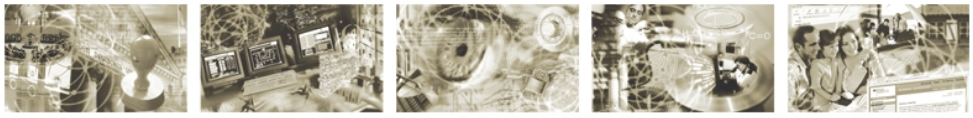
Bundesamt
für Sicherheit in der
Informationstechnik



Common Criteria Protection Profile
eID-Client based on eCard-API

Common Criteria

BSI-CC-PP-0066-V2

Foreword

This ‘Protection Profile — eID-Client based on eCard-API’ 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 3 [1], [2], [3].

Correspondence and comments to this PP eID-Client 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

1. PP Introduction

1.1. PP reference

Title:	Protection Profile — eID-Client based on eCard-API
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1 (Revision 3)
Assurance Level:	The assurance level for this PP is EAL3 augmented.
General Status:	Final
Version Number:	2.0.5.14
Date	01.12.2011
Registration:	BSI-CC-PP-0066-V2
Keywords:	eCard-API-Framework, eID, EAC, PACE, nPA

1.2. TOE Overview

The protection profile defines the security objectives and requirements for an application implementing the client side of the eCard-API Framework [4] with respect to the eID-Application, called "eID-Client" in the following and a corresponding Browser-Plugin.

The eID-Client is placed at the citizen's disposal on a personal computer. It allows utilizing eID-Cards compliant to TR-03110 [5], e.g. the new German electronic Identity Card (German: neuer Personalausweis, nPA) as it is based on the eCard-API Framework. This Framework provides all necessary interfaces for a so called middle-ware component allowing different PC applications and remote server (e.g. electronic identification (eID), applications for the electronic Health Card, Signature Creation Applications) to access different card applications in a unified way. The eID-Client provides interfaces for the eCard-Holder as user, the eService via Browser-Plugin, the eID-Server and the eID-Card via an IFD and acts therefore as middle-ware between these parties. The corresponding Browser-Plugin is needed to forward messages from the eService to the eID-Client and vice versa.

The TOE consists of the eID-Client itself and the security relevant parts of the Browser-Plugin corresponding to the eID-Client (see Figure 1).

The evaluation assurance level (EAL) for the eID-Client is chosen to be EAL3 augmented by AVA_VAN.3 (and all resulting dependencies). Furthermore the EAL is augmented by the component ALC_FLR.1. For details cf. to sec. 2.3 and 6.2.

1.2.1. TOE Type definition

The Target of Evaluation (TOE) is the eID-Client comprising an eCard-API-Framework BSI-TR-03112 (cf. [4]) based middle-ware component and the corresponding Browser-Plugin with respect to the security functionality

- implementing the terminal part of PACE in accordance to TR-03110 [5],
- checking the signatures of the CVC and the consistency of the X.509 certificates contained in the CVC extension with the certificates used for the TLS-Channels
- providing the possibility to securely display the CVC information completely and unaltered to the End-User
- providing the possibility to restrict the access rights contained in the CVC and forward those restricted rights unaltered to the eID-Card
- protecting the passwords given to the TOE
- performing secure updates provided by the TOE issuer

The eID-Server also based on the 'eCard-API-Framework, BSI TR-03112' is no TOE component with respect to this protection profile.

The TOE supports the usage of the eID-Application on the eID-Card (cf. [6]) by a third party system, e.g. a remote eID-Server. The TOE supports

- the Chip Authentication of the eID-Card to the third party system,
- the Terminal Authentication of the third party system to the eID-Card and
- PIN-Management for the eID-Card

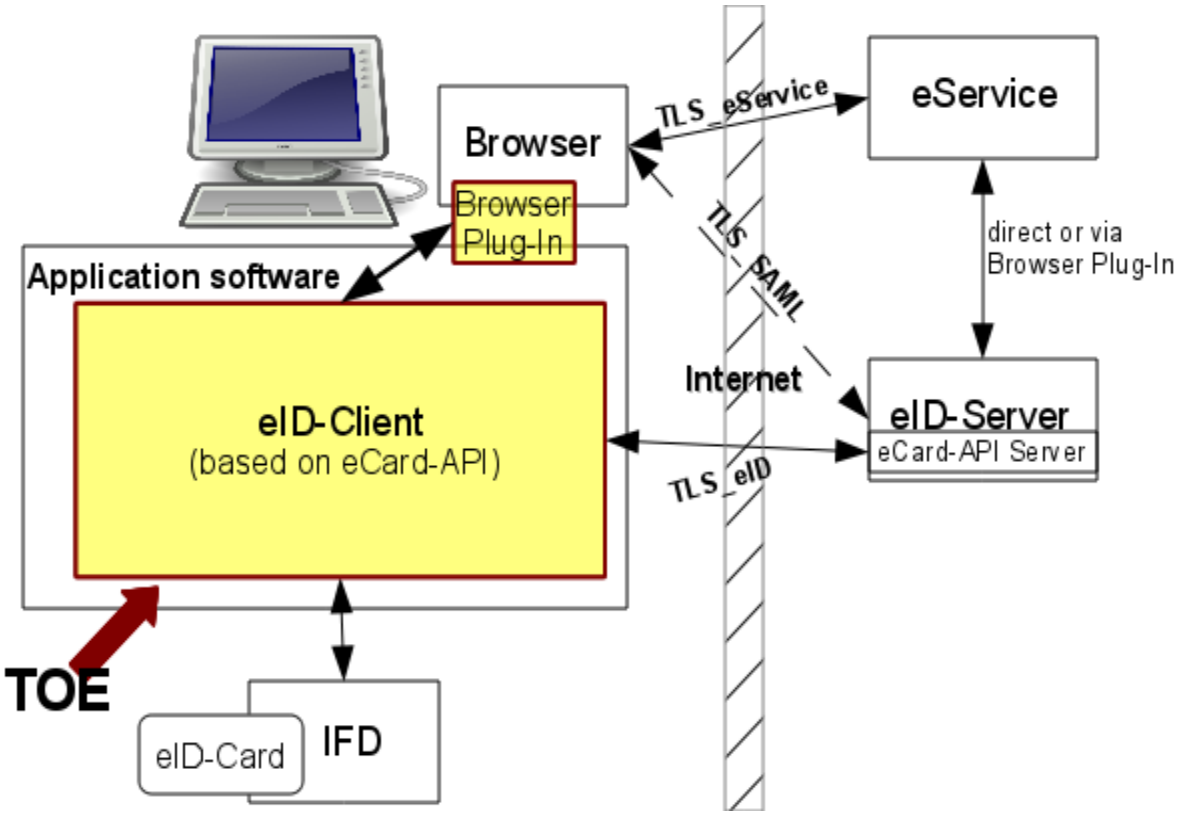


Figure 1: Illustration of the TOE Boundaries

The TOE supports the citizen to perform an Online Authentication (cf. [6], chapter 4.7 and [7], chapter 2.4.2) as illustrated in Figure 1. The eService provides a web-based application which needs reliable identification of the eID-Card holder. The card holder as a costumer of the eService wants to identify himself/herself using the eID-Card.

The eService provider operates an eID-Server which performs the server part of the Online Authentication. The eService provider may delegate the operation of the eID-Server to a third party. In all cases a secure communication channel between eService and eID-Server is assumed to exist. This channel may either be a direct communication link or a secure link which is mediated by the browser (the latter if SAML is used for communication between eService and eID-Server, cf. TR-03130 [7]).

Both the eService and the eID-Server are equipped with X.509 certificates for the establishment of TLS-Channels. These certificates are linked to the CV certificate (CVC) used for Terminal Authentication (cf. [6] 5.2.1 and [5] C.3.1).

The Online Authentication is performed as follows (cf.[6], chapter 4.7 and [7], chapter 2.4.2):

- The card holder communicates with the eService using the browser of his or her personal computer. In order to protect this communication the browser and the eService establish a TLS channel TLS_eService using the X.509 certificate of the eService (called eService-Certificate

in the following) linked to the CVC used for Terminal Authentication, which is transmitted as part of the next step. The eService requests reliable identification of the citizen by means of his or her eID-Card. The eService informs the eID-Server about this authentication request via the secure communication channel between eService and eID-Server. If this channel is mediated by the browser, the browser communicates to the eID-Server via a TLS-Channel TLS_SAML.

- The eService (or the eID-Server in the case of usage of SAML) sends a request to access the eID-Card of the citizen and a pre-shared key PSK to the browser, which redirects this request to the TOE. The TOE establishes a TLS channel TLS_eID to the eID-Server using the pre-shared key PSK. The TOE receives the CVC for Terminal Authentication owned by the eService and used by the eID-Server via TLS_eID.

- The TOE informs the citizen about the request to access the eID-Card and the communication context of this request, i.e.

  i. information about the holder of the CVC for Terminal Authentication (i.e. the eService) to be used to get access to eID-Card,

  ii. the access right the eID-Server wants to gain after successful Terminal Authentication to the eID-Card, and

  iii. the result of the consistency check between the eService-Certificate used by eService for TLS_eService, the X.509 certificate used by the eID-Server for TLS_eID (called eID-Server-Certificate in the following) and the CVC to be used for Terminal Authentication. In the case of mediated communication between eService and eID-Server, the X.509 certificate used to establish TLS_SAML (called SAML-Certificate in the following) is also part of this consistency check.

