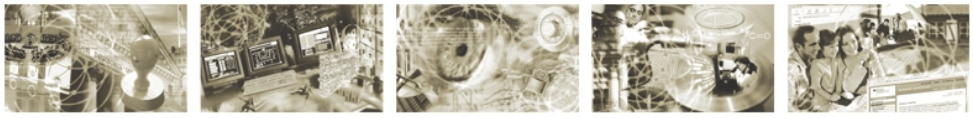
Bundesamt
für Sicherheit in der
Informationstechnik



Common Criteria Protection Profile

Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control

Common Criteria

BSI-CC-PP-0083

Foreword

This ‘Common Criteria Protection Profile — Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control’ (PP Standard Reader) is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria, version 3.1, Revision 4 ([CC part 1 v.3.1], [CC part 2 v.3.1], [CC part 3 v.3.1]).

Correspondence and comments to this PP Standard Reader should be referred to:

CONTACT ADDRESS

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany

Tel **+49 228 99 9582-0**
Fax **+49 228 99 9582-5400**

Email bsi@bsi.bund.de

Table of Content

15

1. PP Introduction

1.1. PP reference

Title:	Protection Profile — Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1 (Revision 4)
Assurance Level:	The assurance level for this PP is EAL3 augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 and AVA_VAN.3.
General Status:	final
Version Number:	1.0
Date	29.11.2013
Registration:	BSI-CC-PP-0083
Keywords:	Card Reader, eID, EAC, PACE, nPA, Smart Card, Standard Reader

1.2. TOE Overview

The TOE is a Smart Card Reader with PIN-Pad according to the “Standard Reader” in BSI [TR-03119] supporting eID based on Extended Access Control.

1.2.1. TOE Type definition

The Target of Evaluation (TOE) is the Standard Reader according to BSI [TR-03119] a Smart Card Reader with PIN-Pad.

1.2.2. TOE usage and security features

The TOE is used with the eID functions of the new German electronic identity card. The purpose of the TOE is to perform the terminal part of PACE according to [TR-03110] and to offer PIN-Management with secure PIN-Entry.

From a technical view, the TOE is a separate device and connected to the host computer via e.g. USB consisting at least of

- a proximity coupling device (PCD) according to [ISO 14443]
- a PIN Pad
- An indicator e.g. a light-emitting diode (LED), which is needed to signal the PIN-Pad mode to the End-User (see also “Indication of the Secure Mode” in [TR-03119]). If the card reader is always in secure mode no explicit signalling and therefore no indicator is necessary.
- an interface to the host computer according to [TR-03119]
- firmware
  - implementing the terminal part of PACE according to [TR-03110]
  - key generation needed for the terminal part of PACE according to [TR-03119]

- enforcing filtering rules for passwords according to [TR-03119]
- enabling PIN Management
- supporting EAC according to [TR-03110] executed by an remote terminal (via the host computer) and the eID-Card

The TOE complies with the Technical Guideline BSI TR-03119 “Requirements for Smart Card Readers Supporting eID and QES Based on EAC” (cf. [TR-03119]).

The TOE provides the following security features:

PACE Authentication of the eID-Card user

The TOE implements the terminal part of the user authentication of the eID-Card holder to the eID-Card by means of PACE according to BSI [TR-03110] and protects the passwords given to the TOE.

Filtering rules

To prevent circumvention of the secure PIN input using the PIN Pad, the TOE must filter certain commands, i.e. it must not execute or must not forward these commands to the eID-Card (cf. [TR-03119]).

PIN Management

Change the PIN of the eID-Card after authentication of the card holder using the current PIN and unblock the PIN of the eID-Card using the PIN Unblocking Key (PUK) (cf. [TR-03119]).

Support for Extended Access Control

The TOE supports EAC according to [TR-03110] executed by a remote terminal (via the host computer) and the eID-Card:

- forwarding the CVC Certificates sent by the host computer to the eID-Card
- forwarding the Final Access Rights sent by the host computer to the eID-Card
- forwarding the result of PACE to the host computer

TOE Integrity Verification

The TOE must be designed in a way allowing the owner to detect if manipulation took place.

TOE Updates

Firmware updates may be made by download on demand. The Update data must be signed and may only be installed if the signature has been successfully verified.

1.2.3. Non-TOE hardware, firmware and software

The TOE is intended to be used as an IT product used with a user client (personal computer) supported by the TOE. This means not in any case a desktop PC but a combination of hardware and operating system related to one person or a defined group of trusted persons. The IT-environment supports protection of the TOE and the resources used by the TOE against unauthorized modifications by suitable protection mechanisms. Users of the product are trustworthy and follow the instructions of the user guidance delivered with the TOE.

Remote Terminal

The Terminal Authentication protocol as part of EAC according to [TR-03110] will be executed by

an remote terminal (via the host computer) and the eID-Card. This remote terminal is not directly known to the TOE. It is only relevant as the result of the Terminal Authentication protocol determined by the eID-Card must be forwarded to the host computer.

85 **Operating System/Host Personal Computer**
In order to support the communication between the eID-Card and the remote terminal (as described above) the TOE will be connected to the user's personal computer (host computer) running an operating system which is supported by the TOE.

eID-Card

90 The TOE supports eID-Cards compliant to BSI [TR-03110] and [TR-03127]. The TOE may support additional types of smart cards. This is out of scope of this Protection Profile.

Driver-Software

The TOE may be delivered together with a driver software to be installed on the users personal computer (host computer) which supports the interoperability between TOE and host computer and
95 an update functionality. This is out of scope of this Protection Profile.

2. Conformance Claims

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-2012-09-001, Version 3.1, Revision 4, September 2012 ([CC part 1 v.3.1])

100 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 ([CC part 2 v.3.1])

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 ([CC part 3
105 v.3.1])

as follows

– Part 2 extended,

– Part 3 conformant.

The

110 • Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012, ([CC eval. meth. v.3.1])

has to be taken into account.

2.2. PP Claim

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

2.3. Package Claim

115 This PP is conforming to assurance package EAL3 augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 and AVA_VAN.3 defined in CC part 3 ([CC part 3 v.3.1]).

2.4. Conformance rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

2.5. Conformance statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

3. Security Problem Definition

120 The following section describes the threats, organizational policies and assumptions for the TOE addressed within this protection profile.

3.1. Introduction

Assets

Asset	Comment	Protection goal
PACE passwords	The passwords of the eID-Card holder used to authenticate himself/herself to the eID-Card. The PACE password can either be PIN, PUK or CAN, refer to [TR-03110] and [TR-03127]. This includes the current PIN and the PIN which is given to the TOE in order to set it as new one during PIN-Management.	confidentiality and integrity
Final Access Rights	CVC Access Rights requested with the presented CVC reduced and/or accepted by the End-User sent by the host computer to the TOE.	integrity
Update data	Data intended to be used for an update of the TOE.	authenticity and integrity

table 1: List of TOE assets

Application note 1: The personal data of the End-User resp. eID-Card holder is stored on the eID-Card (e.g. birth date). Please note that personal data will never be processed by the TOE and
125 only personal data encrypted by the eID-Card will be forwarded by the TOE to the host computer. Therefore the TOE is not responsible for the confidentiality of these data. Confidentiality and integrity of the personal data are protected by the card.

