICAO 9303], Part 11 for eMRTDs [TR-03110-2] for eIDs	$\widetilde{PK_{PACE}}$ = ephemeral public key of the terminal $\widetilde{SK_{PACE}}$ = ephemeral private key of the terminal	confidentiality of the submitted chip data, authentication & secure channels Is provided by the TOE
Chip Authentication	CAv1: [TR-03110-1] CAv2 & CAv3: [TR-03110-2]	$\widetilde{PK_{CA}}$ = ephemeral public key of the terminal $\widetilde{SK_{CA}}$ = ephemeral private key of the terminal	originality of the electronic identity document chip, secure channels, confidentiality of the submitted chip data Is provided by the TOE
Passive Authentication	[ICAO 9303], Part 11 and [TR-03110-1]	CSCA-Certificates and CRLs of the issuing states of the documents to be read	authenticity and integrity of the chip data Is provided by the TOE
Terminal Authentication	TAv1: [TR-03110-1] TAv2: [TR-03110-2]	PK_{PCD} = public key of the terminal SK_{PCD} = private key of the terminal C_{DV} = Document Verifier Certificate(s) C_V = Terminal Certificate	authenticity and authorisation of the terminal Private key storage and signing operation is provided by the private key storage

Table 1: Overview of the protocols to be supported by the TOE

2 Conformance Claim

2.1 CC Conformance Claim

This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [CC 1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [CC 2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [CC 3]

as follows

– Part 2 extended,

– Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [CEM]

has to be taken into account.

2.2 PP Claim

This PP does not claim conformance to any another Protection Profiles.

2.3 Package Claim

This PP is conforming to assurance package EAL3 as defined in CC part 3 [CC 3].

2.4 Conformance Claim Rationale

Because there is no conformance claim to a Protection Profile, a rationale is not applicable.

2.5 Conformance Statement

The Document Management Terminal may implement an external user interface unit running a dedicated operation system that can be detached from the base unit. To claim conformance to this Protection Profile, the conforming Security Target or Protection Profile shall comply with one of the following two rules:

1. If **no** user interface unit is implemented the Security Target or Protection Profile shall claim for “strict” conformance to version 2.0 of the Base-PP DMT-PP.
2. If **at least one** user interface unit is implemented the Security Target or Protection Profile shall claim for “strict” conformance to version 2.0 of the PP-Configuration DMT-with-UIU.

   Note: *The PP-Configuration consists of version 2.0 of the Base-PP DMT-PP and version 2.0 of the PP-module DMT-PP-UIU (DMT-PP Module – User Interface Unit).*

3 Security Problem Definition

3.1 TOE security policy

3.1.1 Subjects

Operator (S1)

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

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).

Revisor (S3)

The revisor is a person who is able to access the Document Management Terminal on a dedicated service interface to inspect the log files of the TOE.

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.

Electronic identity document holder (S5)

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

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

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.

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 storage is protected by further security measures to enforce the protection needs of the Document Management Terminal's key pair.

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.

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.

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.

Input device (O6)

The input device shall provide necessary input data to the TOE. For a Document Management Terminal input devices may be e.g. an OCR reading device to scan the MRZ information, a keyboard to provide the MRZ and further information to the TOE or biometric input devices (e.g. camera, finger print scanner).

Output device (O7)

The output device delivers results of the inspection process as well as further information obtained during the process to the user of the TOE (S1, S2 and/or S5). One example for an output device is a monitor but also a traffic light display indicating the results of the Document Management Terminal may be possible.

Control software (O8)

The control software is a software component that is executed on an external computer 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.

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), as well as a user interface unit, if existent.

3.2 Assets

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

R.ChipData

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

Required Protection: integrity, confidentiality

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 according to [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

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

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

R.TerminalPrivateKey

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

Required Protection: integrity, confidentiality

R.SessionKeys

R.SessionKeys are any non-static session and ephemeral keys that are needed by the TOE to perform the protocols in section 1.3.5.

Required Protection: integrity, confidentiality

R.RandomNumbers

R.RandomNumbers are those random numbers needed by the TOE to perform the protocols in section 1.3.5.

Required Protection: integrity

R.Certificates

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

Required Protection: integrity

R.CRL

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

Required Protection: integrity

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

R.PairingData

The pairing data is used to configure a secure connection between the Document Application (O9) and an external user interface unit in order to establish a one-to-one relationship between the TOE and the user interface unit. R.PairingData is also used to establish a secure connection between the TOE and the control software (O8). These secure connections ensure authenticity and confidentiality of the transferred data.

Required Protection: integrity, confidentiality

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

R.SensitiveInputData

All further input data besides R.ChipPassword and R.PersonalChipPassword received from a input interface (II) are considered as R.SensitiveInputData.

Required Protection: integrity, confidentiality

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

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.

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

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

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

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

T.Eavesdropping - Eavesdropping of sensitive chip data

Adverse action: An attacker (S6) eavesdrops chip data (R.ChipData) or input data (R.PersonalChipPassword, R.SensitiveInputData) 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

T.TerminalManipulation – Manipulation of the terminal hardware

Adverse action: An attacker (S6) tries to manipulate hardware components of the Document Management Terminal, e.g. input (O6) or output (O7) devices. 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

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.

Asset: R.ChipData, R.AuthenticDocumentData

3.5 Assumptions

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 1.3.3) 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.

A.SecureComponents

It is assumed that the components in the TOE environment that are required for the operation of the Document Management Terminal (c.f. section 1.3.3) 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.).

