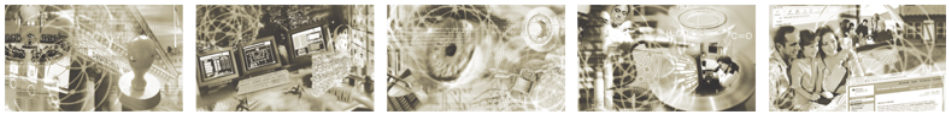
Federal Office
for Information Security



Common Criteria Protection Profile

electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK)

Common Criteria

BSI-CC-PP-0020-V3-2010

Approved by the
Federal Ministry of Health

Version 2.83, 13th September 2010

—— this page was intentionally left blank ——

Foreword

This 'Protection Profile — electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK)' 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 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

—— this page was intentionally left blank ——

Contents

List of Tables

1 PP Introduction

1 There exist the following Protection Profiles for the electronic Health Card (eHC):

2 • "Common Criteria Protection Profile electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)", BSI-PP-0020, version 1.02 from 12. December 2005. This Protection Profile has been prepared as initial version according the "Die Spezifikation der elektronischen Gesundheitskarte" (version 0.99) following the rules and formats of Common Criteria Version 2.1 with final interpretations of CCIMB.

3 • "Common Criteria Protection Profile electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)", BSI-PP-0020-V2-2007, version 2.00 from 29. January 2007. This Protection Profile has been prepared according the new update of the "Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der Betriebssystem-Plattform" (version 1.1.0, 07.02.2006) and "Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Anwendungen und anwendungsspezifische Strukturen" (version 1.2.1, 07.09.2006) and the new rules and formats according to the Common Criteria Version 2.3.

4 • "Common Criteria Protection Profile electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)", BSI-PP-0020-V2-2007-MA01, version 2.50 from 2. January 2008. This Protection Profile has been prepared according the new update of the "Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle" (version 2.0.0, 13.12.2007) and "Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen" (version 2.0.0, 13.12.2007) following the rules and formats of Common Criteria Version 2.3.

5 • "Common Criteria Protection Profile electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)", BSI-PP-0020-V2-2007-MA02, version 2.60 from 29. July 2008. This Protection Profile has been prepared according the new update of the "Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle" (version 2.2.1, 01.07.2008) and "Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen" (version 2.2.1, 19.06.2008) following the rules and formats of Common Criteria Version 2.3.

6 • The current "Common Criteria Protection Profile electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)", BSI-PP-0020-V3, version 2.83 from 13th September 2010. This Protection Profile has been prepared according the "Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle" (version 2.2.2, 16.09.2008) and "Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen" (version 2.2.1, 19.06.2008) and is updated following the rules and formats of Common Criteria Version 3.1, Revision 3.

1.1 PP reference

7	Title:	Protection Profile — electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK)
8	Sponsor:	Bundesamt für Sicherheit in der Informationstechnik
9	Editors:	Dr. Bertolt Krüger, Hendrik Dettmer SRC Security Research & Consulting GmbH
10	CC Version:	3.1, Revision 3
11	Assurance Level:	The minimum assurance level for this PP is EAL4 augmented.
12	General Status:	final version
13	Version Number:	2.83
14	Registration:	BSI-CC-PP-0020-V3-2010
15	Keywords:	electronic Health Card (eHC), elektronische Gesundheitskarte (eGK)

1.2 TOE Overview

1.2.1 Usage of the TOE

16 The protection profile defines the security objectives and requirements for the electronic Health Card (German: “elektronische Gesundheitskarte”) based on the regulations for the German health care system. It addresses the security services provided by this card, mainly:

17 • Mutual Authentication between the eHC and a Health Professional Card (HPC) or a Security Module Card (SMC),

18 • Mutual Authentication between the eHC and a security device (e. g. for online update of contract data in the card),

19 • Authentication of the cardholder by use of one of two PINs, called PIN.CH and PIN.home (which of these PINs is relevant depends on the service the cardholder wants to use),
Note: Both of these PINs are used for general functions of the eHC. The electronic signature application (see below) requires a separate third PIN for its exclusive purposes.

20 • Secure storage of contractual and medical data, with respect to confidentiality, integrity and authenticity of these data,

21 • Authentication of the card using a private key and a X.509 certificate and

22 • Document content key decipherment using a private key.