TSF data	Comment	Protection goal
Public key for update data verification	This public key is used for verification of data of the manufacturer intended for use for TOE updates. The protection of the integrity ensures the correct functionality resp. behaviour of the TOE. This public key is generated by the TOE vendor in a secure way and part of the TOE internal data. This public key is trusted.	authenticity and integrity

table 2: List of TSF data

3.1.1. External Entities

End-User

Any human entity having direct (physical) access to the TOE and especially to the human user
130 interfaces of the TOE. Note that the End-Users are local (human) Users.

eID-Card holder

The eID-Card holder is an End-User identified by holding the eID-Card and knowing (and entering) the PACE password corresponding to the eID-Card.

3.2. Threats

This section describes the threats to be averted by the TOE independently or in conjunction 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.Malware **Insertion of Malware into or through the TOE**

Assets: The TOE and therefore all assets of the TOE

Security goal: The integrity of the TOE and confidentiality, authenticity and integrity of its assets.

Adverse action: Insertion of Malware via one of the following communication interfaces: Interface to host computer, PIN Pad, PCD

Attacker: The attacker has access to one of the communication interfaces of the TOE listed above. He is assumed to have enhanced-basic attack potential.

T.Passwords **Compromise of the eID-PIN, CAN or eID-PUK**

Assets: The eID-PIN, eID-PUK and CAN

Security goal: The confidentiality of the assets.

Adverse action: The attacker gains access to a representation of the eID-PIN, eID-PUK or CAN in the TOE via a communication interface of the TOE.

Attacker: The attacker has access to one of the communication interfaces of the TOE. He is assumed to have enhanced-basic attack potential.

T.HardwareMan **Manipulation of the hardware of the TOE**

Assets: The TOE and therefore all assets of the TOE

Security goal: The integrity of the TOE and confidentiality, authenticity and integrity of its assets.

Adverse action: The attacker manipulates either the hardware of the TOE itself, e.g. by bringing a hardware-keylogger into the TOE, or the attacker bypasses the defined and secured interfaces of the TOE by opening the TOE hardware for a transfer of Malware.

Attacker: The attacker has access to the hardware of the TOE. He is assumed to have enhanced-basic attack potential.

3.3. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices or guidelines imposed by an organization upon its operations (see [CC part 1 v.3.1], sec. 3.2).

P.AccessRights **Handling CVC Access Rights**

In order to support the fulfilment of the requirements of §18(5) [PAuswG] the Final Access Rights gained from the host computer must be sent unaltered to the eID-Card as part of the PACE protocol (cf. BSI [TR-03110]).

P.PACE Password Authenticated Connection Establishment support

The [PAuswG] stipulates that the eID-Card holders authenticate themselves to their eID-Cards with their eID-PIN or another PACE password (PUK, CAN) and a trusted channel to the eID-Card is established using the PACE protocol in accordance with BSI [TR-03110]. Entering the PIN or other PACE password only directly on the TOE will enforce a much better protection of the password than using PIN-Entry via the host computer. The use of the eID-Application of the eID-Card by the End-User requires the execution of Terminal Authentication protocol according to [TR-03110]. Therefore the response of the eID-Card about success or failure of the authentication attempt via PACE protocol must be forwarded to the host computer.

P.TerminalAuth Forwarding the result of Terminal Authentication

The Terminal Authentication protocol executed by eID-Card and remote terminal (according to [TR-03110]) is used to decide which (or if) personal data the remote terminal is allowed to read from the eID-Card. If the host computer gets a wrong negative result of the protocol execution this would lead to a denial of service.Otherwise if the host computer gets a wrong positive result the End-User might trust the remote terminal misleadingly.

3.4. Assumptions

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

A.End-User Trustworthy End-User

It is assumed that the End-Users of the product are trustworthy and follow the instructions of the user guidance delivered with the TOE. Further it is assumed that the End-Users verify the physical integrity of the TOE each time before use. The eID-Card holder is assumed to know and protect the PACE passwords for authentication to the eID-Card.

A.Environment Location of the TOE

It is assumed that the TOE is located in an admission restricted area (e.g. domestic area or company area) or under constant supervision by the End-User ensuring by one of these methods that the TOE cannot be manipulated without user notification.

A.ChoiceOS Choice of the Operating System

It is assumed that only host computers with operating systems still supported by the OS vendor are used with the TOE.

Application note 2: Operating systems supported by the TOE have to be listed by the ST writer.

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE
200 environment.

4.1. Security Objectives for the TOE

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

OT.Interfaces Interfaces of the TOE

The TOE shall only accept incoming messages which are syntactically correct according to the
205 corresponding application provided by the TOE on the following interfaces:

1. Pin-Pad
2. PCD
3. Interface to host computer

The TOE shall ensure that data contained in those messages is never executed as program code
210 except for successfully verified update data.

OT.PACE PACE support

The TOE shall provide the capability for the eID-Card holder to authenticate himself against an eID-Card and establishing a trusted channel to the eID-Card using the PACE protocol in accordance with BSI [TR-03110]. Therefore the TOE shall implement the terminal part of the PACE protocol in
215 accordance with BSI [TR-03110]. The TOE shall forward the response of the eID-Card about success or failure of the authentication attempt to the host computer.

OT.Integrity Verification of TOE integrity

The TOE shall provide mechanisms to detect manipulations of its firmware and/or hardware. The TOE shall pass an integrity check of it's firmware at least during every update process. The process
220 to check the hardware integrity shall be explained in the user guidance and performable by the End-User.

OT.Update Authenticity of Update data

The TOE shall verify the authenticity and integrity of data received on the Update-Interface as Update data signed by the manufacturer and discard data detected as not being authentic or if the
225 integrity check fails. Additionally the TOE shall not accept Update data which is older or the same than the installed version of the TOE.

OT.SecretPass Keeping the passwords secret

The TOE shall ensure the confidentiality of any PACE password given to the TOE by preventing any export or use of the passwords except for the following cases:

230 • The TOE shall only use the PIN for authentication of the eID-Card holder to the eID-Card by means of PACE according to [TR-03110] or PIN-Management according to [TR-03110].

• The PUK and CAN shall only be used for PIN-Management according to [TR-03110].

OT.Password Password security

Any PACE password given to the TOE shall be overwritten by the TOE when it is not longer

needed for its purpose.

OT.AccessRights Final Access Rights

The TOE shall ensure to forward the Final Access Rights gained from the host computer unaltered to the eID-Card.