A.TrainedUser

It is assumed that the authorised users of the TOE, Operators (S1), Administrators (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.

A.ValidKeyAndCertificateData

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

A.PKI

It is assumed that the environment provides a public key infrastructure for EAC and Passive Authentication.

3.6 Organizational Security Policies (OSP)

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 Management 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.

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. 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.

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.

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 and time is correct.

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).

Application note 1: *This distance is to be defined in the Security Target of the individual TOE depending on its operation purpose. Alternatively, measures which restrict the visibility of the in- and output devices to the Operator (S1) have to be defined.*

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 sufficient 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).

Application note 2: *This distance is to be defined in the Security Target of the individual TOE depending on its operation purpose. Alternatively, the measures which restrict the visibility of the in- and output devices to the electronic identity document holder (S5) have to be defined.*

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 (O2) is a device certified according to common criteria assurance package EAL4+ or higher, whereby augmentation results from AVA_VAN.5.

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).

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 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.

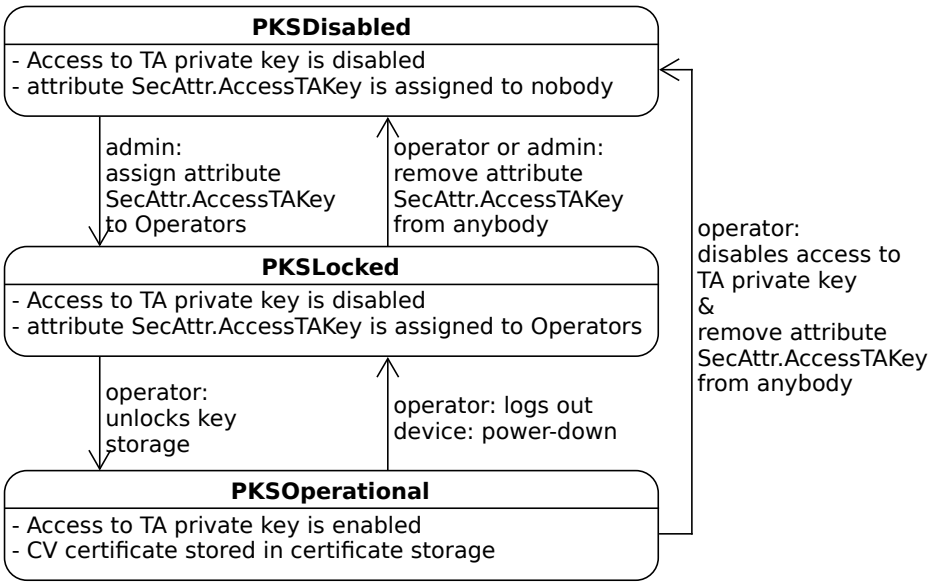


Figure 2: State diagram for Terminal Authentication keys

  - Attribue 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.

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 their 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.

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 an external user interface unit or 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).

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

4.1 Security Objectives for the TOE

OT.PrivilegedRoleAuthorization

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 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. 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.*

OT.OperatorAuthorization

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 (S2) 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.*

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.

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).

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.

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).

OT.Protocols

The TOE shall implement the:

1. Basic Access Control (BAC) protocol according to the specifications [ICAO 9303], Part 11, Sect. 4.3 (Basic Access Control)
2. Password Authenticated Connection Establishment (PACE) protocol according to [ICAO 9303], Part 11, 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).*

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.

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.

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

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.

OE.SecureBoot

The components in the TOE environment that are required for the operation of the Document Management Terminal (c.f. section 1.3.3) 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.*

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 Inspection System 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 implementedby 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).

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 neither the TOE installation itself nor the assets secured by the TOE and the TOE environment.

OE.ValidKeyAndCertificateData

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

OE.PKI

The environment must provide public key infrastructures for EAC and Passive Authentication according to the specifications in [ICAO 9303], [TR-03110-1] and/or [TR-03110-2] depending on the used protocols.

Each PKI environment must provide a certificate policy.

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.

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.

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. Additionally, if the Document Management Terminal implements an external user interface unit according to PP-Module DMT-PP-UIU, the Operator (S1) shall perform the same checks for that unit and shall also check the pairing between that unit and the base unit.

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

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.

OE.ChipPassword

The environment must enable the Operator (S1) or the Electronic identity document holder (S5) 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, either special distance between the Document Management Terminal and any other person shall be enforced. Alternatively, measures which restrict the visibility of the in- and output devices to the Operator (S1) or the Electronic identity document holder (S5) have to be defined. These measures may be different for the different types of passwords.

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.
  - 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 their 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.

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

	OT.PrivilegedRoleAuthorization	OT.OperatorAuthorization	OT.DisplayVersion	OT.LogData	OT.VerifySoftwareUpdateSignature	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 2: Security Objectives Rationale

4.3.1 Threats and objectives

T.AcceptForgedIdentity

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

- **OT.PrivilegedRoleAuthorization** 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).

- **OT.Protocols** makes sure that the TOE uses the specified cryptographic protocols to verify the authenticity of data provided by an electronic identity document.
- **OE.SignedCertsAndCRLs** makes sure that only legitimate public keys are accepted for the verification of signatures or certificates provided by an electronic identity document (O1) and/or used by the TOE.
- **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.*

T.MaliciousDataUpdate

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

- **OT.OperatorAuthorization** and **OE.AuthenticationMeans** makes sure that only authorized 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.

T.DataCompromise

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

- **OT.OperatorAuthorization** and **OE.AuthenticationMeans** makes 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.