23 Note: The eHC may contain an electronic signature application for the cardholder. This application is subject to the requirements for electronic signatures as defined in national and European law. Separate Protection Profiles exist defining such requirements, for example the SSCD-PPs [10]. Therefore the security requirements for this security feature are not contained in this eHC-PP. Annex 7.1 gives guidance, how this eHC-PP and for example the SSCD-PP can be integrated in a Security Target.

1.2.2 Major security features of the TOE

24 German health insurance companies issue electronic Health Cards to patients insured by them. The card is used by the cardholders, when they use health care services, which are covered by the insurance. A picture of the patient is printed on the card in order to support identification. The eHC contains data for

25 • cardholder identification,

26 • contractual and financial information to be exchanged between cardholder and health care provider and/or the health insurance company and

27 • medical data, including electronic prescriptions.

28 (For a more detailed definition of the assets see section 3.1.1.)

29 In detail the functionality of the card is defined in the specifications[1]:

30 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

31 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

32 The following list gives an overview of the main security services provided by the electronic Health Card during the usage phase. In order to refer to these services later on, short identifiers are defined.

33 **Service_Asym_Mut_Auth_w/o_SM[2]:**

34 Mutual Authentication using asymmetric techniques between the eHC and a Health Professional Card (HPC) or a Security Module Card (SMC) without establishment of a Secure Channel.

35 This service is meant for situations, where the eHC requires authentication by a HPC or SMC, but where the following data exchange is done without help of a security module.

36 **Service_Asym_Mut_Auth_with_SM:**

37 Mutual Authentication using asymmetric techniques between the eHC and a Security Module Card (SMC) or another security module with establishment of a Secure Channel.

38 This service is meant for situations, where the eHC requires authentication by a SMC or another security module, which provides similar functionality, and where the following data exchange is done with the help of this security module and can therefore be encrypted and/or secured by a MAC.

39 **Service_Sym_Mut_Auth_with_SM:**

40 Mutual Authentication using symmetric techniques between the eHC and a security module with establishment of a Secure Channel.

41 This service is meant for situations, where the eHC communicates with a central security module, which shares symmetric keys with the card. This may be a security module of the health insurance organisation, when managing the patient contractual

[1] In future these specifications may be replaced by further versions. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications.

[2] The Abbreviation SM here stands for Secure Messaging, which is the card security protocol realising a secure channel.

data, or a module of the Download Service Provider, which may add new applications to the eHC (or manage the existing ones).

42 **Service_User_Auth_PIN:**

43 The cardholder authenticates himself with one of his PINs, either PIN.CH or PIN.home.

44 This service is meant as a support service for some of the other services, which may require user authentication. In addition it provides privacy protection because certain data in the card (or secured by the card) can only be accessed after user authentication. In particular this applies to sensitive medical data.

45 Functions to change the PIN or to unblock the PIN, when it was blocked (because of successive false PIN entries) are supporting this service. For the latter the PIN unblocking code (PUC) is used, this authentication will be called **Service_User_Auth_PUC**.

46 **Service_Privacy:**

47 The cardholder may deactivate sensitive medical data in the eHC. In order to use this service he authenticates himself with a PIN.

48 This service allows the cardholder to prevent health care providers from accessing data, which the cardholder doesn't want them to know. Note, that that the name Service_Privacy doesn't mean that this is the only privacy related service. In fact all other services also support privacy.

49 **Service_Client_Server_Auth:**

50 The eHC implements a PKI application, which in particular allows using the TOE as an authentication token for an authentication of a client to a server (by means of an asymmetric method using X.509 certificates). The eHC contains two different keys and corresponding certificates for this service. In order to use this service the cardholder authenticates himself with a PIN. One of the keys can also be used without authentication by the cardholder, but requires authentication by a HPC or SMC in this case.

51 This service may for example be useful if the cardholder wants to access a server provided by the health insurance organisation, where confidential data of the cardholder are managed. So it can also be seen as an additional privacy feature.

52 Note, that a potential authentication of the server to the client is not supported by the eHC.

53 **Service_Data_Decryption:**

54 The eHC implements a PKI application, which in particular allows using the TOE as a data decryption token. Symmetric document encipherment keys, which are themselves encrypted with the cards public key can only be decrypted with the help of the card. There are two sets of asymmetric key pairs in the eHC to allow the following two possibilities of authentication for this service:

55 • In order to use this service the cardholder authenticates himself with a PIN.