- The TOE enables the card holder to reduce the requested access rights. If the card holder accepts this request or the request with reduced access rights he or she continues by authenticating himself/herself to the eID-Card as card holder using his secret PIN. If an IFD without secure PIN entry is used, the TOE performs PACE and sends the reduced access rights to the eID-Card. If an IFD with secure PIN entry is used, the reduced access rights are forwarded to the IFD and PACE is performed by the IFD. If the IFD with secure PIN entry should be able to display the access rights too nevertheless the access rights must be displayed and handled by the TOE as described in the sentences before.

- The eID-Server and the eID-Card perform Terminal Authentication (authentication of the eID-Server to the card) and Chip Authentication (authentication of the card to the eID-Server and establishing a secure channel between card and eID-Server) according to BSI TR-03110 [5] in order to authenticate each other. They are supported by the TOE, which mediates the communication between these entities. The TOE

  i. ensures that the CVC used during Terminal Authentication is the same as the one displayed to the card holder

  ii. displays the result of the Terminal Authentication and Chip Authentication to the card

holder.

- The TOE provides access for the eID-Server through the TLS channel TLS_eID, the operating system of the personal computer and the IFD to the eID-Card. After reading the personal data of the eID-Card in the limits of the access rights gained the eID-Server forwards these data via the secure communication channel to the eService, concluding the Online Authentication.

Furthermore, the TOE enables the citizen to

- change the PIN of his eID-Card after authentication of the card holder using the current PIN, and to

- unblock the PIN of his eID-Card using the PIN Unblocking Key (PUK).

1.2.2. TOE usage and security features

From a technical view, the TOE is a product that is intended to be used as a stand-alone application as well as to be integrated into third party applications requiring authentication services.

The TOE complies with the Technical Guideline BSI TR-03112 "eCard-API-Framework" (cf. [4]). The eCard-API-Framework intends to provide a simplified, platform independent and unified interface for different smart cards and card application types. The card dependent information may be provided in card-info-files (CIF). An IFD-List may be used in order to list all compliant IFDs.

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 [5] if a card terminal (IFD) without secure PIN entry is used and protects the passwords given to the TOE. The TOE also supports the usage of a card terminal with secure PIN entry (e.g. PIN-Pad). The card terminals shall comply to BSI TR-03119 [8]. The TOE may support further card terminals not conforming to TR-03119.

Support for Online Authentication

The TOE supports an EAC compliant Online Authentication by the eID-Server running Terminal Authentication and Chip Authentication in accordance to BSI TR-03110 [5] and BSI TR-03130 [7]. The TOE provides an user interface for performing Online Authentication in context of eID-Applications in order

(i.) to identify the X.509 certificates used by the browser for the communication with the eService and the eID-Server,

(ii.) to verify the CVC used by the eID-Server for Terminal Authentication,

(iii.) to verify the link between the CVC and the X.509 certificates of the eService and the eID-Server,

150 (iv.) unambiguously display the content of the CVC and the corresponding extension,

(v.) to unambiguously display the rights the eID-Server given in the CVC and the eID-Server wants to use for access to the eID-Card, and

(vi.) communicating a user demanded restriction of these access rights unaltered to the eID-Card.

TOE Integrity Verification

155 The TOE is capable to validate its integrity on demand. The TOE is capable to detect unauthorized manipulations of the TOE itself. In case of a detected manipulation the TOE disables its external interfaces.

TOE Updates

Updates may be made for example by download on demand or the TOE asks its issuer regularly for
160 Updates. In both cases 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 on a user client (personal computer) with an operating system and a browser 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
165 persons. This also includes mobile devices. 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.

Operating System

170 Supported operating systems have to be listed by the ST writer. Only operating systems still supported by the OS vendor shall be used.

eID-Card

The TOE supports eID-Cards compliant to BSI TR-03110 [5].

Card Terminals

175 The TOE supports at least card terminals (IFDs) compliant to BSI TR-03119 [8].

Supported browser programs

Supported internet browsers have to be listed by the ST writer. Only browsers still supported by the vendor shall be used. The TOE's implementation, specifically any Browser-Plugins that are part of the TOE, shall not be affected by potentially installed pop-up-blockers.

2. Conformance Claims

2.1. CC Conformance Claim

180 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]

185
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

as follows

- Part 2 extended,
- Part 3 conformant.

190 The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009, [9]

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

195 This PP is conforming to assurance package EAL3 augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_FLR.1, ALC_TAT.1 and AVA_VAN.3 defined in CC part 3 [3].

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

200 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
passwords	The passwords of the eID-Card holder used to authenticate themselves to the eID-Card. The password can either be PIN, PUK or CAN, refer to [5], [6], 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. This asset comprises only passwords submitted to the TOE as long as they are in the domain of the TOE. If PIN-Management is executed by the IFD the passwords are not assets of the TOE.	confidentiality and integrity
Authentication Results[1]	The result of the Terminal Authentication and the result of the consistency check between the eService-Certificate, the eID-Server-Certificate and the CVC to be used for Terminal Authentication.	integrity
Communication Data (CD)	Communication Data are all data exchanged between the TOE and the eService and between the TOE and the eID-Server. Personal data (see below) are not part of the Communication Data.	confidentiality and integrity
CVC data	i. information about the holder of the CVC for Terminal Authentication (i.e. the eService) to be used to get access to eID-Card, ii. the access rights the eID-Server wants to gain after successful Terminal Authentication to the eID-Card (CVC Access Rights)	integrity
CVC Access Rights (part of CVC data)	the access rights the eID-Server wants to gain after successful Terminal Authentication to the eID-Card defined in the CertificateHolderAuthorizationTemplate of the CVC.	integrity
Final Access Rights	CVC Access Rights requested with the presented CVC reduced and/or accepted by the End-User as long as they are in the domain of the TOE.	integrity

[1] The results of the PACE authentication are not part of the assets because there is no security functionality of the eID-PIN verification concerning the TOE. The PIN verification and any rights depending on its result are totally managed by the eID-Card.

Pre-Shared Key	The Pre-Shared Key (PSK) is sent by the eService (or the eID-Server in the case of usage of SAML) to the Internet Browser, imported from there by the TOE The purpose of the Pre-Shared Key is to establish the TLS channel with the eID-Server. The integrity and confidentiality of the Pre-Shared Key have to be protected by the TOE.	integrity and confidentiality
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 stored on the eID-Card (e.g. birth date). Please note that personal data will never be processed by the TOE and only
205 personal data encrypted by the eID-Card will be forwarded by the TOE to the eID-Server. 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 CVC verification (CVCA trust anchor)	The public key of the root CV certificate is generated by the issuer of the eID-Card and provided to the TOE vendor in a secure way. This public key is trusted. This public key is used for verification of digital signatures in the CV certificates used for Terminal Authentication. The protection of the integrity ensures the correct functionality resp. behaviour of the TOE.	Authenticity, integrity
Public key for update data verification	This public key is used for verification of data of the developer intended for use for TOE updates. The protection of the integrity ensures the correct functionality resp. behaviour of the TOE. This public is generated by the TOE vendor in a secure way and part of the TOE internal data. This public key is trusted.	Authenticity, integrity

table 2: List of TSF data

User

The TOE defined in this protection profile is capable to identify the following users. This PP does
210 not differentiate in the terminology between the user and the subject acting for this user.

End-User

Any human entity having direct (physical) access to the TOE platform and especially to the human user interfaces of the TOE (e.g. GUI, Secure Viewer, etc.) and of the IFD is identified as End-User.

Note that the End-Users are local (human) Users.

eID-Card holder

The eID-Card holder is a local End-User (i.e. End-User with the security attribute Localization "local"). The eID-Card holder is identified by holding the eID-Card and knowing (and entering) the password corresponding to the eID-Card. Note, that an authentication is carried out against the eID-Card and not against the TOE itself.

Technical User

Any technical entity (e.g. PC application, browser etc.) having access to the TOE platform is identified as Technical User. Note that there are local Technical Users (i.e. Technical User with the security attribute Localization "local") having direct access to eCard-API and remote Technical Users (i.e. Technical Users with the security attribute Localization "remote") interacting with the TOE via a TLS channel.

Browser

The internet browser is used by the End-User to communicate with the eService. It is a local technical user directly communicating with the Browser-Plugin of the TOE.

eID-Server

The eID-Server is a remote server system acting as an internet based authentication terminal implementing Extended Access Control in accordance to the BSI TR-03110 [5] and communicating in accordance with BSI TR-03130 [7]. The eID-Server has to be successfully authenticated to the TOE by using TLS.

IFD

IFDs are card interface devices used by the TOE connecting to the eID-Card. The TOE supports usage of interface devices compliant to BSI TR-03119 [8].

Note: Since the TOE (especially the eCard-API-Framework part) does not support an authentication of local Technical Users, the local interface can be used by any local entity having access to the TOE platform.

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.Server-Com	**Manipulation or disclosure of Server Communication**
Asset:	Communication Data transmitted between the TOE and the eID-Server.
Security goal:	The integrity and confidentiality of the asset.

	Adverse action:	Sensitive data are manipulated or disclosed during the transmission between the TOE and the eID-Server. The manipulation can be systematic or random by the means of interception, eavesdropping, replay or manipulation.
250	Attacker:	The attacker has access to the communication channel between the TOE and the eID-Server. He is assumed to have enhanced-basic attack potential.
	T.Malware	**Insertion of Malware into or through the TOE**
	Assets:	The TOE and therefore all assets of the TOE
255	Security goal:	The integrity of the assets.
	Adverse action:	Insertion of Malware via one of the following communication interfaces[2]: IFD-Interface (including card), Browser-Interface (interface between Browser-Plugin and Browser), Update-Interface, eID-Server-Interface
260	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.eID-PIN[3]	**Compromise of the eID-PIN, CAN or eID-PUK**
	Assets:	The eID-PIN, eID-PUK and CAN
	Security goal:	The confidentiality of the assets.
265	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.ManDisplaying	**Manipulation of Authentication data or results displayed to the user**
270	Assets:	CVC data, CVC Access Rights, Final Access Rights, Authentication Results
	Security goal:	The integrity of the assets.
	Adverse action:	The attacker manipulates or reduces the representations of CVC data, CVC Access Rights, Final Access Rights or Authentication Results (see chapter 3.1) which shall be displayed to the user.[4]
275	Attacker:	The attacker has access to one of the communication interfaces of the

2 The underlying operating system is assumed not to insert malware, see A.Platform
3 This threat is only relevant if no IFD with secure PIN-Entry is used
4 The TOE shall enable the End-User to get these data displayed even if the IFD can display those data itself.