T.FakedLogFileEntries

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

- **OT.PrivilegedRoleAuthorization** and **OE.AuthenticationMeans** makes 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** make sure that the log files (R.LogData) are not manipulated during their storage in the logfile storage (O4).

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.

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).

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

A.SecureBoot

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

A.SecureComponents

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

A.TrainedUser

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

A.ValidKeyAndCertificateData

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

A.PKI

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

4.3.3 Organizational Security Policies

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.

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.

OSP.Date

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

OSP.ChipPassword

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

OSP.PersonalChipPassword

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

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.

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.

OSP.RNG

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

OSP.Logging

The policy is enforced by the following combination of objectives:

- **OT.LogData** enforce 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 Definitions

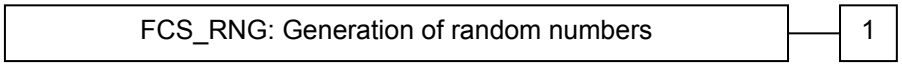
5.1 Family: Generation of random numbers (FCS_RNG)

This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behaviour:

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

Component levelling:



Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1	Generation of random numbers
	Hierarchical to: No other components.
	Dependencies: No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers*]] that meet [assignment: *a defined quality metric*].

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.*

5.2 Family: Authentication Proof of Identity (FIA_API)

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

Application note 11: *Other families of the class FIA describe only the authentication verification 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.*

Family behaviour:

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

Component levelling:

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1	Authentication Proof of Identity	
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorized user or role*].	

6 Security Requirements

This part defines detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE must satisfy in order to meet the security objectives for the TOE.

Common Criteria allows several operations to be performed on security requirements on the component level: refinement, selection, assignment and iteration, cf. sec. 8.1 of [CC 1]. Each of these operations is used in this PP.

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are underlined and removed words are ~~crossed out~~.

The selection operation is used to select one or more options provided by CC in stating a requirement. Selections that have been made by the PP author are denoted as underlined. Selections to be filled in by the ST author appear in square brackets with an indication that a selection has to be made, [selection: *choose from these options*], and are *italicised*. In some cases the selection made by the PP authors defines a assignment to be performed by the ST author. Then this text is *underlined and italic*.

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 author are denoted as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment has to be made [assignment: *choose your assignment*], and are *italicized*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Then this text is *underlined and italic*.

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.

6.1 Security functional requirements

6.1.1 Class FAU - Logging

FAU_GEN.1	Audit data generation
	Hierarchical to: No other components.
	Dependencies: FPT_STM.1 Reliable time stamps
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 [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) every modification 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) [assignment: *other specifically defined auditable events*][3].

3 [assignment: *other specifically defined auditable events*]

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, [assignment: *other audit relevant information*].

Refinement: The TSF supports the storage of audit records by the TOE environment (cf. OE.SecureComponents) by providing 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).*

6.1.2 Class FCS - Cryptographic Protocols

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[4] and specified cryptographic key sizes 112 bit[5] that meet the following: [selection: *[[ICAO 9303], Part 11, Sect. 4.3 (Basic Access Control), [assignment: list of standards]*][6].

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 Document Management Terminal 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.*

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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm password authenticated Diffie-Hellman key agreement[7] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the

4 [assignment: *cryptographic key generation algorithm*]
5 [assignment: *cryptographic key sizes*]
6 [assignment: *list of standards*]
7 [assignment: *cryptographic key generation algorithm*]

following: [selection: *[[ICAO 9303], Part 11, Sec 4.4 (PACE)], [[TR-03110-2], Sec. 3.2 (PACE)], [assignment: list of standards]*][8].

Application note 14: *The ST writer shall perform the open operation in the element FCS_CKM.1.1/DH_PACE. 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. [ICAO 9303], Part 11, Sec 4.4 (PACE) or [TR-03110-2], Sec. 3.2 (PACE) describes the key agreement protocol for PACE. [ICAO 9303], Part 11, Sec 4.4.3 or [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 [ICAO 9303], Part 11, Sec 9.7.4 (Secure Messaging Keys) or [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

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [selection: [*[TR-03110-1] Sec. 3.4 (Chip Authentication Version 1)], [[TR-03110-2], Sec. 3.4 (Chip Authentication Version 2)], [assignment: list of standards]*][9].

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) or [[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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method physical deletion by overwriting the memory data with other values or the new key[10] that meets the following: none[11].

Refinement: The TOE shall destroy the BAC session keys and PACE session keys
(i) after detection of an error in a received command by verification of the MAC, or
(ii) after successful run of the Chip Authentication protocol.
The TOE shall destroy the chip session keys as well as the Chip Authentication ephemeral key pair after detection of an error in a received command by verification of the MAC.
The TOE shall clear the memory area of any session keys as well as ephemeral keys after ending a session and therefore before starting the communication with the electronic identity document in a new session.

8 [assignment: *list of standards*]
9 [assignment: *list of standards*]
10 [assignment: *cryptographic key destruction method*]
11 [assignment: *list of standards*]

FCS_COP.1/SHA	Cryptographic operation - Hash

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform hashing[12] in accordance with a specified cryptographic algorithm SHA-1, SHA-256 and [assignment: other approved algorithms][13] and cryptographic key sizes none[14] that meet the following: [selection: *FIPS 180-2, [assignment: list of standards]*][15].

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)).*

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform secure messaging – encryption and decryption[16] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [selection: [*[ICAO 9303], Part 11, Sec 9.8 (Secure Messaging)], [[TR-03110-3], Sec. F (Secure Messaging)], [assignment: list of standards]*][17].