56 • One of the keys can also be used without authentication by the cardholder, but requires authentication by a HPC or SMC in this case.

57 This service is meant for situations, where confidential data are stored on a server, but shall only be accessible with the cardholder's permission or with the authentication of a health professional. So it can also be seen as a privacy feature.

58 **Service_Card_Management:**

59 The eHC allows creation of new applications and management of existing applications to the card management system. This is secured by the service Service_Sym_Mut_Auth_with_SM.

60 **Service_Logging:**

61 The eHC provides a file, which allows to store information about the fifty last accesses to medical data in the card. The card itself doesn't control the content of these data, it is up to the authorised persons, who have write access to these data, to write them correctly.

62 Note: The eHC may implement a PKI application, which in particular makes it possible to use the TOE as an electronic signature creation device for qualified signatures. The specification of requirements for this service is **not** covered by this PP. Annex 7.1 gives information on the combination of this PP with PPs suitable for electronic signature services.

63 In detail the functionality of the card is defined in the specifications[3]:

64 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

65 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

[3] In future these specifications may be replaced by further versions. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications.

1.2.3 TOE Type

66 The Target of Evaluation (TOE) is a smart card, the electronic Health Card (eHC), which is conformant to the specification documents [5] and [6][4]. The size of the card is type ID-1 according to ISO 7810 (the usual credit-card-size).

67 The card is a card with contacts according to ISO 7816-1 to –3. If it has an additional contactless interface, none of the eHC functions shall be accessible via this interface.

1.2.4 Required non-TOE hardware/software/firmware

68 The TOE is the electronic Health Card (contact based smart card). For the usage of this smart card an appropriate terminal resp. the health care system is necessary.

[4] In future these specifications may be replaced by further versions. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications.

1.3 TOE Description

1.3.1 TOE definition

69 The overall system including the TOE and its environment are intended to comply to the relevant German legal regulations, in particular the “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”).

70 The TOE comprises the following parts

71 **TOE_IC**, consisting of:

72 • the circuitry of the eHC’s chip (the integrated circuit, IC) and

73 • the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software

74 **TOE_ES**,

75 • the IC Embedded Software (operating system)

76 **TOE_APP**,

77 • the eHC applications (data structures and their content)

and

78 **guidance** documentation delivered together with the TOE.

79 Note: The short terms TOE_IC, TOE_ES and TOE_APP will be used were appropriate in the rest of this document in order to refer to these parts of the TOE.

1.3.2 TOE life cycle

80 The following description is a short summary of the eHC life cycle model based on a common model normally used for smart cards. The TOE life cycle is described in terms of the seven life cycle phases as usually defined for smart cards, see for example the SSVG-PP [11]. They are summarized in the following table:

Phase		Description
1	**Smartcard Embedded Software Development**	The **Smartcard Embedded Software Developer** is in charge of • the development of the Smartcard Embedded Software of the TOE, • the development of the TOE related Applications • the specification of the IC initialisation and pre-personalisation requirements (though the actual data for the IC initialisation and pre-personalisation come from Phase 4, 5 resp. 6). The purpose of the Smartcard Embedded Software and Applications designed during phase 1 is to control and protect the TOE and its different configurations during phases 4 to 7 (product usage).The global security requirements of the TOE are such that it is mandatory during the development phase to anticipate the security threats of the other phases.
2	**IC Development**	The **IC Designer** • designs the IC, • develops the IC Dedicated Software, • provides information, software or tools to the Smartcard Embedded Software Developer, and • receives the Smartcard Embedded Software from the developer through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the **IC Designer** • constructs the smartcard IC database, necessary for the IC photo mask fabrication.
3	**IC Manufacturing and Testing**	The **IC Manufacturer** is responsible for producing the IC through three main steps: • IC manufacturing, • IC testing, and • IC pre-personalisation. The **IC Mask Manufacturer**