TOE. He is assumed to have enhanced-basic attack potential.

T.FinalAccessRights **Manipulation of the Final Access Rights**

Asset: Final Access Rights

Security goal: The integrity of the asset.

280 Adverse action: The CVC Access Rights reduced and/or accepted by the user are manipulated before or during the transmission to the IFD-Interface as long as they are in the domain 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

3.3. Organizational Security Policies

285 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 [1], sec. 3.2).

P.ServerCheck **Checking of server data**

The TOE shall verify the signature of the CVC sent by the eID-Server using the public key for CVC
290 verification stored in the TOE. Additionally the TOE has to compare the hashes of the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate with the corresponding values from the CVC. The TOE must make the information about the eService gained from the CVC (cf. BSI TR-03110 [5]) available to the user.

P.AccessRights **Handling CVC Access Rights**

295 The TOE shall display the CVC Access Rights of the eID-Server gained from the CVC to the eID-Card holder. The TOE must enable the eID-Card holder to restrict those CVC Access Rights to get his Final Access Rights before PIN entry. The TOE must send the Final Access Rights to the eID-Card during PACE protocol (cf. BSI TR-03110 [5]).

P.PACE **Password Authenticated Connection Establishment support**

300 The TOE shall support the eID-Card holder to authenticate themselves to the eID-Card with the eID-PIN or another password (PUK, CAN) and establishing a trusted channel to the eID-Card using the PACE protocol in accordance with BSI TR-03110 [5]. If the End-User uses a IFD without secure PIN entry (cf. BSI TR-03119 [8]) the passwords are provided by the client platform (e.g. the user enters the PIN through the keyboard) and the TOE shall perform the terminal part of the PACE
305 protocol. If the End-User uses a IFD with secure PIN entry (cf. BSI TR-03119 [8]) the End-User shall enter the PIN or password directly on this IFD implementing the terminal part of the PACE protocol. The TOE waits for the response of the eID-Card about success or failure of the authentication attempt forwarded by the IFD.

P.Integrity Integrity verification of parts of the TOE

310 The TOE shall enable the End-User to verify the integrity of the TOE or parts of the TOE. This policy intends to allow the integrity verification directly on receipt of the TOE or parts of the TOE (e.g. updates, etc.) directly after delivery or installation procedure or on demand at any later point in time. This verification of integrity shall also include the TSF data as there are the Public key for CVC verification and the Public key for update data verification. Only authentic data signed by the
315 developer shall be installed.

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 personnel

The End-Users of the product are trustworthy and follow the instructions of the user guidance
320 delivered with the TOE. The End-User verifies regularly the integrity of the TOE. The eID-Card holder knows and protects the passwords for authentication to the eID-Card.

A.Platform Underlying platform

The TOE is installed on a personal computer[5] located in an admission restricted area (e.g. domestic area or company area) or under constant supervision by the End-User (e.g. a cell phone carried by
325 the user) ensuring that those resources the TOE is relying on (inclusive. the browser) cannot be manipulated without user notification. The End-user implements security measures protecting the integrity of the platform against logical attacks by Malware.

A.IFD Interface Devices

If an IFD with secure PIN-Entry according to BSI TR-03119 [8] is used it is assumed to neither
330 compromise the eID-PIN, CAN or PUK nor to manipulate the Final Access Rights.

A.Cert Certificates

The issuer of the eID-Server CVC encodes the CVC Access Rights defined for the eService and links of the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate . The CVC issuer ensures the validity and correct identification of the certificate holder
335 in the X.509 certificates linked by the hash value mechanism.

A.Browser Browser support

The browser supports the export to the TOE of the eService-Certificate and, if applicable, the SAML-Certificate.

5 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. This also includes mobile devices.

A.eService eService

340 The eService communicates with the Browser through TLS channel authenticated by a X.509 certificate (eService-Certificate) linked to the CVC certificate used by the eID-Server.

A.Browser-Plugin Browser-Plugin and eCard-API client

Only eCard-API client software and Browser-Plugin software (as parts of the TOE) belonging together are installed on the underlying platform.

4. Security Objectives

345 This chapter describes the security objectives for the TOE and the security objectives for the TOE 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.Com-Sec Communication security

350 The TOE shall establish TLS communication channel protecting confidentiality and integrity of the Communication Data exchanged between eID-Server and TOE. The TOE shall use the pre-shared key gained via TLS channel between Browser and eService from the eService for the communication with the eID-Server. The TOE shall restrict the access to the eID-Card of remote Technical Users to successful authenticated eID-Server.

355 **OT.Com-Check Communication check**

The TOE shall verify the signatures of the CVC using the public key for CVC verification of the TOE. The TOE shall display the content of the CVC extension according to BSI TR-03110 [5] and BSI TR-03127 [6][6] and the validity time frame of the CVC. The TOE shall import from the browser the eService-Certificate and, if applicable, the SAML-Certificate and the TOE shall import the eID-
360 Server-Certificate. The TOE shall generate hashes of all these X.509 certificates and compare them to the corresponding hashes gained from the CVC extension according to [5]. In case of mismatch in the links the TOE shall display a suitable error message to the End-User and abort the Online Authentication.

OT.Interfaces Interfaces of the TOE

365 The TOE shall only accept incoming messages which are syntactically correct according to the corresponding technical guideline on the following interfaces:

1. IFD-Interface (including card), which shall receive messages according to [8]
2. Browser-Interface (interface between Browser-Plugin and Browser), which shall receive messages according to [4], part 7.
370 3. eID-Server-Interface, which shall receive messages according to [4], part 7 and part 4.

The TOE shall ensure that data contained in those messages is never executed as program code.

[6] [5] Describes how to process the CVC and which data it can contain while [6] sets the requirements which data at least have to be displayed to the End-User

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
375 with BSI TR-03110 [5]. Therefore the TOE shall implement the terminal part of the PACE protocol in accordance with BSI TR-03110 [5] if the End-User uses an IFD without secure PIN entry (cf. BSI TR-03119 [8]) and the PIN or password is provided by the client platform (e.g. the user enters the PIN through the keyboard) [8]. If the End-User uses a IFD with secure PIN entry (cf. BSI TR-03119 [8]) the End-User shall enter the PIN or password directly on this IFD implementing the terminal
380 part of the PACE protocol. The TOE waits for the response of the eID-Card about success or failure of the authentication attempt forwarded by the IFD.

OT.Integrity Verification of TOE integrity

The TOE provides mechanisms to enable End-User to verify the integrity of the TOE on receipt of the TOE and of the TOE parts installed on the platform on demand. This verification of integrity
385 shall also include the TSF data as there are the Public key for CVC verification and the Public key for update data verification. In case of detected integrity violation the TOE shall enter a secure state.

OT.Update Authenticity of Update data

The TOE shall verify the authenticity of data received on the Update-Interface as Update data signed by the developer and discharge data detected as not being authentic.

390 **OT.Password Password security**

The TOE shall ensure the confidentiality of any password given to the TOE. 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 [5] or PIN-Management according to [5]. The PUK and CAN shall only be used for PIN-Management according to [5]. Any password given to the TOE shall be overwritten by the TOE
395 when it is not longer needed for its purpose.

OT.Pre-SharedKey Usage of Pre-Shared Key

The TOE shall ensure the confidentiality of the Pre-Shared Key generated by the eService and sent to the TOE via TLS_eService and the Internet Browser as long as the Pre-Shared Key is in the domain of the TOE. The Pre-Shared Key shall be used for communication with the eID-Server.

400 **OT.SecureDisplay Display of the CVC and authentication information**

The TOE shall ensure that the following information can be displayed completely and unaltered to the End-User according to BSI TR-03127 [6] on his or her choice[7]:

i. CVC data according to chapter 3.1,

ii. the result of the consistency check between the eService-Certificate, the eID-Server-
405 Certificate and the CVC to be used for Terminal Authentication. In the case of

7 The TOE shall enable the End-User to get these data displayed even if the IFD could display resp. displays those data too. Therefore this objective is relevant regardless of which IFD type is used.

mediated communication between eService and eID-Server, the SAML-Certificate is also part of this consistency check,

iii. the results of Terminal Authentication, and,

iv. the Final Access Rights as defined by the End-User.

410 **OT.FinalAccessRights Final Access Rights**

The TOE shall enable the End-User to restrict the CVC Access Rights gained from the CVC or accept them unaltered in order to generate Final Access Rights before password entry. The TOE shall protect the integrity of the Final Access Rights as long as they are in the domain of the TOE and forward them unaltered to the IFD (see chapter 1.2.1).

4.2. Security Objectives for the Operational Environment

415 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 regularly the integrity of the TOE and download
420 and install the Updates provided by the TOE vendor. Additionally the eID-Card holder has to ensure the confidentiality of the passwords used for authentication to the eID-Card.