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

12 [assignment: *list of cryptographic operations*]
13 [assignment: *cryptographic algorithm*]
14 [assignment: *cryptographic key sizes*]
15 [assignment: *list of standards*]
16 [assignment: *list of cryptographic operations*]
17 [assignment: *list of standards*]

FCS_COP.1.1 The TSF shall perform secure messaging – message authentication code[18] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [selection: [*[ICAO 9303], Part 11, Sec 9.8 (Secure Messaging)], [[TR-03110-3], Sec. F (Secure Messaging)], [assignment: list of standards]*][19].

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.*

FCS_COP.1/CER	Cryptographic operation – Signature Check

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform signature check using CRLs and the whole certificate chain[20] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

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], Part 11, 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.*

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform digital signature verification of software update[21] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

FCS_RNG.1	Generation of random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

18 [assignment: *list of cryptographic operations*]
19 [assignment: *list of standards*]
20 [assignment: *list of cryptographic operations*]
21 [assignment: list of cryptographic operations]

FCS_RNG.1.2 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: *format of the numbers*]] that meet [assignment: *a defined quality metric*].

6.1.3 Class FDP – User Data Protection

FDP_RIP.1	Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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[22] the following objects: chip password (R.ChipPassword), personal chip password (R.PersonalChipPassword), personal chip data (R.ChipData), sensitive input Data (R.SensitiveInputData)[23].

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

6.1.4 Class FIA – Identification and Authentication

FIA_API.1	Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a Terminal Authentication protocol according to[selection: [*[TR-03110-1] Sec. 3.5 (Terminal Authentication Version 1), [[TR-03110-2], Sec. 3.3 (Terminal Authentication Version 2)]*][24] to prove the identity of the TOE[25].

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 to implement that operation itself but shall rely on the private key storage for the signing operation (c.f. OE.SecureComponents).*

FIA_UAU.1	Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

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

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).

22 [selection: *allocation of the resource to, deallocation of the resource from*]
23 [assignment: *list of objects*]
24 [assignment: *authentication mechanism*]
25 [assignment: *authorized user or role*]

Application note 23: *The ST author may specify actions, which are allowed before authentication, however any management function listed in FMT_SMF.1 must not be on the list, since authentication is required for these activities. If the list is empty, FIA_UAU.2 shall be used in the ST instead.*

FIA_UAU.4	Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to
a) Basic Access Control authentication mechanism;
b) Password Authenticated Connection Establishment[26].

Application note 24: *The Basic Access Control authentication mechanism ([ICAO 9303], Part 11, Sect. 4.3 (Basic Access Control)) and the Password Authenticated Connection Establishment ([ICAO 9303], Part 11, Sec 4.4 (PACE) or [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

Hierarchical to: No other components.

Dependencies: No dependencies.

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[27]
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 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[28].

Application note 25: *Basic Access Control mechanism or the Password Authenticated Connection Establishment authentication mechanism include the secure messaging for all commands and response codes*

26 [assignment: *identified authentication mechanism(s)*]
27 [assignment: *list of multiple authentication mechanisms*]
28 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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[29].

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.1	Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

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

6.1.5 Class FMT – Security Management

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to modify[30] the
1) TOE configuration data (Modify R.ConfigurationData)
2) Pairing between the TOE and the control software (Modify R.PairingData)

29 [assignment: *list of conditions under which re-authentication is required*]
30 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

3) the further TSF data: [assignment: list of TSF data][31]
to Administrators (S2)[32].

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to assign[33] the
security attribute SecAttr.AccTerminalPrivateKey to Operators (S1)[34]
to Administrators (S2)[35].

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to enable[36] the
access to or usage (generation, renewal and signing operation) of any terminal private key (R.TerminalPrivateKey) stored in the private key storage (O2)[37]
to Operators (S1) with the security attribute SecAttr.AccTerminalPrivateKey[38].

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to query[39] the TOE log data (R.LogData)[40] to Revisors (S3)[41].

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to query[42] the TOE version and further TSF data: [assignment: *list of TSF data*][43] to Operators (S1), Administrators (S2) and Revisors (S3)[44].

FMT_SMF.1	Specification of Management Functions

Hierarchical to: No other components.

31 [assignment: *list of TSF data*]
32 [assignment: *the authorised identified roles*]
33 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
34 [assignment: *list of TSF data*]
35 [assignment: *the authorised identified roles*]
36 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
37 [assignment: *list of TSF data*]
38 [assignment: *the authorised identified roles*]
39 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
40 [assignment: *list of TSF data*]
41 [assignment: *the authorised identified roles*]
42 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
43 [assignment: *list of TSF data*]
44 [assignment: *the authorised identified roles*]

Dependencies: No dependencies.

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 27)
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) [assignment: *list of further management functions to be provided by the TSF*][45].

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles Operators (S1), Administrators (S2), Revisors (S3) and [assignment: the authorised identified roles][46].

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

6.1.6 Class FPT - TSF physical protection

FPT_PHP.1/BaseUnit	Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 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 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.*

6.1.7 Class FTP - Trusted Paths

FTP_TRP.1/ControlSoftware	Trusted path – Control Software

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and local[47] ~~users~~ control software (O8) that is logically distinct from other communication paths and provides

45 [assignment: *list of management functions to be provided by the TSF*]
46 [assignment: *the authorised identified roles*]
47 [selection: *remote, local*]

assured identification of its end points and protection of the communicated data from modification, disclosure, [assignment: *other types of integrity or confidentiality violation*][48].

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users*][49] to initiate communication via the trusted path.