OT.FilterRules Accept passwords and execute PACE only on given rules

To prevent circumvention of the secure PIN input using the PIN pad, the card reader must filter certain commands, i.e. it must not execute or forward the commands to the card.

- It must be prevented that the terminal part of PACE can be executed by the host computer while using the TOE as reading device for the eID-Card.
- eID-PIN and PUK must not be accepted if provided by the host computer. These passwords must only be imported via the PIN Pad.
- If EstablishPACEChannel according to [TR-03119] is used with CAN provided by the host computer, the card reader must request a user confirmation before establishing the secure channel.
- The TOE must not support any combinations of role-and-password pairs except the following ones:
  - “unauthenticated terminal” with CAN, PUK or eID-PIN
  - Authentication Terminal with CAN or eID-PIN
- It must be prevented that the eID-PIN can be changed by the host computer (cf. [TR-03119]: “RESET RETRY COUNTER”).
- It must be prevented that the End-User is misled to input his/her PACE passwords other than during the PACE process.

OT.TerminalAuth Forwarding the result of Terminal Authentication

The TOE shall forward the result of the Terminal Authentication protocol executed by eID-Card and remote terminal unaltered to the host computer.

4.2. Security Objectives for the Operational Environment

The following security objectives of the TOE environment have to be met by the TOE’s operational environment.

OE.End-User Trustworthy End-User

The End-User of the product shall be trustworthy and follow the instructions of the user guidance delivered with the TOE. The End-User shall verify the physical integrity of the TOE each time before use and download and install the Updates provided by the TOE manufacturer. Additionally the eID-Card holder has to ensure the confidentiality of the PACE passwords used for authentication to the eID-Card.

OE.Environment TOE environment

The TOE shall be located in an admission restricted area or under constant supervision by the End-User ensuring by one of these methods that the TOE cannot be manipulated without user notification.

OE.Update Updates

The manufacturer shall provide only certified updates of the TOE. The data provided for the download shall contain either a version number or the date of the update and be signed by the
275 manufacturer.

OE.ChoiceOS Choice of the Operating System

Only host computers with operating systems still supported by the OS vendor shall be used with the TOE. The vendor shall list the OS supported by the TOE in the user guidance and recommend only to use those OS still supported by the OS vendor.

4.3. Security Objective Rationale

280 The following table 3 provides an overview for security objectives coverage.

	OT.Interfaces	OT.PACE	OT.Integrity	OT.Update	OT.Password	OT.SecretPass	OT.AccessRights	OT.FilterRules	OT.TerminalAuth	OE.End-User	OE.Environment	OE.Update	OE.ChoiceOS
T.Malware	x		x	x								x	
T.Passwords					x	x		x		x			
T.HardwareMan			x							x	x		
P.AccessRights							x						
P.PACE		x											
P.TerminalAuth									x				
A.End-User										x			
A.Environment											x		
A.ChoiceOS													x

table 3: Security Objective Rationale

The threat **T.Malware** “Insertion of Malware into or through the TOE” is addressed by the objectives **OT.Interfaces**, **OT.Integrity**, **OT.Update** and the objectives for the environment **OE.Update**. The objective **OT.Interfaces** requires the TOE to only accept syntactically correct messages according to the corresponding technical guidelines on the interfaces to the host
285 computer, the eID-Card and the PIN Pad and to never execute data contained in these messages as program code (except for authenticated update data). **OT.Update** enforces the TOE to check the authenticity and integrity of update data and only execute those data on a positive check result, while **OE.Update** arranges for signed Update data provided by the TOE manufacturer. Due to **OT.Integrity** the TOE is capable to check the integrity of its firmware.

290 The threat **T.Passwords** “Compromise of the eID-PIN, CAN or eID-PUK” is directly addressed by the objective **OT.SecretPass** which requires the TOE to protect the PACE passwords by only using them within the PACE protocol and by **OT.Password** which requires the TOE to overwrite them after usage in the TOE and only use them for PACE or PIN-Management. **OT.FilterRules** enforces the TOE to deny all PACE password entries providing a circumvention of the TOE's security
295 features to protect the PACE passwords. Additionally **OE.End-User** requests the eID-Card holder to keep his/her PACE password secret.

The threat **T.HardwareMan** “Manipulation of the hardware of the TOE” is adressed by the security objectives **OT.Integrity**, **OE.Environment** and **OE.End-User.** Due to **OT.Integrity** the TOE it is possible for the End-User to check the hardware integrity, what is combined with **OE.End-User**
300 requiring the check of the TOE hardware integrity by the End-User in the user guidance. The latter is assisted by **OE.Environment** providing an admission restricted environment for the TOE.

The OSP **P.AccessRights** “Manipulation of the Final Access Rights” is directly addressed by the objective **OT.AccessRights** requiring the TOE to forward the Final Access Rights gained from the host computer unaltered to the eID-Card and so supporting the fulifilment of [PAuswG].

305 The OSP **P.PACE** “Password Authenticated Connection Establishment support” requires the support of the PACE protocol as the chosen mechanism to authenticate the eID-Card holder to the eID-Card. The OSP is directly addressed by the security objective **OT.PACE** “PACE support” which demands the TOE to implement the terminal part of the PACE protocol according to [TR-03110].

310 The OSP **P.Terminal Auth** “Forwarding the result of Terminal Authentication” is directly addressed by the security objective **OT.TerminalAuth** as it requires the TOE to forward the result of the Terminal Authentication protocol as announced by the eID-Card in order to prevent the eID-Card holder from trusting misleadingly a non-authenticated Terminal.

The assumption **A.End-User** “Trustworthy End-User” is directly covered by the security objective
315 for the TOE environment **OE.End-User** “Trustworthy End-User” claiming that the End-User is trustworthy and follows the TOE’s user guidance.

The assumption **A.Environment** “Location of the TOE” is directly addressed by the security objective for the environment **OE.Environment**.

The assumption **A.ChoiceOS** “Choice of the Operating System” is directly addressed by the
320 security objective for the environment **OE.ChoiceOS**.

5. Extended Components Definition

5.1. Definition of the Family FCS_RNG

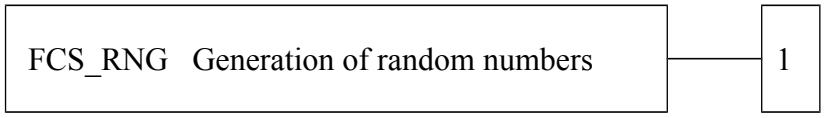
This section describes the functional requirements for the generation of random number to be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family (FCS_RNG) of the Class FCS (cryptographic support).

The family “Generation of random numbers (FCS_RNG)” is specified as follows according to
325 [AIS20/31].

FCS_RNG Generation of random numbers
Family behaviour

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

330 Component levelling:



FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

335 There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

340 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 random numbers that meet [assignment: *a defined quality metric*].