OE.Platform Underlying platform

The TOE is installed on a platform located in an admission restricted area or under constant supervision by the End-User ensuring that those resources the TOE is relying on (inclusive. the
425 browser) cannot be manipulated without user notification. The platform is configured to be used with protection mechanisms to avoid unauthorized modification. The client platform is protected against viruses, other Malware and attacks from network connections. The client platform is assumed not to harm the confidentiality and integrity of the eID-PIN or password if entered through the keyboard and provided to the TOE.

430 **Application note 2:** In order to maintain this security objective the web browser used with this platform it is recommended not to allow execution of program code on the user's platform retrieved from websites (active content) unless the TOE, the eService and the eID-Server are operated in one private network under full control of a trusted administrator.

OE.IFD Smart card interface devices

435 An IFD with secure PIN-Entry and display for CVC Access Rights according to BSI TR-03119 [8] shall neither compromise the eID-PIN or PUK or CAN nor manipulate the Final Access Rights.

OE.Browser Browser support

The browser running on the client platform of the user shall communicate through TLS channels

with the eService and (if applicable) the eID-Server. The browser supports the export of the eService-Certificate and the SAML-Certificate. .

OE.eService eService

The eService shall communicate with the Browser through TLS channel authenticated by a X.509 certificate (eService-Certificate) linked to the CVC certificate used by the eID-Server as required by [7].

OE.eID-Server eID-Server

The eID-Server communicates with the TOE through a TLS channel using a X.509 certificate, the eID-Server-Certificate, linked to the CVC certificate used by the eID-Server and the pre-shared key gained from the eService.

OE.Cert CVC issuer

The issuer of the eID-Server CVC encodes the CVC Access Rights defined for the eService and links of the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate. The CVC issuer ensures the validity and correct identification of the certificate holder in the X.509 certificates linked by the hash value mechanism.

OE.Update Updates

The developer shall provide updates of the TOE. The data provided for the download shall be signed by the developer.

Application note 3: If the ST writer decides to include security for Updates by checking the authenticity of the Update server, the ST writer must include adequate Security Objectives for the TOE and corresponding SFRs in order to check the authenticity of the connected Update server and protect the associated trust anchor.

OE.CurrentDate Current date

The Operating System provides a reasonable accurate source of the current time to support the check of the validity period of certificates performed by the TOE.

OE.Browser-Plugin Browser-Plugin and eCard-API client

Only eCard-API client software and Browser-Plugin software (as parts of the TOE) belonging together are installed on the underlying platform.

4.3. Security Objective Rationale

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

	OT.Com-Sec	OT.Interfaces	OT.Com-Check	OT.PACE	OT.Integrity	OT.Update	OT.Password	OT.Pre-SharedKey	OT.SecureDisplay	OT.FinalAccessRights	OE.End-User	OE.Platform	OE.Browser	OE.IFD	OE.Cert	OE.Update	OE.eService	OE.eID-Server	OE.CurrentDate	OE.Browser-Plugin
T.Server-Com	x							x										x		
T.Malware		x			x	x					x					x			x	x
T.eID-PIN							x					x		x						
T.ManDisplaying									x											
T.FinalAccessRights									x	x		x		x						
P.ServerCheck			x																x	
P.AccessRights									x	x										
P.PACE				x																
P.Integrity					x	x										x				
A.End-User											x									
A.Platform												x								
A.Browser													x							
A.IFD														x						
A.Cert															x					
A.eService																	x			
A.Browser-Plugin																				x

table 3: Security Objective Rationale

The threat **T.Server-Com** "Manipulation or disclosure of Server Communication" is directly addressed by the objective **OT.Com-Sec** requiring the TOE to protect the confidentiality and integrity of Communication Data transferred between the TOE and an eID-Server and **OT.Pre-SharedKey** requiring the TOE to protect the Pre-Shared Key gained out of the communication with the eService and to use it for communication with the eID-Server. The security objectives for the operational environment **OE.eID-Server** requires the eID-Server to use TLS-Channels for communication with the TOE.

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, OE.CurrentDate, OE.Browser-Plugin and OE.End-User. The objective **OT.Interfaces** requires the TOE to only accept syntactically correct messages according to the corresponding technical guidelines on the interfaces to the IFD, the eID-Server and the Browser and to never execute data contained in these messages as program code. The objective for the environment

OE.Browser-Plugin requires the user to install only eCard-API client and Browser-Plugin software belonging together in order to have a defined communication link with each other. The objective **OT.Update** requires the TOE to verify the updates and de-allocate negatively verified data received on the Update-Interface. The security objective for the operational environment **OE.Update** requires the developer of the TOE to provide signed updates for the TOE and **OE.CurrentDate** requires the operating systems to provide the current date needed for signature verification of the update. The objective **OE.End-User** requires the End-User to perform regularly integrity checks of the TOE and download and install Updates provided by the vendor as required in **OE.Update**. The objective **OT.Integrity** requires the TOE to verify itself.

The threat **T.eID-PIN** "Compromise of the eID-PIN, CAN or eID-PUK" is directly addressed by the objective **OT.Password** which requires the TOE to protect the passwords, overwrite them after usage in the TOE and only use them for PACE or PIN-Management. The objective **OE.Platform** requires the platform where TOE is installed on to be protected against viruses, other Malware and attacks from network connections. The objective **OE.IFD** requires the IFD not to compromise the passwords used for user authentication against the eID-Card.

The threat **T.ManDisplaying** "Manipulation of Authentication data or results displayed to the user" is directly addressed by the objective **OT.SecureDisplay** requiring the TOE to provide the possibility to display the CVC information, CVC Access Rights and the Authentication Results to the End-User completely and unaltered.

The threat **T.FinalAccessRights** "Manipulation of the Final Access Rights" is directly addressed by the objective **OT.FinalAccessRights** requiring the TOE enable the user to restrict the CVC Access Rights to Final Access Rights or to accept the CVC Access Rights as Final Access Rights and to forward the Final Access Rights unaltered to the IFD. The objective **OT.SecureDisplay** requires the TOE to display the Final Access rights unaltered to the End-User. The objective **OE.Platform** requires the platform where TOE is installed on to be protected against viruses, other Malware and attacks from network connections. The objective **OE.IFD** requires the IFD not to compromise the final access right sent by the TOE.

The organisational security policy **P.ServerCheck** "Checking of server data" is directly addressed by the objectives **OT.Com-Check** requiring the TOE to verify the CVC signatures and the consistency of the X.509 certificates used for the TLS-Channels with the corresponding hashes from the CVC extensions. The security objective for the operational environment **OE.CurrentDate** requires the operating system to provide the current date needed for signature verification.

The organisational security policy **P.AccessRights** "Handling CVC Access Rights" is addressed by the objective **OT.SecureDisplay** requiring the TOE to enable the End-User to get displayed

1. the information about the holder of the CVC
2. the CVC Access Rights of the eID-Server contained in the CVC,
3. and the result of the consistency checks between the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate and the corresponding information from the CVC extension

complete and unaltered on his/her choice. The objective **OT.FinalAccessRights** is requiring the TOE to enable the End-User to restrict the CVC Access Rights before password entry and to send them unaltered to the IFD.

The OSP **P.PACE** "Password Authenticated Connection Establishment support" is directly addressed by the security objective **OT.PACE** "PACE support".

The OSP **P.Integrity** is addressed by the security objectives **OT.Integrity, OT.Update** and **OE.Update**. **OT.Integrity** requires the TOE to verify its integrity which includes the verification of the integrity of the TSF data (listed in table 2). **OT.Update** requires the TOE to verify the integrity and authenticity of the update data. The **OE.Update** requires the developer to provide signed updates of the TOE.

The assumption **A.End-User** "Trustworthy personnel" is directly covered by the security objective for the TOE environment **OE.End-User** "Trustworthy personnel" claiming that the user are trustworthy and are following the TOE's guidance.

The assumption **A.Platform** "Underlying platform" is directly covered by the security objective for the TOE environment **OE.Platform** "Underlying platform" describing the hardware and software requirements for the TOE and requiring the platform not to harm the confidentiality and integrity of the eID-PIN or password if entered through the keyboard and provided to the TOE.

The assumption **A.IFD** "Interface devices" is directly addressed by **OE.IFD** requiring the TOE environment to provide an IFD with secure PIN-Entry and display for CVC Access Rights which shall neither compromise the eID-PIN or PUK or CAN nor manipulate the Final Access Rights.

The assumption **A.Browser** "Browser support" is directly addressed by OE.Browser Requiring the TOE environment to communicate through TLS channels with the eService and (if applicable) the eID-Server and to support the export of the eService-Certificate and the SAML-Certificate.

The assumption **A.Cert** "Certificates" is directly addressed by **OE.Cert** requiring the TOE environment to encode the CVC Access Rights defined for the eService and links of the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate in the CVC and to ensure the validity of and correct identification of the certificate holder in the X.509 certificates linked by the hash value mechanism.

The assumption **A.eService** "eService" is directly addressed by **OE.eService**.

The assumption **A.Browser-Plugin** "Browser-Plugin and eCard-API client" is directly addressed by **OE.Browser-Plugin**.

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).

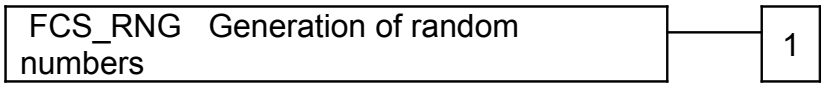
The family "Generation of random numbers (FCS_RNG)" is specified as follows.

555 **FCS_RNG Generation of random numbers**

Family behaviour

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

Component levelling:



560

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

Management: FCS_RNG.1

565 There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

570 Dependencies: No dependencies.

FCS_RNG.1.1	The TSF shall provide a [selection: *non-physical true, deterministic, physical hybrid, deterministic hybrid*] random number generator, which 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 the other families of the class FIA address the verification of the identity of an external entity.