FTP_TRP.1.3 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
[assignment: *other services for which trusted path is required*][50].

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).*

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.*

6.2 Security Assurance Requirements

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

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage as well as evidence for sufficiency and necessity of the SFRs chosen:

48 [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
49 [selection: *the TSF, local users, remote users*]
50 [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

	OT.PrivilegedRole Authorization	OT.Operator Authorization	OT.DisplayVersion	OT.LogData	OT.VerifySoftware UpdateSignature	OT.Deletion EphemeralData	OT.Protocols	OT.Tamper Evidence	OT.ControlSoftware SecureComm	OT.Random NumberGenerator
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.4 Single-use authentication mechanisms							X			
FIA_UAU.5 Multiple authentication mechanisms							X			
FIA_UAU.6 - Re-authenticating							X			
FIA_UID.1 - Timing of Identification	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									
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/ControlSoftware									X	

Table 3: Coverage of Security Objectives for the TOE by SFRs

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

OT.PrivilegedRoleAuthorization

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

- **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.1** makes sure that any user must be authenticated to the TOE before performing any of the actions listed in FMT_SMF.1.
- **FIA_UID.1** makes sure that users can be identified as Administrators (S2) or Revisors (S3) by the TOE.

OT.OperatorAuthorization

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

- **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.1** makes sure that any user must be authenticated to the TOE before performing any actions.
- **FIA_UID.1** makes sure that users can be identified as Operators (S1) by the TOE.

OT.DisplayVersion

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

OT.LogData

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

OT.VerifySoftwareUpdateSignature

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

OT.DeletionEphemeralData

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

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 SFR **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.

OT.TamperEvidence - Tamper Detection

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

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.

OT.RandomNumberGenerator - Random number quality

This objective is directly addressed by the SFR **FCS_RNG.1**.

6.3.2 Security Functional Requirements Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The dependency analysis is provides in the following table. All dependencies being expected by CC part 2 and by extended components definition in chapter 5 are either fulfilled or their non-fulfilment is justified.

SFR	Dependencies	Support for Dependencies
FAU_GEN.1	FPT_STM.1 Reliable Time Stamps	FPT_STM.1 is not fulfilled. It is assumed that the TOE makes use of the time stamps provided by the TOE environment. The correctness of the time is verified by the administrator at least once a day, which is considered sufficient here (cf. OE.Date).
FCS_CKM.1/ KDF_BAC	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]	fulfilled by FCS_COP.1/SYM and FCS_COP.1/MAC (note that FIA_UAU.5 specifies the mutual authentication mechanism, which derives session keys from the BAC key)

SFR	Dependencies	Support for Dependencies
	FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4
FCS_CKM.1/ DH_PACE	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]	fulfilled by FCS_COP.1/SYM and FCS_COP.1/MAC
	FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4
FCS_CKM.1/ DH_CA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]	fulfilled by FCS_COP.1/SYM and FCS_COP.1/MAC
	FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data withoutsecurity attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	fulfilled by FCS_CKM.1/*
FCS_COP.1/ SHA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Dependencies are not fulfilled. Hash algorithms do not need cryptographic keys and therefore none of the dependencies applies.
FCS_COP.1/ SYM and FCS_COP.1/ MAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	fulfilled by FCS_CKM.1/*
	FCS_CKM.4 Cryptographic key destruction	fulfilled by FCS_CKM.4
FCS_COP.1/ CER	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Dependencies are not fulfilled. Signature verification algorithms for Passive Authentication only rely on public keys, which are provided by the environment (c.f. OE.SignedCertsAndCRLs and OE.PKI) and therefore none of the dependencies applies.

SFR	Dependencies	Support for Dependencies
FCS_COP.1/ UpdateSig	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Dependencies are not fulfilled, but justified. Signature verification algorithms for update signature verification only rely on public keys, which are provided to the TOE during production of the document management terminal and are fixed over the whole life time of the TOE.
FIA_UAU.1	FIA_UID.1 Timing of identification	fulfilled by FIA_UID.1
FMT_MTD.1/*	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 and FMT_SMF.1
FMT_SMR.1	FIA_UID.1 Timing of identification	fulfilled by FIA_UID.1

Table 4: Dependencies between the SFR for the TOE

6.3.3 Security Assurance Requirements Rationale

The EAL3 was chosen to permit a developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security and require a thorough investigation of the TOE and its development without substantial re-engineering.

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 6.3.2 Security Functional Requirements Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL3 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistencies between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 6.3.2 Security Functional Requirements Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements

and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

A PP-Module – User Interface Unit DMT-PP-UIU

A.1 PP-Module introduction

A.1.1 PP-Module reference

Title:	DMT-PP Module – User Interface Unit
Abbreviation:	DMT-PP-UIU
CC revision:	v3.1 release 5
Version:	2.0
Authors:	Federal Office for Information Security
Publication Date:	6th June 2018
Keywords:	ICAO, inspection system, machine readable travel document, extended access control

A.1.2 Base-PP identification

This PP-Module relies on the following Base Protection Profile:

- DMT-PP (Common Criteria Protection Profile – Document Management Terminal), Version 2.0

A.1.3 Extended package overview

The Base-PP defined in DMT-PP only applies to a document management terminal that consist of a single base unit. This PP-module augments the Base-PP to include the possibility to implement an external user interface unit that can be detached from the base unit (see also Figure 1). That user interface unit provides a dedicated tamper-evident enclosure that contains input- and output-devices of the document management terminal which is part of the TOE. Furthermore, this PP-Module demands the TOE to implement a secure link between the base and the user interface unit, providing integrity, authenticity and confidentiality of the transferred data. The enclosure must not provide connections for any other external devices.