5.2. Definition of the Family FIA_API

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

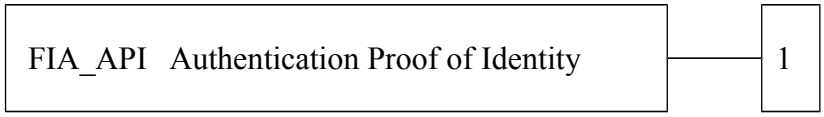
Application note 3: The other families of the Class FIA describe only the authentication verification of users’ identity performed by the TOE and do not describe the functionality to prove the TOE identity or supporting the user to prove its identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [CC part 1 v.3.1], chapter “Extended components”) from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove its own identity or supporting the user to prove its identity to be verified by an external entity in the TOE operational environment.

Component levelling:



FIA_API.1 Proof of Identity.

Management: FIA_API.1

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

Audit: FIA_API.1

There are no auditable events foreseen.

FIA_API.1 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

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in [CC part 1 v.3.1]. 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. Refinement of security requirements is denoted in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

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

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

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.

6.1. Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into one sub-section for the cryptographic support and further sub-sections for groups of security objectives.

6.1.1. Cryptographic Support

Application note 4: The ST writer shall amend the SFRs concerning cryptographic support by adding direct references to the relevant chapters in the standards given and where applicable additional information so that each cryptographic function to be used by the TOE is unambiguously determined.

6.1.1.1. Cryptographic key generation (FCS_CKM.1)

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

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/PACE Cryptographic key generation – Key Agreement PACE

FCS_CKM.1.1/ PACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm session key agreement using PACE[1] and specified cryptographic key sizes of at least 128 bit[2] that meet the following: BSI [TR-03110] using the [PKCS#3] for Diffie-Hellman Key-Agreement or using the [TR-03111] for ECKA Key-Agreement[3].

Application note 5: The TOE shall at least implement the key derivation function in accordance to [TR-03110] with the concrete algorithm specified as [PKCS#3] or ECKA as specified in [TR-03111].

6.1.1.2. Cryptographic key destruction (FCS_CKM.4)

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

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_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroization[4] that meets the following: none[5].

Application note 6: The ephemeral keys established during PACE shall be actively overwritten when they are no longer used. The PACE passwords given to the TOE for PACE or PIN-Management shall also the actively overwritten when they are no longer used.

6.1.1.3. Cryptographic operation (FCS_COP.1)

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

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

1 [assignment: *cryptographic key generation algorithm*]
2 [assignment: *cryptographic key sizes*]
3 [assignment: *list of standards*]
4 [assignment: *cryptographic key destruction method*]
5 [assignment: *list of standards*]

FCS_COP.1/AES Cryptographic operation – Encryption and Decryption using AES

FCS_COP.1.1/ AES	The TSF shall perform decryption and encryption[6] in accordance with a specified cryptographic algorithm AES – CBC mode[7] and cryptographic key sizes of at least 128 bit[8] that meet the following: [FIBS_PUB_197][9].

FCS_COP.1/CMAC Cryptographic operation – Message Authentication using AES-CMAC

FCS_COP.1.1/ CMAC	The TSF shall perform calculation of Message Authentication Code[10] in accordance with a specified cryptographic algorithm AES-CMAC[11] and cryptographic key sizes at least 128 bit[12] that meet the following: [RFC4493] and [NIST_800_38B][13].

Application note 7: The cryptographic algorithms AES-CBC and AES-CMAC are used for secure messaging channel established with PACE keys, as well as part of the PACE protocol and the responses of the eID-Card during the process.

FCS_COP.1/Sig Cryptographic operation – Signature verification

FCS_COP.1.1/ Sig	The TSF shall perform digital signature verification[14] in accordance with a specified cryptographic algorithm [assignment: *digital signature algorithm listed in [TR-02102]*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [TR-02102][15]

Application note 8: FCS_COP.1/Sig shall be used for Update data verification.

6.1.1.4. Random Number Generation (FCS_RNG.1)

The TOE shall meet the requirement “Random Number Generation (FCS_RNG.1)” as specified below (Common Criteria Part 2 extended, cf. sec. 5.1).

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1 Random Number Generation

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 random numbers that meet [assignment: *a defined quality metric*].

Application note 9: This SFR requires the TOE to generate random numbers used for the authenti-cation protocols and key derivation mechanisms (i.e. FCS_CKM.1). The ST writer shall complete FCS_RNG.1 and for that consider the requirements for random number generation of [TR-03119].

6 [assignment: *list of cryptographic operations*]
7 [assignment: *cryptographic algorithm*]
8 [assignment: *cryptographic key sizes*]
9 [assignment: *list of standards*]
10 [assignment: *list of cryptographic operations*]
11 [assignment: *cryptographic algorithm*]
12 [assignment: *cryptographic key sizes*]
13 [assignment: *list of standards*]
14 [assignment: *list of cryptographic operations*]
15 [assignment: *list of standards*]

6.1.2. Filtering Rules

The following SFRs handle the security objectives OT.PACE, OT.Passwords and OT.FilterRules.

6.1.2.1. FDP_IFC.1/PACE Subset information flow control

The TOE shall meet the requirement “Subset information flow control (FDP_IFC.1)” as specified
445 below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1/PACE Subset information flow control

FDP_IFC.1.1/PACE	The TSF shall enforce the PACE control SFP[16] on the following subjects and information: **1.** subjects: **1.1.** TOE **1.2.** host computer **1.3.** eID-Card **1.4.** End-User **2.** information: messages sent by the host computer or the eID-Card in the context of PACE **3.** operation: PIN Management, EstablishPACEChannel according to [TR-03119], request of the Retry Counter by the host computer[17].

6.1.2.2. FDP_IFF.1/PACE Simple security attributes

450 The TOE shall meet the requirement “Simple security attributes (FDP_IFF.1)” as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

455 **FDP_IFF.1/PACE Simple security attributes**

FDP_IFF.1.1/PACE	The TSF shall enforce the PACE control SFP[18] based on the following types of subject and information security attributes: **1.** subjects: **1.1.** TOE with security attribute “PIN-Pad mode” **1.2.** host computer with security attribute “authentication status” **1.3.** eID-Card **1.4.** End-User **2.** information: **2.1.** messages sent by the host computer in the context of PACE protocol **2.2.** messages sent by the eID-Card in the context of PACE protocol[19].