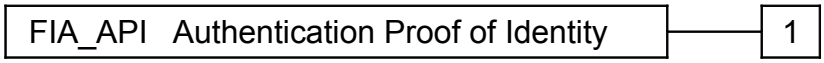
Application note 4: The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality to prove the TOE identity or supporting the user to prove its identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [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 paragraph C.4 of Part 1 [1] of the CC. 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 5: 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.

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

FCS_CKM.1/KAPACE Cryptographic key generation – Key Agreement PACE

FCS_CKM.1.1/ KAPACE	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm session key agreement during PACE[8] and specified cryptographic key sizes of at least 128 bit[9] that meet the following: 'BSI TR-03110', [5] using the 'PKCS #3: Diffie-Hellman Key-Agreement Standard', [10] or using the TR-03111 [11] ECKA Key-Agreement Standard[10].

Application note 6: The TOE shall at least implement the key derivation function in accordance to
635 'BSI TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents' [5] with the concrete algorithm specified as PKCS #3: Diffie-Hellman Key-Agreement Standard', [10] and ECKA as specified in TR-03111 [11].

FCS_CKM.1/KATLS Cryptographic key generation – Key Agreement TLS

FCS_CKM.1.1/ KATLS	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm session key agreement during TLS that meet the following RFC 4279 [12] or [selection: *cryptographic key algorithm*] [11] and specified cryptographic key sizes at least 100 bit [12] that meet the following: RFC 4279 [12], TR-02102 [13][13].

Application note 7: The TOE shall implement the key derivation function for TLS in accordance to
640 RFC 4279 [12] with the exception of the signature verification regarding the server certificate. The server certificate is verified by means of the hash value link in the CVC of the eID-Server.

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).

645 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

8 [assignment: *cryptographic key generation algorithm*]
9 [assignment: *cryptographic key sizes*]
10 [assignment: *list of standards*]
11 [assignment: *cryptographic key generation algorithm*]
12 [assignment: *cryptographic key sizes*]
13 [assignment: *list of standards*]

cryptographic key destruction method zeroization[14] that meets the following: none[15].

Application note 8: The ephemeral keys established during TLS and PACE shall be actively overwritten when they are no longer used. The 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

FCS_COP.1/X.509 Cryptographic operation – X.509 certificates verification

FCS_COP.1.1/X.509: The TSF shall perform verification of eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate[16] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and [assignment: *cryptographic key sizes*] that meet the following: 'TR-02102' [13][17].

Application note 9: This SFR addresses the authentication of the eID-Server during TLS channel establishment.

FCS_COP.1/CVC Cryptographic operation – CVC verification

FCS_COP.1.1/CVC: The TSF shall perform verification of CVC with link check[18] in accordance with a specified cryptographic algorithm ECDSA[19] and cryptographic key sizes according to TR-03110 [5][20] that meet the following: BSI TR-03110 [5][21].

Application note 10: This SFR addresses the verification of the eID-Server CVC including check of the link to the eService-Certificate and the eID-Server-Certificate and, if applicable, the SAML-Certificate. The verification of the CVC includes (1) the examination of the CVC content according to [5], Annex C, (2) the verification of the digital signature with the public key for the CVC

14 [assignment: *cryptographic key destruction method*]
15 [assignment: *list of standards*]
16 [assignment: *list of cryptographic operations*]
17 [assignment: *list of standards*]
18 [assignment: *list of cryptographic operations*]
19 [assignment: *cryptographic algorithm*]
20 [assignment: *cryptographic key sizes*]
21 [assignment: *list of standards*]

verification and (3) the check of the validity period of the CVC. The link check includes (1) the verification of the hash values of the eService-Certificate imported from the Browser against the hash value of the eService-Certificate contained in the CVC certificate extension, (2) the verification of the hash value of the SAML-Certificate imported from the browser against the hash values of the SAML-Certificate contained in the CVC certificate extension, and (3) the verification of the hash value of the eID-Server-Certificate against the hash values of the eID-Server-Certificate contained in the CVC certificate extension (cf. [5] section C.3 for details).

FCS_COP.1/SHA Cryptographic operation – Hash value calculation (SHA)

FCS_COP.1.1/ SHA	The TSF shall perform computation of hash values[22] in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[23] and cryptographic key sizes none[24] that meet the following: [14][25].

Application note 11: This SFR requires implementation of a full set of hash function for key agreement, certificate verification and data integrity mechanisms.

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

FCS_COP.1.1/ AES	The TSF shall perform decryption and encryption[26] in accordance with a specified cryptographic algorithm AES – CBC mode[27] and cryptographic key sizes of at least 128 bit[28] that meet the following: FIPS PUB 197, [15][29].

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[30] in accordance with a specified cryptographic algorithm AES-CMAC[31] and cryptographic key sizes at least 128 bit[32] that meet the following: RFC 4493 [16] and NIST Special Publication 800-38B [17][33].

Application note 12: The cryptographic algorithms AES and AES-CMAC are used for secure messaging channel established with PACE keys, as well as part of the PACE protocol and TLS messaging.

22 [assignment: *list of cryptographic operations*]
23 [assignment: *cryptographic algorithm*]
24 [assignment: *cryptographic key sizes*]
25 [assignment: *list of standards*]
26 [assignment: *list of cryptographic operations*]
27 [assignment: *cryptographic algorithm*]
28 [assignment: *cryptographic key sizes*]
29 [assignment: *list of standards*]
30 [assignment: *list of cryptographic operations*]
31 [assignment: *cryptographic algorithm*]
32 [assignment: *cryptographic key sizes*]
33 [assignment: *list of standards*]

685 **FCS_COP.1/Sig Cryptographic operation – Signature verification**

FCS_COP.1.1/ Sig	The TSF shall perform digital signature verification[34] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *digital signature algorithm listed in [13]*][35]

FCS_COP.1/DES3 Cryptographic operation – Encryption and Decryption using Triple-DES

FCS_COP.1.1/ DES3	The TSF shall perform decryption and encryption[36] in accordance with a specified cryptographic algorithm Triple-DES[37] and cryptographic key sizes168bit[38] that meet the following: FIPS PUB 46-3, [18][39].

FCS_COP.1/HMAC Cryptographic operation – Message Authentication using HMAC

FCS_COP.1.1/ HMAC	The TSF shall perform calculation of Message Authentication Code[40] in accordance with a specified cryptographic algorithm HMAC-SHA-1[41] and cryptographic key sizes at least 128 bit[42] that meet the following: 'RFC2104' [19], 'RFC2404' [20][43].

FCS_COP.1/TLS Cryptographic operation – TLS with RSA and PSK

FCS_COP.1.1/ TLS	The TSF shall perform TLS[44] in accordance with a specified cryptographic algorithm all from RFC 4279 [12][45] and cryptographic key sizes at least 100 bit[46] that meet the following: RFC 4279 [12], TR-02102 [13] [47].

Application note 13: The cryptographic algorithms RSA, AES, DES3 and HMAC are used for TLS
690 channels.

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.

695 Dependencies: No dependencies.

34 [assignment: *list of cryptographic operations*]
35 [assignment: *list of standards*]
36 [assignment: *list of cryptographic operations*]
37 [assignment: *cryptographic algorithm*]
38 [assignment: *cryptographic key sizes*]
39 [assignment: *list of standards*]
40 [assignment: *list of cryptographic operations*]
41 [assignment: *cryptographic algorithm*]
42 [assignment: *cryptographic key sizes*]
43 [assignment: *list of standards*]
44 [assignment: *list of cryptographic operations*]
45 [assignment: *cryptographic algorithm*]
46 [assignment: *cryptographic key sizes*]
47 [assignment: *list of standards*]

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1	The TSF shall provide a [selection: *non-physical true, deterministic, physical hybrid, deterministic hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet TR-02102 chapter 9 [13][48].

Application note 14: This SFR requires the TOE to generate random numbers used for the authentication protocols and key derivation mechanisms (i.e. FCS_CKM.1).

6.1.2. Information flow between eID-Server and eID-Card

In this chapter the following objectives are handled: OT.Com-Check, OT.Com-Sec, OT.PACE,
700 OT.SecureDisplay, OT.Pre-SharedKey and OT.FinalAccessRights.

6.1.2.1. FDP_IFC.1/eID Subset information flow control

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

Hierarchical to: No other components.

705 Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1/eID Subset information flow control

FDP_IFC.1.1/eID The TSF shall enforce the eID control SFP[49] on the following subjects and information:

1. subjects[50]:
   - 1.1. eID-Server
   - 1.2. eID-Card
   - 1.3. Browser
   - 1.4. End-User
2. information:
   - 2.1. every information to be exchanged between eID-Server and eID-Card (via IFD) according to [4] and [5]
   - 2.2. every information to be displayed to the End-User according to FDP_IFF.1.2/eID and FDP_IFF.1.3/eID
   - 2.3. the Pre-Shared Key provided by the eService and the eService-Certificate and, if applicable, the SAML-

48 [assignment: *a defined quality metric*]
49 [assignment: *information flow control SFP*]
50 As there is no direct communication between TOE and eService, Browser and eService will be the same role concerning the TOE.

Certificate imported from the Browser

2.4. the eID-Server-Certificate imported from the eID-Server

3. operation: establishing communication between TOE and eID-Server[51].