The user interface unit is supposed to be handled by a customer, i.e. the holder of an electron identity document (S5), in order to

– view the data stored on the customer's electron identity document,

– enter the personal electronic identity document access password (PIN),

– capture fingerprints of the customer, and/or

– provide other functionality that requires interaction of the customer with the Document Management Terminal

A.2 Consistency Rationale

This PP-module does not depend on any other PP-modules. This PP-module can only be claimed together with the Base-PP, in the version defined in section 1.1.

This PP-module does not define any additional threats, assumptions or organizational security policies.

This PP-module does not change the objectives for the environment of the Base-PP.

This PP-module adds three new security objectives for the TOE and two new security objectives for the environment in order to satisfy the security problem definition, if required non-TOE hardware is not situated in the base enclosure but in an additional user interface unit. These objectives only apply to that user interface unit which is covered by this PP-module and thus are consistent with the objectives of the base-PP.

The PP-module adds two new SFRs in order to satisfy the security objectives for the TOE of this PP-module. Thus, these SFRs only apply to the user interface unit covered by this PP-module and thus are consistent with the SFRs of the base-PP.

The unions of the security problem definition, the objectives and the security functional requirements from the base PP and from the PP-module do not lead to a contradiction.

A.3 Conformance Claim

A.3.1 CC Conformance Claim

The CC Conformance Claim of this PP-module is identical to the conformance claim of the base protection profile as specified in chapter 2.

A.3.2 Conformance Statement

This PP-Module inherits the conformance statement from the Base-PP. Thus, this PP-Module calls for “strict” conformance.

A.4 Security Problem Definition

The security problem definition of the PP-module is consistent with the security problem definition of the base protection profile. This PP-module does not define any additional threats, assumptions or organizational security policies.

However, the implementation of an external user interface units requires additional measures to satisfy the security problem definition, which are covered by the additional security objectives given in following section.

A.5 Security Objectives

A.5.1 Security Objectives for the TOE

OT.UIUSecureComm– Secure communication between base unit and user interface unit.

The TOE must provide a secure channel between the base unit and the user interface unit, ensuring integrity and confidentiality of the transmitted data. The secure channel must enforce a one-to-one relationship between the base unit containing the Document Application and the user interface unit. The secure channel must be initiated by the base unit containing the Document Application.

Furthermore, the TOE must provide data to the environment, which allows the Operator (S1) to identify the user interface unit that is connected to the base unit.

Application Note 32: *The secure channel is initiated by the TOE and the TOE can only by configured by an Administrator (S2) (c.f. OT.PrivilegedRoleAuthorization). Thus, the secure channel must also be configured by an Administrator (S2).*

OT.UIUTamperEvidence - Tamper Detection

The TOE shall provide features to protect its security functions and its environment inside the enclosure of the Document Management Terminal

The enclosure of the user interface unit shall protect any integrated input and output device (O6+O7) against tampering. In particular, the any physical manipulation within the scope of the intended environment shall be detectable for the Operators (S1) and Administrators (S2) of the TOE.

OT.UIULogPairing

The TOE shall write log data about every change of the pairing between the TOE and an user interface unit (R.PairingData).

A.5.2 Security Objectives for the Operational Environment

OE.UIUSecureBoot

The user interface unit must provide mechanisms to boot its OS and the device drivers of any integrated input and output device (O6+O7) in a secure way so that an initial secure state without protection compromise is guaranteed.

OE.UIUCloseProximity

The Document Management Terminal must ensure that the user interface unit is in close proximity to the base unit during operation and must close the secure channel between the base-unit and that enclosure otherwise.

Application Note 33: *The ST writer has to describe how the Document Management Terminal itself can detect if the user interface unit is out of the allowed range to the base unit. In particular, the device must not communicate with the base unit over a fraudulently relayed connection.*

A.5.3 Security Objectives Rationale

	OT.UIUSecureComm	OT.UIUTamperEvidence	OT.UIULogPairing	OE.UIUSecureBoot	OE.UIUCloseProximity
T.Eavesdropping	X	X			
T.DataCompromise					X
T.TerminalManipulation	X	X			
A.SecureBoot				X	
OSP.TAKeyManagement	X				
OSP.CheckTerminal		X			
OSP.Logging			X		

Table 5: Security Objectives Rationale – Package DMT-PP-UIU

T.Eavesdropping

- **OT.UIUTamperEvidence** prevents tampering of the components inside the user interface unit the TOE relies on, by embedding them into a tamper-resistant enclosure.

- **OT.UIUSecureComm** make sure that attackers cannot eavesdrop secret data during transport between the base unit of the Document Management Terminal and the external user interface unit.

T.DataCompromise

- **OE.UIUCloseProximity** makes sure that the external user interface unit cannot make use of the TOE, if it is brought out of range from the base unit.

T.TerminalManipulation

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

- **OT.UIUTamperEvidence** prevents tampering of the components inside the user interface unit the TOE relies on, by embedding them into a tamper-resistant enclosure.
- **OT.UIUSecureComm** ensures that only user interface units may communicate with the TOE that have been authorised by an Administrator (S2).

A.SecureBoot

- **OE.UIUSecureBoot** addresses this assumption directly as a requirement for the user interface unit.

OSP.TAKeyManagement

- **OT.UIUSecureComm** makes sure that the base unit can only communicate with an user interface unit that have been authorized by an Administrator (S2) and that the transferred data is protected in integrity, authenticity and confidentiality.