16 [assignment: *information flow control SFP*]
17 [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
18 [assignment: *information flow control SFP*]

FDP_IFF.1.2/ PACE	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **1.** EstablishPACEChannel must not be performed with an eID-PIN or PUK provided by the host computer, the input of these secret codes exclusively at the PIN pad must be enforced. **2.** If EstablishPACEChannel is used with CAN provided by the host computer, the TOE must request the End-User[20] to confirm the use of the CAN via the PIN Pad before establishing the secure channel. **3.** When EstablishPACEChannel is initiated by the host computer the message must be interpreted according to [TR-03119] **3.1.** if the CHAT contains the role “Authentication Terminal” according to [TR-03119] the value of the security attribute “authentication status” shall be set to “Authentication Terminal”, **3.2.** if EstablishPACEChannel contains no CHAT the value of the security attribute “authentication status” shall be set to “Unauthenticated terminal”, **3.3.** if the CHAT contains the role [assignment: *“authentication role”*] according to [TR-03110] the value of the security attribute “authenti-cation status” shall be set to [assignment: *“authentication status”*] **4.** The following combinations of security attribute “authentication status” and PACE password pairs must be supported: **4.1.** “Unauthenticated terminal” with CAN, PUK or eID-PIN **4.2.** “Authentication Terminal” with CAN or eID-PIN **4.3.** [assignment: *“authentication status”*] with [assignment: *password(s)*] **4.4.** all other combinations must be filtered out. **5.** It must be prevented that the eID-PIN can be changed by the host computer (RESET RETRY COUNTER)[21].
FDP_IFF.1.3/ PACE	The TSF shall enforce the following rules: **1.** the TOE shall prevent that PACE can be executed by the host computer. **2.** the CHAT sent by the host computer and containing the Final Access Rights shall be forwarded unaltered to the eID-Card. **3.** the result of the Terminal Authentication protocol transmitted by the eID-Card and announced by the eID-Card shall be forwarded by the TOE to the host computer. **4.** The status of the security attribute “PIN Pad mode” shall be unambiguously signalled to the End-User. **4.1.** The value of the security attribute “PIN Pad mode” is set to “secure” if [assignment: *conditions for secure mode*]. **4.2.** The value of the security attribute “PIN Pad mode” is set to “unsecure” if

19 [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

20 via the host computer or a special signal on the card reader to be described in the user's manual

21 [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

	[assignment: *conditions for unsecure mode*].[22]
FDP_IFF.1.4/ PACE	The TSF shall explicitly authorise an information flow based on the following rules: none[23].
FDP_IFF.1.5/ PACE	The TSF shall explicitly deny an information flow based on the following rules: • If the security attribute “PIN Pad mode” is set to “unsecure”, the TOE shall not request the End-User to give any of his/her PACE passwords to the TOE; • If the security attribute “PIN Pad mode” is set to “secure”, the TOE shall deny any flow of information input on the PIN Pad to any other subject.[24]

Application note 10: For the fulfilment of FDP_IFF.1.3/PACE 3 e.g. a LED could signal the PIN-Pad mode to the End-User (see also “signal secure mode” in [TR-03119]). If the card reader is always in secure mode, the ST writer shall complete the assignments in FDP_IFF.1.3/PACE with “always” and “never”, respectively. In this case no explicit signalling is necessary.

460 **Application note 11:** FDP_IFF.1.2/PACE 3.3 and 4.3 may be completed by the ST writer if needed for additional functions of the TOE e.g. qualified electronic signature.

6.1.2.3. FMT_MSA.3/PACE Static attribute initialisation

The TOE shall meet the requirement “Static attribute initialisation (FMT_MSA.3)” as specified below (Common Criteria Part 2).

465 Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3/PACE Static attribute initialisation

FMT_MSA.3.1/ PACE	The TSF shall enforce the PACE control SFP[25] to provide restrictive[26] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/ PACE	The TSF shall allow the none[27] to specify alternative initial values to override the default values when an object or information is created.

Application note 12: The default value of the security attribute “authentication status” is “none”.

470 The default value of the security attribute “PIN Pad mode” shall be defined by the ST writer.

6.1.2.4. FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

475 Dependencies: FIA_UID.1 Timing of identification

22 [assignment: *additional information flow control SFP rules*]
23 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
24 [assignment: *rules, based on security attributes, that explicitly deny information flows*]
25 [assignment: access control SFP, information flow control SFP]
26 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
27 [assignment: *the authorised identified roles*]

FMT_SMR.1/PACE Security roles

FMT_SMR.1.1/PACE	The TSF shall maintain the roles **1.** host computer **2.** eID-Card[28].
FMT_SMR.1.2/PACE	The TSF shall be able to associate users with roles.

6.1.2.5. Proof of Identity (FIA_API.1)

The TOE shall meet the requirement “Proof of Identity (FIA_API.1)” as specified below (Common Criteria Part 2 extended, cf. sec. 5.2).

480 Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1 Proof of Identity

FIA_API.1.1	The TSF shall provide an execution of the terminal part of PACE in accordance with [TR-03110] including PIN-Management and the forwarding of the PACE result to the host computer; the terminal part of PACE must be performed by the TOE itself, whereby the PIN, PUK and CAN given to the TOE shall only be used for PACE and PIN-Management,[29] to prove the identity of the eID-Card holder[30] **to the eID-Card**.

Application note 13: The terminal part of PACE includes the possibility to use PIN, PUK or CAN for user authentication.

485 ### 6.1.2.6. Subset residual information protection (FDP_RIP.1)

The TOE shall meet the requirement “Subset residual information protection” as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: No dependencies.

490 **FDP_RIP.1 Subset residual information protection**

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from[31] the following objects: • the object the local user enters as a representation of PIN or password and every copy made of it. • Update data not being successful verified as authentic by a digital signature[32]. **The deallocation of a PIN or password representation shall be performed immediately after usage in the PACE protocol, except if PIN-Management shall be performed. In this case the password representation shall be deallocated immediately after usage for PIN-Management. The deallocation shall also be performed immediately if the PACE protocol resp.**

28 [assignment: *the authorised identified roles*]
29 [assignment: *authentication mechanism*]
30 [assignment: *authorized user or rule*]
31 [selection: *allocation of the resource to, deallocation of the resource from*]
32 [assignment: *list of objects*]

	PIN-Management cannot be started or is aborted.

Application note 14: Deallocation in this case means the complete destruction of the object e.g. by overwriting it.

6.1.3. Import of data by the TOE

The following SFRs handle the security objectives OT.Interfaces and OT.Update.

6.1.3.1. FDP_ITC.1 Import of user data without security attributes

495 Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1	The TSF shall enforce the interface control SFP[33] when importing ~~user~~ **data**, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the ~~user~~ **data** when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing ~~user~~ **data** controlled under the SFP from outside the TOE: imported data shall not be interpreted as program code but as pure data except for update data with the value “successfully verified” for the security attribute “verification status Update data”[34].