Phase		Description
		• generates the masks for the IC manufacturing based upon an output from the smartcard IC database.
4	**IC Packaging and Testing**	The **IC Packaging Manufacturer** is responsible for • the IC packaging (production of modules) and • testing.
5	**Smartcard Product Finishing Process**	The **Smartcard Product Manufacturer (shorter also "Card Manufacturer")** is responsible for • the initialisation of the TOE (in form of the initialisation of the modules of phase 4) and • its testing. The Smartcard product finishing process comprises the embedding of the initialised modules for the TOE and the card production what may be done alternatively by the Smartcard Product Manufacturer or by his customer (e.g. Personaliser or Card Issuer).
6	**Smartcard Personali-sation**	The **Personaliser** is responsible for • the smartcard personalisation and • final tests. The personalization of the smart card includes the printing of the (cardholder specific) visual readable data onto the physical smart card, and the writing of (cardholder specific) TOE User Data and TSF Data into the smart card.
7	**Smartcard** **End-usage**	The **Smartcard Issuer** is responsible for • the smartcard product delivery to the smartcard end-user (the cardholder), and the end of life process. • The authorized personalization agents (card management systems) might be allowed to add data for a new application, modify or delete an eHC application, but not to load additional executable code. Functions used for this are specifically secured functions for this usage phase (for example the require card-to-card authentication and secure messaging). This functionality doesn't imply that the card can be switched back to an earlier life cycle stage. • The TOE is used as eHC by the smart cardholder in the End-usage phase.

Table 1: Smart Card Life Cycle Overview

81 The following paragraphs describe, how the application of the CC assurance classes is related to these phases.

82 The CC do not prescribe any specific life cycle model. However, in order to define the application of the assurance classes, the CC assume the following implicit life cycle model consisting of three phases:

83 • TOE development (including the development as well as the production of the TOE)

84 • TOE delivery

85 • TOE operational use

86 For the evaluation of the eHC the phases 1 up to 4 as defined in Table 1 are part of the TOE development in the sense of the CC. The phases 6 and 7 are part of the operational use in the sense of the CC. The phase 5 may be part of one of these CC phases or may be split between them depending on the specific model used by the TOE Manufacturer[5]. The writer of the ST shall define the exact boundary. However, this Protection Profile requires that the following conditions have to be met:

87 • All executable software in the TOE has to be covered by the evaluation.

88 • The data structures and the access rights to these data as defined in the eHC specification [5], [6] are covered by the evaluation.

89 **Application note 1**: The following examples and remarks may help ST writers to define the boundary of TOE development.

90 a. The following variations for the boundary of the TOE development are acceptable:

91 • Phase 5 completely belongs to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software and at least the data structures as defined in the specification [5], [6].

92 • The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the specification [5], [6], but isn't embedded in a plastic card yet.

93 • The TOE is delivered in (at least) two parts: The hardware as a module or already embedded in a plastic card on the one hand and a file containing parts of the initialisation data on the other hand. Both parts together again contain all software and at least the data structures as defined in the specification [5], [6] (which in particular means that all of this is evaluated during ADV activities). In this case the evaluation must also show as a result that the functions used by the customer (personaliser/card issuer) for loading the initialisation data into the hardware provide sufficient protection against modification and (where applicable) disclosure of these data.

[5] Therefore in the remaining text of this PP the TOE Manufacturer will be the subject responsible for everything up to TOE delivery and finer roles like "IC mask manufacturer" will not be distinguished any more.

94 b. The following remarks may show how some CC assurance activities apply to parts of the life cycle[6]:

95 • The ALC and ACM classes, which deal with security measures in the development environment of the TOE apply to all development and production environments of Phases 1 up to 4 and those parts of Phase 5 belonging to TOE development as defined in the ST for a TOE. In particular the sites, where the software of the TOE is developed as well as the hardware development and production sites are subject to these CC classes (for example with regard to site visits). In the context of a composite evaluation some of the phases may already be covered by a IC hardware evaluation.

96 • The measures for delivery of the TOE to the personaliser/ card issuer are subject to ALC_DEL.

97 • If the third model described in a. above is used (delivery of hardware and initialisation file), the loading of the initialisation data can be interpreted as part of installation, generation and start-up and is therefore covered by assurance class ALC and ADV.

98 • The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures are covered by AGD_PRE. Since the personaliser/card issuer is the first “user” of the TOE after delivery, the guidance documentation is mainly directed to him. He may be defined as the administrator of the TOE or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:

99 • Secure handling of the personalisation of the TOE

100 • Secure handling of delivery of the personalised TOE from the personaliser/card issuer to the cardholder.

101 • Security measures for end-usage, which the personaliser/card issuer needs to communicate to the cardholder. A simple example for this may be the requirement for the cardholder, to handle his PIN(s) securely. Since the documents accompanying the card during transport from card issuer to cardholder will probably not be available at the time of evaluation, the guidance documents for the personaliser/card issuer need to contain this information connected with the requirement that the card issuer covers all such issues in his delivery documents.