6.1.2.2. FDP_IFF.1/eID Simple security attributes

The TOE shall meet the requirement "Simple security attributes (FDP_IFF.1)" as specified below
710 (Common 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/eID Simple security attributes

FDP_IFF.1.1/eID The TSF shall enforce the eID control SFP[52] based on the following types of subject and information security attributes:

1. subjects[53]:
   1.1. eID-Server: security attribute: "authentication status"
   1.2. eID-Card: any entity sending messages to IFD-Interface is defined as eID-Card
   1.3. Browser: any entity sending messages to Browser-Interface is defined as Browser
   1.4. End-User: any entity having direct access to the human user interface is defined as End-User
2. information:
   2.1. every information to be exchanged between eID-Server and eID-Card (via IFD) according to [4] and [5]
   2.2. every information to be displayed to the End-User according to FDP_IFF.1.2/eID and FDP_IFF.1.3/eID
   2.3. the Pre-Shared Key provided by the eService and the eService-Certificate and , if applicable, the SAML-Certificate imported from the Browser
   2.4. the eID-Server-Certificate imported from the eID-Server [54].

51 [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
52 [assignment: *information flow control SFP*]
53 As there is no direct communication between TOE and eService, Browser and eService will be the same role concerning the TOE.

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

1. the TOE shall import the Pre-Shared Key provided by the eService and the eService-Certificate from the Browser,
2. in order to protect integrity and confidentiality the TOE shall not transmit the imported Pre-Shared Key to any external entity nor shall the TOE store the Pre-Shared Key on any persistent storage,
3. the TOE and the eID-Server shall establish a TLS-Channel for communication using TLS authentication by means of the eID-Server-Certificate gained during the TLS-Handshake and the Pre-Shared Key,
4. the TOE shall process the following checks and display their results to the End-User:
   - 4.1. the signature of the CVC to be used for Terminal Authentication of the eID-Server is successfully verified with the public key for CVC verification stored in the TOE,
   - 4.2. the eService-Certificate imported from the browser as used for TLS channels between the browser and the eService is linked with the verified CVC to be used for TA of the eID-Server,
   - 4.3. the eID-Server-Certificate used for TLS channels between the TOE and the eID-Server is linked with the verified CVC to be used for TA of the eID-Server,
   - 4.4. only in the case of mediated communication between eService and eID-Server, the SAML-Certificate used to establish TLS_SAML is also part of this consistency check with the verified CVC to be used for TA of the eID-Server,
5. if the TLS-Channel has been successfully established and every check in 4 came to the result "true", the security attribute "authentication status" of the subject eID-Server shall be set to the value "successfully authenticated". If one of these conditions could not be fulfilled the TOE shall display a warning about the fail and the reason for it to the End-User and the value of "authentication status" stays "not authenticated"[55].

FDP_IFF.1.3/eID The TSF shall enforce the following rules:

1. Information flow shall only be permitted, if the following steps (1.1 to 1.5) are fulfilled in the order given below. If at least one

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

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

of the steps can not be fulfilled, the subsequent steps shall not be processed and no information flow shall be permitted:

1.1. the "authentication status" of the subject eID-Server must have the value "successfully authenticated".

1.2. the TOE shall ensure that at least the owner of the CVC will be displayed unambiguous to the End-User and the remaining content of the CV Certificate and included extensions as well as the validity time frame will be displayed completely and unambiguous according to [5] and [6][56] at least on End-User's demand.

1.3. the TOE shall display the CVC Access Rights gained from the Certificate Holder Authorization Template of the CVC unambiguous and completely to the End-User and provide her/him with the possibility either to restrict those CVC Access Rights or to accept them unaltered in order to get Final Access Rights. This includes an short explanation[57] of every single CVC Access Right gained from the Bits of the Certificate Holder Authorization Template. The integrity of these Final Access Rights shall be ensured by the TOE as long they are in the domain of the TOE.

1.4. PACE according to FIA_API.1 shall be processed and the result shall be displayed to the End-User,

1.5. the Final Access Rights (the restrictions defined by the End-User) shall be displayed to the End-User as applied to the Certificate Holder Authorization Template and be sent unaltered to the eID-Card directly after PACE protocol for use in the Terminal Authentication protocol according to [5].

2. the TOE shall support the information flow by forwarding the messages exchanged between eID-Server and eID-Card to the corresponding recipient,

3. the result of the Terminal Authentication protocol processed between eID-Server and eID-Card and announced by the eID-Card shall be displayed by the TOE to the End-User[58].

FDP_IFF.1.4/eID	The TSF shall explicitly authorise an information flow based on the following rules: none[59].
FDP_IFF.1.5/eID	The TSF shall explicitly deny an information flow based on the following rules: none[60].

56 [5] Describes how to process the CVC and which data it can contain while [6] sets the requirements which data at least have to be displayed to the End-User

57 This means e.g. displaying a check box for the CVC Access Right giving read access to data group 5 and a text label "family name" beneath

58 [assignment: *additional information flow control SFP rules*]

59 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

715 **6.1.2.3. FIA_UID.1/eID Timing of identification**

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

Hierarchical to: No other components.

Dependencies: No dependencies.

720 **FIA_UID.1/eID Timing of identification**

FIA_UID.1.1/eID	The TSF shall allow access to eCard-API interface[61][62] on behalf of the **local** user to be performed before the user is identified.
FIA_UID.1.2/eID	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note 15: Browser, eID-Server and eID-Card are identified at the moment they send a message to the corresponding interface (which means IFD-Interface for the eID-Card). The End-User is a local user.

6.1.2.4. FMT_MSA.3/eID Static attribute initialisation

725 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

730 **FMT_MSA.3/eID Static attribute initialisation**

FMT_MSA.3.1/eID	The TSF shall enforce the eID control SFP[63] to provide restrictive[64] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/eID	The TSF shall allow the none[65] 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 "authentication status" is "not authenticated".

60 [assignment: *rules, based on security attributes, that explicitly deny information flows*]
61 This means not the interface between eCard-API part of the TOE and Browser-Plugin, but the interfaces to the IFD/eID-Card, to eID-Server and between Browser and Browser-Plugin
62 [assignment: *list of TSF-mediated actions*]
63 [assignment: access control SFP, information flow control SFP]
64 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
65 [assignment: *the authorised identified roles*]

6.1.2.5. FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1/eID Security roles

FMT_SMR.1.1/eID	The TSF shall maintain the roles 1. eID-Server 2. eID-Card 3. Browser[66] 4. End-User[67].
FMT_SMR.1.2/eID	The TSF shall be able to associate users with roles.

6.1.2.6. Proof of Identity (FIA_API.1)

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

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 [5] including PIN-Management and the display of the PACE result to the End-User; a) in the case an IFD without secure PIN-Entry is used, 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, b) in the case an IFD with secure PIN-Entry is used, the terminal part of PACE must be performed by the IFD and the TOE shall simply retrieve the result by the IFD and display it to the End-User[68] to prove the identity of the eID-Card holder[69] **to the eID-Card**.

66 As there is no direct communication between TOE and eService, Browser and eService will be the same role concerning the TOE.
67 [assignment: *the authorised identified roles*]
68 [assignment: *authentication mechanism*]
69 [assignment: *authorized user or rule*]

745 **Application note 17:** The terminal part of PACE includes the possibility to use PIN, PUK or CAN for user authentication.

6.1.2.7. Subset residual information protection (FDP_RIP.1)

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

750 Hierarchical to: No other components.

Dependencies: No dependencies.

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[70] 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 • the Pre-shared Key after finishing communication between TOE and eID-Server via TLS-Channel[71]. **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. PIN-Management cannot be started or is aborted.**

Application note 18: 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

755 The following SFRs handle the security objectives OT.Interfaces und OT.Update.

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

Hierarchical to: No other components.

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

70 [selection: *allocation of the resource to, deallocation of the resource from*]
71 [assignment: *list of objects*]

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1	The TSF shall enforce the interface control SFP [72] 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" .[73].

6.1.3.2. Subset information flow control (FDP_IFC.1)

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

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1/Inter Subset information flow control

FDP_IFC.1.1/ Inter	The TSF shall enforce the interface control SFP[74] on: 1 subject: TOE (eCard-API part of the TOE), Browser-Plugin, IFD, eID-Server, Browser, Update Provider 2 information: 2.1 IFD-message 2.2 eID-Server-message 2.3 Browser-message 2.4 Browser-Plugin-message 2.5 Update data 3 operations: 3.1 receiving messages from one of the subjects 3.2 receiving update data[75]

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

72 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
73 [assignment: *additional importation control rules*]
74 [assignment: *information flow control SFP*]
75 [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

Subject	Description
IFD	an external entity which is sending messages to IFD-Interface
eID-Server	an external entity which is sending messages to eID-Server-Interface
Browser	an external entity which is sending messages to Browser-Interface, i.e. the interface between Browser-Plugin and Browser (see Figure 1, page 7)
Update Provider	any entity giving Update data to the TOE

table 4: Subjects of the interface control SFP

Information	Description	
IFD-message	Any type of message received via IFD-Interface	
Security Attribute	Value	Implication
syntactical correctness	correct	Syntactically correct according to [8]
	incorrect	every message which is not correct
Information	**Description**	
eID-Server-message	Any type of message received via eID-Server-Interface	
Security Attribute	Value	Implication
syntactical correctness	correct	Syntactically correct according to [4], part 7 and part 4.
	incorrect	every message which is not correct
Information	**Description**	
Browser-Plugin-message	Any type of message received by the eCard-API part of the TOE from Browser-Plugin, which shall receive messages according to [4], part 7.	
Security Attribute	Value	Implication
syntactically correctness	correct	Syntactically correct according to [4], part 7
	incorrect	every message which is not correct
Information	**Description**	
Browser-message	Any type of message received or imported by the Browser-Plugin via Browser-Interface (interface between Browser-Plugin and Browser)	
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) and additional data (e.g. help files)[76].	
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 developer.

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

	negatively verified	Update data which could not be verified as authentic by means of digital signature of the TOE developer.