6.1.3.2. Subset information flow control (FDP_IFC.1)

500 The TOE shall meet the requirement “Subset information flow control” as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

505 **FDP_IFC.1/IF Subset information flow control**

FDP_IFC.1.1/IF	The TSF shall enforce the interface control SFP[35] on: **1.** subject: **1.1.** TOE, **1.2.** host computer, **1.3.** Chipcard, **1.4.** PIN Pad User **1.5.** Update Provider **2.** information: **2.1.** Update data

33 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
34 [assignment: *additional importation control rules*]
35 [assignment: *information flow control SFP*]

	2.2. interface-messages **3.** operations: **3.1.** receiving messages from one of the subjects **3.2.** receiving update data[36]

These subjects, information and security attributes for the interface control SFP are defined the followed:

Subject	**Description**
Update Provider	any entity giving data to the TOE in order to initialise an Update
Chipcard	any entity connecting the TOE at its PCD being or pretending to be an eID-Card or any other kind of chipcard to be used with the TOE
PIN Pad User	any entity using the PIN Pad of the TOE
host computer	any entity connecting the TOE at its interface to be used by the host computer

table 4: Subjects of the interface control SFP

Information	**Description**	
interface-message	Any type of message received via host computer interface, PCD or PIN Pad	
Security Attribute	Value	Implication
syntactical correctness	correct	a message is correct if • its syntax correct corresponding to the requirements of the application of the TOE addressed by this message • the addressed application expects an information block to be forwarded unparsed at this point of the communication
	incorrect	every message which is not correct
Information	**Description**	
Update data	Data given to the TOE with the intention to be used for an update of the TOE which includes any packaging of the actual program code needed for the update (e.g. zip files), additional data (e.g. help files) and a version number or date of the update[37].	
Security Attribute	Value	Implication
verification status Update data	successfully verified	Update data which is successfully verified as authentic by means of digital signature of the TOE manufacturer and containing a version number or date which is higher than the version number or date of the TOE resp. last update installed by the TOE.
	negatively verified	Update data which could not be verified as authentic by means of digital signature of the TOE manufacturer or/and and

36 [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

37 This means the signature of update data has to be checked before data is unpacked or used.

		containing a version number or date which is lower/same than the version number or date of the TOE resp. last update installed by the TOE.

table 5: Information and corresponding security attributes of the interface control SFP

6.1.3.3. Simple security attributes (FDP_IFF.1)

The TOE shall meet the requirement “Simple security attributes” as specified below (Common
510 Criteria Part 2).

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1/IF Simple security attributes

FDP_IFF.1.1/IF	The TSF shall enforce the interface control SFP[38] based on the following types of subject and information security attributes: **1.** subjects: **1.1.** TOE **1.2.** any entity sending messages at the host computer interface, PCD or the PIN Pad **1.3.** any entity giving data to the TOE in order to initialise an Update is defined as Update Provider **2.** information: **2.1.** messages received by the TOE are defined as information named interface-message with the security attribute “syntactically correctness” **2.2.** data given to the TOE with the intention to be used for an update of the TOE are defined as information named Update data with the security attribute “verification status Update data” **3.** [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*][39].
FDP_IFF.1.2/IF	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **1.** messages are checked on their syntactically correctness according to one of the applications provided by the TOE: **1.1.** if the message is syntactical correct the security attribute “syntactically correctness” is set to “correct”, and the message shall be processed by the TOE, **1.2.** otherwise the value of the security attribute is set to “incorrect”and the message must be rejected or discarded. **2.** Update data are verified on their authenticity and integrity by means of digital

38 [assignment: *information flow control SFP*]

39 [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

	signature of the TOE manufacturer by using the “public key for update data verification” before they are used or unpacked: **2.1.** if the signature is verified as correct and is containing a version number or date which is higher than the version number or date of the TOE resp. last update installed by the TOE the security attribute “verification status Update data” is set to “successfully verified”, **2.2.** otherwise the security attribute is set to “negatively verified” and the data must be handled according to FDP_RIP.1. **2.3.** [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*][40].
FDP_IFF.1.3/IF	The TSF shall enforce the none[41].
FDP_IFF.1.4/IF	The TSF shall explicitly authorise an information flow based on the following rules: none[42].
FDP_IFF.1.5/IF	The TSF shall explicitly deny an information flow based on the following rules: none[43].

Application note 15: FDP_IFF.1/IF shall also be completed by the ST writer, if further types of information and/or security attributes for the TOE are needed, e.g. because the TOE has more interfaces to external entities than defined in this Protection Profile. If FDP_IFF.1.1/IF is extended for the use of additional interfaces to external entities FDP_IFF.1.2/IF must be extended too in order to counter new vulnerabilities which may occur due to these additional interfaces.

6.1.3.4. Static attribute initialisation (FMT_MSA.3)

The TOE shall meet the requirement “Static attribute initialisation (FMT_MSA.3)” as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3/IF Static attribute initialisation

FMT_MSA.3.1/IF	The TSF shall enforce the interface control SFP [44] to provide restrictive[45] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/IF	The TSF shall allow ~~the~~ none[46] to specify alternative initial values to override the default values when an object or information is created.

Application note 16: The default value of the security attribute “syntactical correctness” is “incorrect”. The default value of the security attribute “Verification status Update data” is “negatively verified”.

40 [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].
41 [assignment: *additional information flow control SFP rules*]
42 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
43 [assignment: *rules, based on security attributes, that explicitly deny information flows*]
44 [assignment: *access control SFP, information flow control SFP*]
45 [selection, choose one of: *restrictive, permissive,* [assignment: *other property*]]
46 [assignment: *the authorised identified roles*]

6.1.3.5. Security roles (FMT_SMR.1)

The TOE shall meet the requirement “Security roles (FMT_SMR.1)” as specified below ([CC part 2 v.3.1]).

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1/IF Security roles

FMT_SMR.1.1/IF	The TSF shall maintain the roles **1.** host computer, **2.** eID-Card, **3.** PIN Pad User, **4.** Update Provider, **5.** [assignment: *additional authorised identified roles*][47].
FMT_SMR.1.2/IF	The TSF shall be able to associate users with roles.

Application note 17: The ST author shall perform the open assignment in element FMT_SMR.1.1/IF. The assignment may be “none”.

6.1.3.6. User identification before any action (FIA_UID.2)

The TOE shall meet the requirement “User identification before any action (FIA_UID.2)” as specified below (Common Criteria Part 2).

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2 User identification before any action

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

Application note 18: Host computer, eID-Card and PIN Pad are identified by sending a message to the corresponding interface. The Update Provider is identified by the signature on update data corresponding to the Public key for update data verification stored in the TOE.

6.1.4. Integrity of the TOE

The objective OT.Integrity is served by the following SFRs.

6.1.4.1. Failure with preservation of secure state (FPT_FLS.1)

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: the integrity violation of the TSF data or parts of the TSF[48].

47 [assignment: *the authorised identified roles*]

Application note 19: The integrity violation of parts of the TSF and TSF data might be detected as an outcome of the TSF testing provided by FPT_TST.1.