[6] These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However these explicit notes may serve as a help for ST writers and TOE developers to understand the connection between the life cycle model and some CC requirements.

2 Conformance Claim

102 This protection profile claims conformance to

103 • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, version 3.1 Revison 3, CCMB-2009-07-001

104 • Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, July 2009, version 3.1 Revision 3, CCMB-2009-07-002

105 • Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, July 2009, version 3.1 Revision 3, CCMB-2009-07-003

106 as follows

107 • Part 2 extended,

108 • Part 3 conformant,

109 • Package conformant to EAL4 augmented with AVA_VAN.5.

110 This PP requires strict conformance of any ST or PP claiming conformance to this PP.

111 This PP does not claim conformance to any other Protection Profile.

3 Security Problem Definition

112 The Security Problem Definition (SPD) is the part of a PP, which describes

113 • **assets**, which the TOE shall protect,

114 • **subjects**, who are users (human or system) of the TOE or who might be threat agents (i.e. attack the security of the assets),

115 • **Operational security policies** , which describe overall security requirements defined by the organisation in charge of the overall system including the TOE (in particular this may include legal regulations, standards and technical specifications),

116 • **threats** against the assets, which shall be averted by the TOE together with its environment,

117 • **assumptions** on security relevant properties and behaviour of the TOE's environment.

3.1 Introduction

3.1.1 Assets

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

Name of asset	**Description**	**Acronym used in eHC Specification[7]**
Personal and health insurance data (open)	Identity data or contractual data, which can be read without authentication	EF.PD, EF.VD, EF.StatusVD
Personal and health insurance data (protected)	Identity data or contractual data, which can be read only with authentication	EF.GVD

[7] In future these specifications may be replaced by further versions. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications. Therefore changes in the acronyms of assets (due to changes in the specifications) are acceptable in an ST as long as it is obvious that the same asset is meant.

Name of asset	Description	Acronym used in eHC Specification
Electronic prescription	A document containing one or more referrals (“Überweisungen”) or medications (“Verordnungen”). Note: The eHC itself cannot control, if an electronic prescription is valid. The eHC only serves as a trusted transport medium for prescriptions. In particular this has the consequence, that the right to write prescriptions into the eGK is not equivalent with the right to sign a prescription. Signing a prescription is an additional process done by a different card, for example the HPC.	EF.eRezept_Ticket, EF.eVerordnungsContainer, EF.StatusVerordnungen.
VAD (eHC)	“Verification Authentication Data”: PIN codes or a resetting code entered by a cardholder to activate certain functions of the TOE. Note: These PINs are in particular **not** the same PIN as a PIN used for qualified electronic signatures. The electronic signature PIN is not listed as an asset in this PP, since it is defined in a suitable Protection Profile for electronic signatures. For the same reason signing keys (PrK.CH.ES) are not listed here.	--
RAD (eHC)	“Reference Authentication Data”: The PINs and corresponding resetting code values stored in the TOE and used for comparison with the VAD entered by the cardholder. Note: Again this is **not** identical to similar values for an electronic signature provided by the eHC.	PIN.CH, PIN.home
Initialisation data	All data stored in the TOE during the initialisation process.	--
Personalisation data	All data stored in the TOE during personalisation process.	--
Logging data	Data stored in the TOE in order to document the last fifty accesses to medical data by care providers.	EF.Logging
Card Authentication Private Key	The Card Authentication Private Key is a asymmetric cryptographic key used for the authentication of an eHC to a HPC, to a SMC or to a service provider.	PrK.eGK.AUT_CVC
Card Verifiable Authentication Certificates	These data include Card verifiable certificates of the Card Authentication Public Key as authentication reference data corresponding to the Card Authentication Private Key and used for the card-to-card authentication. They contain encoded access rights (Role ID) and are signed by a certificate provider on behalf of the card issuer. In addition these data contain a certificate for the CA used in the case of two-step certificate verification. These data are part of the user data provided for use by external entities as authentication reference data of the eHC.	MF/EF.C…