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 Criteria Part 2).

Hierarchical to: No other components.

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

FDP_IFF.1/Inter Simple security attributes

FDP_IFF.1.1/Inter The TSF shall enforce the interface control SFP[77] based on the following types of subject and information security attributes:

1. subjects:
   - 1.1. TOE (eCard-API part of the TOE)
   - 1.2. Browser-Plugin
   - 1.3. any entity sending messages at IFD-Interface is defined as IFD
   - 1.4. any entity sending messages at Browser-Interface is defined as Browser
   - 1.5. any entity sending messages at eID-Server-Interface is defined as eID-Server
   - 1.6. any entity giving Update data to the TOE is defined as Update Provider
2. information:
   - 2.1. messages received by the TOE from IFD are defined as information named IFD-Message with the security attribute "syntactically correctness"
   - 2.2. messages received by the TOE from eID-Server are defined as information named eID-Server-Message with the security attribute "syntactically correctness"
   - 2.3. messages received by the Browser-Plugin from Browser defined as information named Browser-Message which have no security attribute
   - 2.4. messages received by the eCard-API part of the TOE from Browser-Plugin are defined as information named Browser-Plugin-Message with the security attribute "syntactically correctness"
   - 2.5. 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

77 [assignment: *information flow control SFP*]

	Update data" 3. [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*][78].
FDP_IFF.1.2/Inter	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: 1. IFD-Messages are checked on their syntactically correctness according to [8] as messages sent by an IFD or eID-Card via IFD to an eCard-API Client. 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. eID-Server-Messages are checked on their syntactically correctness according to [4], part 7 and part 4 as messages sent by an eID-Server. 2.1. If the message is syntactical correct the security attribute "syntactically correctness" is set to "correct", and the message shall be processed by the TOE, 2.2. otherwise the value of the security attribute is set to "incorrect"and the message must be rejected or discarded.. 3. Browser-Messages are received by the Browser-Plugin. The Browser-Plugin shall not check, modify or process these messages nor perform any other actions on these messages except for forwarding them to the eCard-API part of the TOE. 4. Browser-Plugin-Messages are checked on their syntactically correctness according to [4], part 7 as messages sent by the eService or data to be gained from the Browser itself. 4.1. If the message is syntactical correct the security attribute "syntactically correctness" is set to "correct" and the message shall be processed by the TOE, 4.2. otherwise the value of the security attribute is set to "incorrect"and the message must be rejected or discarded. 5. Update data are verified on their authenticity and integrity by means of digital signature of the TOE developer by using the "public key for update data verification" before they are used or unpacked. 5.1. If the signature is verified as correct the security attribute "verification status Update data" is set to "successfully verified", 5.2. otherwise the security attribute is set to "negatively verified" and the data must be handled according to FDP_RIP.1. 6. [assignment: *for each operation, the security attribute-based*

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

	relationship that must hold between subject and information security attributes][79].
FDP_IFF.1.3/Inter	The TSF shall enforce the none[80].
FDP_IFF.1.4/Inter	The TSF shall explicitly authorise an information flow based on the following rules: none[81].
FDP_IFF.1.5/Inter	The TSF shall explicitly deny an information flow based on the following rules: none[82].

Application note 19: FDP_IFF.1/Inter 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/Inter is extended for the use of additional interfaces to external entities FDP_IFF.1.2/Inter 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/Inter Static attribute initialisation

FMT_MSA.3.1 /Inter	The TSF shall enforce the interface control SFP [83] to provide restrictive [84] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 /Inter	The TSF shall allow ~~the~~ none [85] to specify alternative initial values to override the default values when an object or information is created.

Application note 20: 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".

6.1.3.5. Security roles (FMT_SMR.1)

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

79 [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].
80 [assignment: *additional information flow control SFP rules*]
81 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
82 [assignment: *rules, based on security attributes, that explicitly deny information flows*]
83 [assignment: *access control SFP, information flow control SFP*]
84 [selection, choose one of: *restrictive, permissive,* [assignment: *other property*]]
85 [assignment: *the authorised identified roles*]

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1/Inter Security roles

FMT_SMR.1.1/Inter	The TSF shall maintain the roles 1. Browser, 2. eID-Server, 3. IFD, 4. Update Provider, 5. [assignment: *additional authorised identified roles*][86].
FMT_SMR.1.2/Inter	The TSF shall be able to associate users with roles.

Application note 21: The ST author shall perform the open assignment in element FMT_SMR.1.1/Inter. 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/Inter User identification before any action

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

Application note 22: Browser, eID-Server, IFD and Update-Server are identified by sending a message to the corresponding interface.

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.

86 [assignment: *the authorised identified roles*]

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[87].

Application note 23: 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*] [88] 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[89].
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 24: 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 table 2.

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_FLR.1, ALC_TAT.1 and AVA_VAN.3.

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

87 [assignment: *list of types of failures in the TSF*]
88 [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*]]
89 [selection: [assignment: *parts of TSF data*], *TSF data*]

practices. EAL3 is applicable in those circumstances where developers or users require a moderate
835 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 ehanced-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.Com-Sec	OT.Interfaces	OT.Com-Check	OT.PACE	OT.Integrity	OT.Update	OT.Password	OT.Pre-SharedKey	OT.SecureDisplay	OT.FinalAccess Rights
FCS_CKM.1/KAPACE				x						
FCS_CKM.1/KATLS	x									
FCS_CKM.4	x			x						
FCS_COP.1/AES	x			x						
FCS_COP.1/CMAC				x						
FCS_COP.1/CVC	x		x							
FCS_COP.1/DES3	x									
FCS_COP.1/HMAC	x									
FCS_COP.1/SHA	x		x							
FCS_COP.1/Sig						x				
FCS_COP.1/TLS	x									
FCS_COP.1/X.509	x									
FCS_RNG.1	x			x						
FDP_IFC.1/eID	x		x					x	x	x
FDP_IFC.1/Inter		x				x				
FDP_IFF.1/eID	x		x					x	x	x
FDP_IFF.1/Inter		x				x				
FDP_ITC.1		x								
FDP_RIP.1				x		x	x	x		
FIA_API.1				x			x			
FIA_UID.1/eID	x		x					x	x	x
FIA_UID.2/Inter		x				x				
FMT_MSA.3/eID	x		x							
FMT_MSA.3/Inter		x				x				
FMT_SMR.1/eID	x		x					x	x	x

	OT.Com-Sec	OT.Interfaces	OT.Com-Check	OT.PACE	OT.Integrity	OT.Update	OT.Password	OT.Pre-SharedKey	OT.SecureDisplay	OT.FinalAccess Rights
FMT_SMR.1/Inter		x				x				
FPT_FLS.1					x					
FPT_TST.1					x					

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

The security objective **OT.Com-Sec** "Communication security" is enforced by a secure TLS-Channel (FCS_COP.1/TLS), which shall use the cryptographic primitives for certificate validation in accordance to FCS_COP.1/X.509, encryption in accordance to FCS_COP.1/DES3 or FCS_COP.1/AES and integrity protection in accordance to FCS_COP.1/HMAC and FCS_COP.1/SHA. The keys are derived by a combination of the Pre-shared Key and keys generated in accordance with FCS_CKM.1/KATLS and destroyed according to FCS_CKM.4. The usage of the Pre-shared Key is enforced by FDP_IFF.1/eID in combination with FDP_IFC.1/eID where the authentication of the eID-Server is also demanded before an information flow between eID-Server and eID-Card is allowed. FMT_SMR.1/eID defines the roles needed for this information flow control and FMT_MSA.3/eID defines how the security attribute and its values shall be initialised. FIA_UID.1/eID manages the timing of identification. FCS_COP.1/CVC provides the cryptographic tools and FCS_RNG.1 the random numbers for the different steps of the eID-Server authentication, which consists of the verification of the CVC and the comparing of the hashes of the X.509 from the TLS-Channel with those gained from the CVC.

The security objective **OT.Com-Check** "Communication check" is enforced by FDP_IFF.1/eID in combination with FDP_IFC.1/eID requiring

- the validation and verification of the CVC
- and the contained links to the eService-Certificate, the eID-Server-Certificate and, if applicable, the SAML-Certificate (in order to perform these link checks hashes of the X.509 certificates have to be generated according to FCS_COP.1/SHA),
- the displaying of the CVC content and extension
- giving a warning to the End-User in case of any detected mismatches or failures

FMT_SMR.1/eID, FIA_UID.1/eID, FMT_MSA.3/eID, FCS_COP.1/SHA and FCS_COP.1/CVC enhance these points as described in the section above.

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. This SFP is described by FDP_IFC.1/Inter in combination with FDP_IFF.1/Inter. FMT_SMR.1/Inter defines the roles needed for this information flow control and FMT_MSA.3/Inter defines how the security attributes and their values shall be initialised. Both subjects in this context are identified as soon as they interact with TOE by the interface they use, therefore FIA_UID.2/Inter 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/KAPACE and 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 **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).

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 generated by the TOE developer and therefore the same SFRs except for FDP_ITC.1 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.Password** "Password security" is enforced by the SFRs FDP_RIP.1 and FIA_API.1. FIA_API.1 requires the TOE to use the inserted passwords only for PACE or PIN management and FDP_RIP.1 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.

With the requirement of using the Pre-shared Key for communication with the eID-Server in FDP_IFF.1/eID and protecting the confidentiality and integrity of the PSK the eID control SFP used for OT.Com-Sec also covers the security objective **OT.Pre-SharedKey** "Usage of Pre-Shared Key". Therefore FDP_IFC.1/eID, FMT_SMR.1/eID, and FIA_UID.1/eID are needed for the same reasons. Additionally FDP_RIP.1 ensures the deletion of the Pre-Shared Key when it is not longer needed.