6.1.4.2. TSF testing (FPT_TST.1)

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

Hierarchical to: No other components.

Dependencies: No Dependencies.

FPT_TST.1 TSF testing

FPT_TST.1.1	The TSF shall run a suite of self tests at the request of the authorized user and on receipt of the TOE [assignment: *other conditions under which self test should occur*][49] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data[50].
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *the TSF*].

Application note 20: The ST writer is requested to perform the open assignment. The authorized user is the End-User or any other user having access to the TOE. The TSF data include those data listed in 2.

6.1.4.3. Passive detection of physical attack (FPT_PHP.1)

The TOE shall meet the requirement “Passive detection of physical attack (FPT_PHP.1)” as specified below (Common Criteria Part 2).

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering 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 21: This SFR may be fulfilled by a seal or the TOE's case itself etc. which will be visibly hurt if the TOE's hardware has been opened.

6.2. Security Assurance Requirements for the TOE

The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 3 (EAL3) and augmented by taking the following components:

- ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 and AVA_VAN.3.

48 [assignment: *list of types of failures in the TSF*]

49 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

50 [selection: [assignment: *parts of TSF data*], *TSF data*]

The EAL3 was chosen to permit a manufacturer 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 manufacturers or users require a
580 moderate level of independently assured security and require a thorough investigation of the TOE and its development without substantial re-engineering.

The augmentation of AVA_VAN.3 is chosen because for all threats the attackers are assumed to have enhanced-basic attack potential.

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage.

	OT.Interfaces	OT.PACE	OT.Integrity	OT.Update	OT.Passwords	OT.SecretPass	OT.AccessRights	OT.FilterRules	OT.TerminalAuth
FCS_CKM.1/PACE		x							
FCS_CKM.4		x							
FCS_COP.1/AES		x							
FCS_COP.1/CMAC		x							
FCS_RNG.1		x							
FDP_RIP.1		x		x	x				
FIA_API.1		x				x			
FDP_IFC.1/PACE							x	x	
FDP_IFF.1/PACE							x	x	x
FMT_MSA.3/PACE							x	x	
FMT_SMR.1/PACE							x	x	
FIA_UID.2	x			x			x	x	
FPT_FLS.1			x						
FPT_PHP.1			x						
FPT_TST.1			x						
FCS_COP.1/Sig				x					
FDP_IFC.1/IF	x			x					
FDP_IFF.1/IF	x			x					
FMT_MSA.3/IF	x			x					
FMT_SMR.1/IF	x			x					
FDP_ITC.1	x			x					

Table 6: Coverage of Security Objective for the TOE by SFR

585 The security objective **OT.Interfaces** ”Interfaces of the TOE” is covered by FDP_ITC.1 enforcing the interface control SFP for data imported via one of the external interfaces of the TOE and enforcing imported data not to be interpreted as program code but as pure data except for update data. This SFP is described by FDP_IFC.1/IF in combination with FDP_IFF.1/IF. FMT_SMR.1/IF defines the roles needed for this information flow control and FMT_MSA.3/IF defines how the
590 security attributes and their values shall be initialised. All subjects in this context are identified as soon as they interact with TOE by the interface they use, therefore FIA_UID.2 gives no options before identification.

The security objective **OT.PACE** “PACE support” is enforced by FIA_API.1 describing the use of PACE. The ephemeral keys for the PACE protocol are generated by FCS_CKM.1/PACE and
595 securely deleted by FCS_CKM.4 while FDP_RIP.1 provides the deallocation of all instances of PIN representations possibly existing after the user has entered it. FCS_RNG.1 is used for generating the nonce needed for PACE protocol. PACE (and the subsequent secure communication channel) is realized by the cryptographic primitives required by FCS_COP.1/AES and FCS_COP.1/CMAC.

With the capability to test the integrity of TSF and TSF data (FPT_TST.1) the security objective
600 **OT.Integrity** “Verification of TOE integrity” is enforced. In case of a detected integrity violation the TOE has to enter a secure state (FPT_FLS.1). Additionally the manipulation of the hardware case of the TOE shall be easily detectable for the End-User (FPT_PHP.1).

The interface control SFP used for OT.Interfaces also covers the security objective **OT.Update** “Authenticity of Update data” by enforcing the verification of the signature over the Update data
605 generated by the TOE manufacturer and therefore the same SFRs are needed. Additionally FCS_COP.1/Sig contains the cryptographic specifications for the verification of the signature and FDP_RIP.1 enforces the deallocation of negatively verified Update data.

The security objective **OT.SecretPass** “**Keeping the passwords secret**” is enforced by the SFR FIA_API.1 which requires the TOE to use the inserted passwords only for PACE or PIN
610 management.

The security objective **OT.Password** “Password security” is enforced by the SFR FDP_RIP.1 which requires the TOE to ensure that any of these passwords contained in a resource has to be de-allocated immediately after usage in PACE protocol or for PIN management and will not be available when the resource is de-allocated.

615 The security objective **OT.AccessRights “**Final Access Rights” is enforced by FDP_IFF.1/PACE in combination with FDP_IFC.1/PACE defining the sequence of steps to be fulfilled before the information flow between remote terminal and eID-Card is allowed. This includes the forwarding of the unaltered Final Access Rights to the eID-Card, this is achieved by FMT_SMR.1/PACE defining the roles needed for this information flow control and FMT_MSA.3/PACE defines how the security
620 attributes and their values shall be initialised. All subjects in this context are identified as soon as they interact with TOE by the interface they use, therefore FIA_UID.2 gives no options before identification.

The PACE control SFP used for OT.AccessRights also covers the security objective **OT.FilterRules** “Accept passwords and execute PACE only on given rules” by defining and enforcing the rules to
625 be fulfilled before the information flow from and to the eID-Card starts.

The security objective **OT.TerminalAuth** “Forwarding the result of Terminal Authentication” is enforced by FDP_IFF.1/PACE by requiring the TOE to forward the result of Terminal Authentication executed by the eID-Card and the remote terminal unaltered to the host computer.

6.3.2. Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual
630 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.