Name of asset	Description	Acronym used in eHC Specification
Client-Server Authentication Private Keys	The Client-Server Authentication Private Keys are asymmetric cryptographic keys used for the authentication of a client application acting on behalf of the cardholder to a server.	PrK.CH.AUT, PrK.CH.AUTN
Decipher Private Keys	The Document Cipher Key Decipher Keys are asymmetric private keys used for document decryption on behalf of the cardholder.	PrK.CH.ENC, PrK.CH.ENCV
Display Message	A display message is used as a means for the Cardholder to check, if a secure channel is established. Note: Technically there are two Display messages, one is stored under DF.HCA and another one under DF.ESIGN. The latter is used in the context of the services Service_Client_Server_Auth and Service_Data_Decryption.	EF.DM
X.509 Certificates	The certificates for the keys used in the context of the services Service_Client_Server_Auth and Service_Data_Decryption. These certificates are provided by the card to other entities, which want to verify the validity of the card's keys used for these services.	EF.C.CH.
Public Keys for CV Certificate Verification	Public keys of Certification Authorities used for verification of the card verifiable certificates.	PuK.RCA.CS
Secret Keys for interaction with the "Health Insurance Agency Service Provider"	Two symmetric keys for MAC-Calculation and encryption purposes during interaction with the "Health Insurance Agency Service Provider" (The German term for this service is "Versichertenstammdaten-Dienst" (VSDD).)	SK.VSD
Secret Keys for interaction with the "Download Service Provider"	Two Symmetric keys for MAC-Calculation and encryption purposes during interaction with the "Download Service Provider" (also called card management system, CMS).	SK.CMS
Secret Keys for interaction with the "Combined Services Provider"	Two Symmetric keys for MAC-Calculation and encryption purposes during interaction with the "Combined Services Provider".	SK.VSDCMS
Permission data	These data contain information about the permissions given by the Cardholder to use specific "freiwillige Anwendungen" (these are applications in the card which may only be used if a patient has allowed this explicitly before the first use).	EF.Einwilligung
Reference data (voluntary application)	Data of so called "freiwillige Anwendungen" (these are applications which may only be used if a patient has allowed this explicitly before the first use). Note: In fact the files listed in the next column only contain "pointers" to services, which are handled outside of the TOE.	EF.Verweis

Name of asset	Description	Acronym used in eHC Specification
Emergency data	Emergency data (“Notfalldaten”) are a specific part of “medical data (voluntary application)”.	EF.eNotfalldaten, EFStatusNotfalldaten

Table 2: Assets to be protected by the TOE and its environment

3.1.2 Subjects

119 This protection profile considers the following subjects, who can interact with the TOE:

Name of subject	Description
Cardholder	The cardholder of the TOE is the legitimate user of the card, who is authenticated by use of the PIN.CH or the PIN.home. Note: The following terms are related to the cardholder: • The patient is the person who uses the eGK in order to receive e. g. treatment by a doctor. Normally the patient is identical to the cardholder. However, the patient may be incapable of using the card himself (e.g. children) and the cardholder may be a different person acting on behalf of the patient. • The insured person ("Versicherter") is the person, who has the insurance relation to the health insurance company. Usually this person is again identical to the cardholder, however the latter may be for example a child of the former. However, since the TOE cannot distinguish these roles, only the cardholder is defined as a subject in this PP.
Health Professional	Person acting as health professionals providing medical care to a patient (e.g. physician, dentist, pharmacist, psychotherapist, but also other health professionals yet to be formally defined, like midwives). These health professionals hold a HPC with a Card Verifiable Certificate of the Card Authentication Key with Role ID '2A', '3A', '4A', '5A' or '7A'. Note: As a help for the reader of the PP these Role Ids can be interpreted as follows, where access rights for an electronic prescription can be taken as example: Role Id 2A allows to write an electronic prescription to the eHC or to change it and allows comparable rights for other medical data. So typically physicians and dentists may have this Role Id. Role Id 3A also allows to read and modify/delete an (existing) electronic prescription. Typically pharmacists may have this Role ID. Role Id 4A allows no specific rights for an electronic prescription, but may allow read and write access for certain other medical information. Typically psychotherapists may have this Role Id. Role Id 5A also allows to read and modify/delete an (existing) electronic prescription and may be the Role Id for professionals not belonging to one of the preceding groups. Role Id 7A allows to read non-medical data and the emergency data and may be the Role Id for emergency personnel. The preceding examples are not necessary for the correct and secure implementation of Roles in the eGK itself, because the eGK technically only distinguishes the Role Ids and does not "know" the profession of its users.