The security objectives **OT.SecureDisplay** "Display of the CVC and authentication information" and **OT.FinalAccessRights "**Final Access Rights" are enforced by FDP_IFF.1/eID in combination with FDP_IFC.1/eID defining the sequence of steps to be fulfilled before the information flow between eID-Server and eID-Card is allowed. This includes

- the unambiguous displaying of the CVC content and extensions after successful verification of the CVC and the contained links to the eService-Certificate, the eID-Server-Certificate and, if applicable, the SAML-Certificate used for TLS communication or displaying of a warning in case of unsuccessful verification,
- the possibility to restrict or accept the CVC Access Rights for the End-User in order to gain the Final Access Rights before password entry,
- the forwarding of the unaltered Final Access Rights to the eID-Card,
- the announcement about the result of the Terminal Authentication,

this is achieved by FMT_SMR.1/eID defining the roles needed for this information flow control. FIA_UID.1/eID manages the timing of identification.

6.3.2. Dependency Rationale

910 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.

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

SFR	Dependencies	Fulfilment of Dependencies
FCS_CKM.1/KAPACE	[FCS_CKM.2, FCS_COP.1] FCS_CKM.4	FCS_COP.1/CMAC, FCS_COP.1/AES FCS_CKM.4
FCS_CKM.1/KATLS	[FCS_CKM.2, FCS_COP.1] FCS_CKM.4	FCS_COP.1/DES3, FCS_COP.1/AES FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, FCS_CKM.1]	FCS_CKM.1/KAPACE, FCS_CKM.1/KATLS
FCS_COP.1/AES	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/KAPACE, FCS_CKM.1/KATLS FCS_CKM.4
FCS_COP.1/CMAC	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/KAPACE FCS_CKM.4
FCS_COP.1/CVC	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	not fulfilled (cf. justification 1) not fulfilled (cf. justification 1)
FCS_COP.1/DES3	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/KATLS FCS_CKM.4
FCS_COP.1/HMAC	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/KATLS FCS_CKM.4
FCS_COP.1/SHA	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	not fulfilled (cf. justification 2) not fulfilled (cf. justification 2)
FCS_COP.1/Sig	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	not fulfilled (cf. justification 3) not fulfilled (cf. justification 3)
FCS_COP.1/TLS	[FDP_ITC.1,FDP_ITC.2, FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/KATLS FCS_CKM.4
FCS_COP.1/X.509	[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/eID	FDP_IFF.1	FDP_IFF.1/eID
FDP_IFC.1/Inter	FDP_IFF.1	FDP_IFF.1/Inter
FDP_IFF.1/eID	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/eID FMT_MSA.3/eID
FDP_IFF.1/Inter	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Inter FMT_MSA.3/Inter
FDP_ITC.1	[FDP_ACC.1, FDP_IFC.1] FMT_MSA.3	FDP_IFC.1/Inter FMT_MSA.3/Inter
FDP_RIP.1	no dep.	no dep.
FIA_API.1	no dep.	no dep.

SFR	Dependencies	Fulfilment of Dependencies
FIA_UID.1/eID	no dep.	no dep.
FIA_UID.2/Inter	no dep.	no dep.
FMT_MSA.3/eID	FMT_MSA.1 FMT_SMR.1	cf. Justification 4 FMT_SMR.1/eID
FMT_MSA.3/Inter	FMT_MSA.1 FMT_SMR.1	cf. Justification 4 FMT_SMR.1/Inter
FMT_SMR.1/eID	FIA_UID.1	FIA_UID.1/eID
FMT_SMR.1/Inter	FIA_UID.1	FIA_UID.2/Inter
FPT_FLS.1	no dep.	no dep.
FPT_TST.1	no dep.	no dep.

Table 7: Dependencies between the SFR for the TOE

Justification 1: The key used for certificate verification are internal TSF data (cf. chapter 3.1, table 2), i.e. the root public key for CVC respective for X.509 certificates, thus there is no need for key creation or import nor for key deletion.

Justification 2: The hash algorithms do not use any keys, thus there is no need for key creation or import nor for key deletion.

Justification 3: Since iteration FCS_COP.1/Sig only performs public key operations with internal TSF data for signature verification there is no need for key generation, import or deletion.

Justification 4: 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 developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. The EAL3 is augmented in such a way, that the requirements for EAL4 are met within the assurance classes ASE, ADV, AGD, and AVA.

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.

The selection of the component **ALC_FLR.1** provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE.

All dependencies resulting directly or indirectly from the augmentations AVA_VAN.3 and ALC_FLR.1 are discussed in the following

The component **ALC_FLR.1** has no dependencies.

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

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

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:

950 – ADV_TDS.1 Basic Design

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

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

– ADV_FSP.4 Complete functional specification (FSP.3)

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

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

– ADV_TDS.3 Basic modular design
– 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.

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

– ADV_IMP.1 Implementation representation of the TSF

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
965 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 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined
970 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
975 mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

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.
980 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.

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.
eID-Client	German citizen client, implementing eID authentication and server communication.
Cat B IFD	Category B (cf. category “basic” smart card interface device in [8])
Cat S IFD	Category B (cf. category “standard” smart card interface device in [8])
Cat K IFD	Category B (cf. category “comfort” smart card interface device in [8])
Chip authentication	Authentication of the eID-Card to external entities as defined in [5]
eCard-API	application programming interface defined for the use of eCards in [4]
eCard-API interface	Interface provided by the TOE and defined within the ‘eCard-API-Framework, BSI TR-03112’ parts 2, 4, 5 and 6
Card verifiable certificate	Certificate according to ISO 7816 and [5] which is verifiable by the eID-Card and the TOE
Interface Device	Smart card interface device used for contact card or contactless cards. An interface device for contactless cards is also known as proximity coupling device.
Proximity Coupling Device	Smart card interface device used for contactless cards.
SAML	Security Assertion Markup Language, SAML provides an XML-based framework for creating and exchanging security information between online partners. See http://saml.xml.org/saml-specifications
Terminal authentication	Authentication of external entities to the eID-Card as defined in [5]
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
User data	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [1]).

Table 8: Glossary

Acronym	Term
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CA	Chip Authentication, (cf. [5])
CAN	Card Access Number (cf. [5])
CC	Common Criteria
CHAT	Certificate Holder Authorization Template (cf. [5])
CIF	Card Information File, (cf. [4])
CRL	Certificate Revocation List
CVC	Chip verifiable certificate (cf. [5])
EAC	Extended Access Control (cf. [5])
EAL	Evaluation Assurance Level
eID	Electronic Identity
nPA	Electronic Identity Card (German: elektronischer Personalausweis)
ICC	Integrated Circuit Card
ICCSN	ICC Serial Number
IFD	Interface Device
IP	Internet Protocol
IT	Information Technology
n.a.	Not applicable
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment, (cf. [5])
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PDF	Portable Document Format
PIN	Personal Identification Number (cf. [5])
PKCS	Public Key Cryptography Standard
PP	Protection Profile
PSK	Pre-shared key
PUK	PIN Unblocking Key (cf. [5])
RI	Restricted Identification, (cf. [5])
SAML	Security Assertion Markup Language
SAR	Security assurance requirements
SFR	Security functional requirement
SM	Secure Messaging (cf. [21])
SSL	Secure Sockets Layer (cf. also TLS)
ST	Security Target
TA	Terminal Authentication, (cf. [5])
TLS	Transport Layer Security (cf. also SSL)
TOE	Target of Evaluation
TSF	TOE Security Functions
XML	eXtensible Markup Language
XSD	XML Scheme Definition

Table 9: List of Acronyms

8. Literature

[1]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001 , Version 3.1, Revision 3, July 2009
[2]: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version , July 2009
[3]: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009
[4]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03112, eCard-API-Framework, 23.05.2011
[5]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03110 Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), 14.10.2010
[6]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03127, Technische Richtlinie Architektur Elektronischer Personalausweis, 27.05.2011
[7]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03130, eID-Server Unterstützung , 08.10.2010
[8]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03119, Anforderungen an Chipkartenleser mit nPA Unterstützung, 2009
[9]: Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009
[10]: RSA Laboratories , PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note , 01.11.1993 (Revised)
[11]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-03111, Elliptic Curve Cryptography, 17.04.2009
[12]: P. Eronen, Ed. Nokia, H. Tschofening, Ed. Siemens, Category: Standards Track , RFC4279, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), December 2005
[13]: Bundesamt für Sicherheit in der Informationstechnik , BSI-TR-02102 Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2008
[14]: U.S. Department of Commerce / National Institute of Standards and Technology , Federal Information Processing Standards Publication FIPS PUB 180-3 Secure Hash Standard, October 2008
[15]: U.S. Department of Commerce / National Institute of Standards and Technology , Federal Information Processing Standards Publication FIPS PUB 197, Advanced Encryption Standard (AES), 26.11.2001
[16]: JH. Song et al. University of Washington, Category: Informational , RFC 4493, The AES-CMAC Algorithm , June 2006
[17]: 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 , May 2005
[18]: U.S. Department of Commerce / National Institute of Standards and Technology , Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), 25.10.1999 (Reaffirmed)
[19]: H. Krawczyk, IBM, M. Bellare, UCSD, R. Canetti, IBM, Category: Informational , RFC2104 – HMAC: Keyed-Hashing for Message Authentication, February 1997
[20]: C. Madson, Cisco Systems Inc., R. Glenn, NIST, Category: Standards Track , RFC2404 – The

Use of HMAC-SHA-1-96 within ESP and AH, November 1998
[21]: International Organization for Standardization , ISO/IEC 7816-4, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange, 2005