OSP.CheckTerminal

- **OT.UIUTamperEvidence** allows the Operator (S1) to detect modifications of the user interface unit.

OSP.Logging

- **OT.UIULogPairing** enforces the TOE to write log data about every change of the pairing between the TOE and an user interface unit to a logfile (R.LogData) inside the log storage (O4).

A.6 Security Functional Requirements

A.6.1 Class FAU - Logging

FAU_GEN.1/UIU	Audit data generation
	Hierarchical to: No other components.
	Dependencies: FPT_STM.1 Reliable time stamps
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 [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) every modification the TOE configuration data (R.ConfigurationData); and **d) every modification to the pairing of connected User Interface Units (R.PairingData); and** e) software updates; and f) announcement of having processed the Passive Authentication protocol including the result of the process; and g) announcement of having processed the Chip Authentication protocol including the

result of the process; and
h) [assignment: *other specifically defined auditable events*][51].

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, [assignment: *other audit relevant information*].

Refinement: The TSF supports the storage of audit records by the TOE environment (cf. OE.SecureComponents) by providing the audit records according to FAU_GEN.1.1**/UIU ~~c) and d)~~ c), d) and e)** 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**/UIU ~~e) and f)~~ f) and g)** to the Operator (S1).

Application note 34: *The TOE makes use of the time stamps provided by the TOE environment (cf. OE.SecureComponents and OE.Date).*

Application note 35: *This SFR is a refinement of the SFR FAU_GEN.1 from the Base-PP and further restricts its requirements. The performed refinement operation is denoted in such a way that added words are* **underlined and bold** *and removed words are* ~~**crossed out, underlined and bold**~~.

A.6.2 Class FMT – Security Management

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to modify[52] the
1) TOE configuration data (Modify R.ConfigurationData)
2) Pairing between the TOE and the control software (Modify R.PairingData)
3) Pairing between the TOE and a user interface unit (Modify R.PairingData)
4) the further TSF data: [assignment: list of TSF data][53]
to Administrators (S2)[54].

Application note 36: *This SFR is a refinement of the SFR FMT_MTD.1/TOE-Config from the Base-PP and further restricts its requirements. The performed refinement operation is denoted in such a way that added words are* **underlined and bold**.

FMT_SMF.1/UIU	Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
1) Update the TOE configuration data (Modify R.ConfigurationData),
2) Update the pairing between the TOE and the control software (Modify R.PairingData),
3) Update the pairing between the TOE and an external user interface unit (Modify R.PairingData),

51 [assignment: *other specifically defined auditable events*]
52 [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
53 [assignment: *list of TSF data*]
54 [assignment: *the authorised identified roles*]

4) Identify the paired user interface unit,
5) Read the TOE version,
6) Revise the log data (Read R.LogData),
7) Assign or remove the security attribute SecAttr.AccTerminalPrivateKey to Operators (S1) (see Application Note 27)
8) 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
9) [assignment: *list of further management functions to be provided by the TSF*][55].

Application note 37: *The functionality to identify the paired user interface unit shall allow any user of the TOE to unambiguously detect any user interface unit that is connected to the TOE. Therefore, the TOE must provide suitable data to the environment without disclosing the secret key material associated with R.PairingData.*

Application note 38: *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).*

Application note 39: *This SFR is a refinement of the SFR FMT_SMF.1 from the Base-PP and further restricts its requirements. The performed refinement operation is denoted in such a way that added words are* **underlined and bold**. *Furthermore, Application Note 37 is added.*

A.6.3 Class FPT - Tamper Resistance

FPT_PHP.1/UIU	Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering of the user interface unit that houses *[assignment: list of devices]* that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application note 40: *This SFR allows the ST writer to swap out components which are necessary for the operation of the Document Management Terminal into a separate tamper-evident enclosure. If a separate enclosure is used, the trusted channel between them has to fulfil SFR FPT_TRP.1/UIU. This SFR may be iterated for multiple enclosures. The ST writer shall list any required non-TOE hardware/software according to section 1.3.3 that is situated in the separate enclosure in the "list of devices" of the open assignment operation.*

A.6.4 Class FTP - Trusted Paths

FTP_TRP.1/UIU	Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and local[56] ~~users~~ user interface unit housing the components listed in FPT_PHP.1.1/UIU that is logically distinct from other communication paths and provides assured identification of its end

55 [assignment: *list of management functions to be provided by the TSF*]
56 [selection: *remote, local*]

points and protection of the communicated data from modification, disclosure, [assignment: *other types of integrity or confidentiality violation*][57].

FTP_TRP.1.2 The TSF shall permit the TSF[58] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for any service relying on the components listed in FPT_PHP.1.1/UIU[59].

Application note 41: *The pairing between the user interface unit and the base unit of the Document Management Terminal is configured in R.PairingData and may only be modified by an Administrator (S2).*

A.6.5 Security Functional Requirements Rationale

This section provides the rationale for the internal consistency and completeness of the security functional requirements defined in this PP-module.

Table 6 provides an overview for security functional requirements coverage also giving an evidence for sufficiency and necessity of the SFRs chosen.

	OT.UIU TamperResistance	OT.UIU SecureComm	OT.UIULogPairing
FAU_GEN.1/UIU - Audit data generation			X
FMT_MTD.1/TOE-Config_UIU - Management of TSF data		X	
FMT_SMF.1/UIU - Specification of Management Functions		X	
FPT_PHP.1/UIU - Passive detection of physical attack	X		
FTP_TRP.1/UIU - Trusted path		X	

Table 6: Coverage of Security Objectives for the TOE by SFRs – Package DMT-PP-UIU

The objectives of the PP-Module are met by the SFRs in the following way:

OT.UIUTamperResistance - Tamper Detection

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

OT.UIUSecureComm– Secure communication between the base unit and the user interface unit.