Table 7 shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Fulfilment of Dependencies
FCS_CKM.1/PACE	[FCS_CKM.2, FCS_COP.1] FCS_CKM.4	FCS_COP.1/CMAC, FCS_COP.1/AES FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1]	FCS_CKM.1/PACE
FCS_COP.1/AES	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/PACE FCS_CKM.4
FCS_COP.1/CMAC	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/PACE FCS_CKM.4
FCS_COP.1/Sig	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	not fulfilled (cf. justification 1) not fulfilled (cf. justification 1)
FCS_RNG.1	no dep.	no dep.
FDP_IFC.1/PACE	FDP_IFF.1	FDP_IFF.1/ PACE
FDP_IFC.1/IF	FDP_IFF.1	FDP_IFF.1/IF
FDP_IFF.1/PACE	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/ PACE FMT_MSA.3/PACE
FDP_IFF.1/IF	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/IF FMT_MSA.3/IF
FDP_ITC.1	[FDP_ACC.1, FDP_IFC.1] FMT_MSA.3	FDP_IFC.1/IF FMT_MSA.3/IF
FDP_RIP.1	no dep.	no dep.
FIA_API.1	no dep.	no dep.
FIA_UID.2	no dep.	no dep.
FMT_MSA.3/PACE	FMT_MSA.1 FMT_SMR.1	cf. Justification 2 FMT_SMR.1/PACE
FMT_MSA.3/IF	FMT_MSA.1 FMT_SMR.1	cf. Justification 2 FMT_SMR.1/IF
FMT_SMR.1/PACE	FIA_UID.1	FIA_UID.2
FMT_SMR.1/IF	FIA_UID.1	FIA_UID.2
FPT_FLS.1	no dep.	no dep.
FPT_PHP.1	no dep.	no dep.
FPT_TST.1	no dep.	no dep.

Table 7: Dependencies between the SFR for the TOE

Justification 1: Since iteration FCS_COP.1/Sig only performs public key operations with internal
635 TSF data for signature verification and the key used for update data verification is internal TSF data (cf. chapter 3.1, table 2), thus there is no need for key generation, import or deletion.

Justification 2: Because roles and security attributes shall be only modified by the TOE there is no

management function for the TOE administrator foreseen.

6.3.3. Security Assurance Requirements Rationale

The EAL3 including all chosen augmentations permits a manufacturer to gain maximum assurance
640 from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. The selection of the component **AVA_VAN.3** provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a enhanced-basic attack potential.

645 All dependencies resulting directly or indirectly from the augmentation AVA_VAN.3 are discussed in the following

The component **AVA_VAN.3** has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.4 Complete functional specification
650 – ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design

655 Except for ADV_FSP.4, ADV_TDS.3 and ADV_IMP.1 all these requirements are met or exceeded in the EAL3 assurance package.

The component **ADV_FSP.4** has the following dependencies:

- ADV_TDS.1 Basic Design

ADV_TDS.3 of the chosen augmentation is hierarchical to ADV_TDS.1.

660 The component **ADV_TDS.3** has the following dependencies:

- ADV_FSP.4 Complete functional specification

ADV_FSP.4 is not part of the chosen EAL3 assurance level but is met by the chosen augmentation.

The component **ADV_IMP.1** has the following dependencies:

- ADV_TDS.3 Basic modular design
665 – ALC_TAT.1 Well-defined development tools

ADV_TDS.3 and ALC_TAT.1 are not part of the chosen EAL3 assurance level but are met by the chosen augmentation.

The component **ALC_TAT.1** has the following dependencies:

- ADV_IMP.1 Implementation representation of the TSF

670 ADV_IMP.1 is not part of the chosen EAL3 assurance level but is met by the chosen augmentation.

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

675 consistency demonstrates:

The dependency analysis in section 6.3.2 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.

680 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.

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

7. Glossary and Acronyms

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.
Card verifiable certificate	Certificate according to ISO 7816 and [TR-03110] which is verifiable by the eID-Card and the TOE
PACE passwords	The passwords of the eID-Card holder used to authenticate themselves to the eID-Card. The PACE password can either be PIN, PUK or CAN, refer to [TR-03110] and [TR-03127]. This includes the current PIN and the PIN which is given to the TOE in order to set it as new one during PIN-Management.
password	Any password given to the TOE, including the PACE passwords.
Proximity Coupling Device	Smart card interface device used for contactless cards.
Secure Messaging	Secure Messaging (cf. [ISO7816-4])
Terminal authentication	Authentication of external entities to the eID-Card as defined in [TR-03110]
TSF data	Data created by and for the TOE that might affect the operation of the TOE ([CC part 1 v.3.1]).
User data	Data created by and for the user that does not affect the operation of the TSF ([CC part 1 v.3.1]).

Table 8: Glossary

Acronym	Term
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CAN	Card Access Number (cf. [TR-03110])
CC	Common Criteria
CHAT	Certificate Holder Authorization Template (cf. [TR-03110])
CVC	Card verifiable certificate (cf. [TR-03110])
EAC	Extended Access Control (cf. [TR-03110])
EAL	Evaluation Assurance Level
eID	Electronic Identity
nPA	Electronic Identity Card (German: elektronischer Personalausweis)
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment, (cf. [TR-03110])
PCD	Proximity Coupling Device
PIN	Personal Identification Number (cf. [TR-03110])

Acronym	Term
PP	Protection Profile
PUK	PIN Unblocking Key (cf. [TR-03110])
SAR	Security assurance requirements
SFR	Security functional requirement
ST	Security Target
TA	Terminal Authentication, (cf. [TR-03110])
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 9: List of Acronyms

8. Literature

[CC part 3 v.3.1]: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[CC part 2 v.3.1]: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[CC part 1 v.3.1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[CC eval. meth. v.3.1]: Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[TR-02102]: Bundesamt für Sicherheit in der Informationstechnik, BSI-TR-02102 Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, version 1.0, 2008

[TR-03111]: Bundesamt für Sicherheit in der Informationstechnik, BSI-TR-03111, Elliptic Curve Cryptography, version 1.11, 17.04.2009

[TR-03127]: Bundesamt für Sicherheit in der Informationstechnik, BSI-TR-03127, Technische Richtlinie Architektur Elektronischer Personalausweis, version 1.14, 27.05.2011

[TR-03110]: Bundesamt für Sicherheit in der Informationstechnik, BSI-TR-03110-2 Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), version 2.10, 20.03.2013

[TR-03119]: Bundesamt für Sicherheit in der Informationstechnik, BSI-TR-03119, Technical Guideline BSI TR-03119Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control, version 1.3, March 2013

[ISO7816-4]: International Organization for Standardization, ISO/IEC 7816-4, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, version , 2005

[ISO 14443]: ISO/IEC, ISO 14443 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards,

[RFC4493]: JH. Song et al. University of Washington, Category: Informational, RFC 4493, The AES-CMAC Algorithm , version , June 2006

[PKCS#3]: RSA Laboratories, PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note , version 1.4, 01.11.1993 (Revised)

[NIST_800_38B]: U.S. Department of Commerce / National Institute of Standards and Technology, NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication , version , May 2005

[FIBS_PUB_197]: U.S. Department of Commerce / National Institute of Standards and Technology, Federal Information Processing Standards Publication FIPS PUB 197, Advanced Encryption Standard (AES), version , 26.11.2001

[AIS20/31]: Wolfgang Killmann, T-Systems; Werner Schindler, BSI, A proposal for:Functionality classes for random number generators, version 2.0, September 2011

[PAuswG]: Gesetz über den Personalausweis und den elektronischen Identitätsnachweis(Personalausweisgesetz)