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

- SFR **FTP_TRP.1/UIU** enforces a one-to-one relationship by providing a trusted path to the user interface unit that provides protection in integrity and confidentiality.
- SFR **FMT_SMF.1/UIU** specifies that the TOE must be capable to configure the pairing between the base-unit and an external user interface unit.
- SFR **FMT_MTD.1/TOE-Config_UIU** restricts the ability to configure the pairing between the base-unit and an external user interface unit to Administrators (S2).

The following objective from the Base-PP is met by the SFRs in the following way:

OT.UIULogPairing

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

57 [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
58 [selection: *the TSF, local users, remote users*]
59 [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]

A.6.6 Security Functional Requirements Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

The dependency analysis is provides in the following table. All dependencies being expected by CC part 2 and by extended components definition in chapter 5 are either fulfilled or their non-fulfilment is justified.

SFR	Dependencies	Support for Dependencies
FAU_GEN.1/UIU	FPT_STM.1 Reliable Time Stamps	FPT_STM.1 is not fulfilled. It is assumed that the TOE makes use of the time stamps provided by the TOE environment. The correctness of the time is verified by the administrator at least once a day, which is considered sufficient here (cf. OE.Date).
FMT_MTD.1/ TOE-Config_UIU	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	fulfilled by FMT_SMR.1 and FMT_SMF.1/UIU

Table 7: Dependencies between the SFR for the TOE

B PP-Configuration DMT-with-UIU

B.1 PP-Configuration reference

Title:	DMT-PP Configuration – Document Management Terminal implementing a User Interface Unit
Abbreviation:	DMT-with-UIU
Version:	2.0
Authors:	Federal Office for Information Security
Publication Date:	6th June 2018

B.2 Components statements

This PP-Configuration includes the following Base Protection Profile:

- DMT-PP (Common Criteria Protection Profile – Document Management Terminal), Version 2.0

Additionally, this PP-Configuration includes the following PP-module:

- DMT-PP-UIU (DMT-PP Module – User Interface Unit), Version 2.0

B.3 Conformance statement

This PP-Configuration calls for “strict” conformance.

B.4 Security Assurance Requirements (SAR) statement

The security assurance requirements for this PP-Configuration are those taken from the Evaluation Assurance Level 3 (**EAL3**).

C Appendix

C.1 Glossary

Term	Definition
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Audit entries generated by the TOE and stored in the TOE environment
Authenticity	Ability to confirm the 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], Part 11 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).
Certificate chain	Hierarchical sequence of Document Management Terminal certificate (lowest level), Document Verifier certificate and Country Verifying Certification Authority certificates (highest level), where the certificate of a lower lever 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).
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority public key (KPuCSCA) issued by Country Signing Certification Authority stored in the inspection system.
Country Verifying Certification Authority	The country specific root of the authorization PKI, that grants access to an electronic identity document 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.
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], 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 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 Document Management Terminal [ICAO 9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the electronic identity document's chip. It may carry the Document Signer certificate (CDS). [ICAO 9303]
Document	Certification authority creating the Document Management Terminal certificates and

Term	Definition
Verifier	managing the authorization of the Document Management Terminal 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.
Extended Access Control	Security mechanism identified in [ICAO 9303] and [TR-03110-1] (EACv1) or [TR-03110-2] (EACv2) by means of which the electronic identity document's chip (i) verifies the authentication of the Document Management Terminal 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 Document Management Terminal 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 data.
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
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.
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the electronic identity document or Electronic Passport's 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]
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].
Password Authenticated Connection Establishment (PACE)	The PACE Protocol defined in [TR-03110-2] is a password authenticated Diffie-Hellman key agreement protocol that provides explicit password-based authentication of the electronic identity document's chip and the Document Management Terminal and protects their communication by means of secure messaging.
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.
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.
Secure	Secure messaging using encryption and message authentication code according to

Term	Definition
messaging in encrypted mode	
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.
Terminal Authorization	Intersection of the certificate holder authorizations defined by the Document Management Terminal, 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]
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC 1]).
User data	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC 1]).

C.2 Acronyms

Acronym	Term
BAC	Basic Access Control
CC	Common Criteria
CRL	Certificate revocation list
DS	Document Signer
MRZ	Machine readable zone
n.a.	Not applicable
OCR	Optical character recognition
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity coupling device
PIN	Personal identification number
SAR	Security assurance requirements
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE security functionality

Reference Documentation

CC 1	CC: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5, CCMB-2017-04-001, 2017
CC 2	CC: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5, CCMB-2017-04-002, 2017
CC 3	CC: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, CCMB-2017-04-003, 2017
CEM	CC: Common Methodology for Information Technology Security Evaluation, Evaluation methodology; Version 3.1, Revision 5, CCMB-2017-04-004, 2017
ICAO 9303	ICAO: Doc 9303: Machine Readable Travel Documents, 7th Edition, 2015
ISO/IEC 14443	ISO/IEC: ISO/IEC 14443:2016 - Identification cards - Contactless integrated circuit cards - Proximity cards, 2016
ISO/IEC 7816	ISO/IEC: ISO/IEC 7816:2013 - Identification cards - Integrated circuit cards, 2013
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