Name of subject	Description
Medical Assistant	Persons supporting a Health Professional. These health employees usually hold a HPC with a Card Verifiable Certificate of the Card Authentication Key with a Role ID corresponding to that of the Health Professional, whom they support, i.e. ‘2A’, ‘3A’, ‘4A’, ‘5A’ or ‘7A’. The additional Role IDs '6A', '8A' and ‘9A’ are defined for specific purposes. Note that in medical institutions (e. g. hospitals) some or all of these Role Ids will also be needed for certain administrative personnel.
Security Module Card (health care) (SMC)	This security module card is used in a health care environment in order to allow interaction with the eHC in situations, where employees without a personal card provide services. The SMC has a Card Verifiable Certificate of the Card Authentication Key with a Role ID usually corresponding to that of the Health Professional, who is responsible for its operation, i. e. ‘2A’, ‘3A’, ‘4A’, ‘5A’ or ‘7A’. However, a special type of SMC for hospitals may exist, which has Role Id ‘2A’, but can be activated by HPCs with other Role Ids. The additional Role IDs '6A', '8A' and ‘9A’ are defined for specific purposes.
Self Service Terminal	A self service terminal allows a cardholder of an eHC to perform certain services. The self service terminal has an SMC with a Card Verifiable Certificate of the Card Authentication Key with Role ID ‘1A’, which is distinct from the Role Ids of the preceding subjects.
Health Insurance Agency Service Provider	The “health insurance agency service provider” interacts with the TOE on behalf of the health insurance agency. The German term for this is “Versichertenstammdaten-Dienst” (VSDD). The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.VSDD.
TOE Manufacturer	Person(s) responsible for development and production of the TOE. Note: According to the life cycle description in section 1.3.2 the initialisation of the card is either done by the TOE manufacturer or by the personalisation service provider.
Personalisation Service Provider	Person(s) responsible for personalisation of the card Methods to authenticate this role may be TOE specific and have to be defined in the Security target of a TOE. Note: This role is only responsible for the personalisation in phase 6 of the TOE’s life cycle and has no access rights in phase 7.

Name of subject	Description
Download Service Provider	Person(s) responsible for Downloading additional applications (consisting of file structures, their access rights and data) into the card in phase 7 of the TOE's lifecycle. (Also called card management system, CMS.) The service provider uses a security module (e. g. in form of a SMC), which is authenticated by use of the key SK.CMS. Note: There may be other more specific roles to produce data for the TOE like certificate service providers. However, since the card cannot distinguish such more specific roles technically according to an authentication mechanism in the card, such roles will not be defined as subjects in this PP. Additional authentication mechanisms and corresponding roles may be defined in an ST, for example for download procedures in the context of the application of qualified electronic signatures.
Combined Services Provider	Name for the combination of the Health Insurance Agency Service Provider and the Download Service Provider (in case a decision is made to combine these services or at least to allow the use of a shared key for these services).
Other Person	All persons who interact with the TOE without being authorised (as one of the preceding roles).

Table 3: Subjects

3.2 Organizational Security Policies

120 On the one hand the overall security objectives for the eHC-System can be derived mainly from the legal requirements. On the other hand the concrete security services to be provided by the TOE are defined by the specifications. For this reason the organisational security policies define the greater part of the security needs for the eHC compared to lists of individual threats.

121 OSPs will be defined in the following form:

OSP.name Short Title

Description.

122 The TOE and its environment shall comply to the following organization security policies (which are a set of security rules, procedures or guidelines for an organization, see CC part 1, sec. 4.1).

123 **OSP.eHC_Spec** Compliance to eHC specifications

124 The eHC shall be implemented according to the security relevant requirements of the specifications:

125 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

126 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

127 **Application note 2**: These specifications may be replaced by further versions in future. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications. If a ST author or evaluator is not sure, whether this is fulfilled for some future version of the specifications, he should seek guidance from the responsible CC scheme.

128 **OSP.Additional_Applications** Protection of additional Applications

129 • The TOE shall provide the possibility to authorised parties to load data for additional applications to the card. Loading of additional executable code shall not be possible.

130 • The TOE shall separate existing applications from additional applications. This means that data structures, access rights and data contents of such additional applications can not modify the security properties, in particular access control, for the existing applications.

131 • By defining access rights to the files belonging to additional applications suitably it shall be possible to provide access control to such files using the

mutual authentication services or the PIN authentication services as defined in section 1.2.2.

132 **Application note 3**: This OSP is designed to provide the functionality to add additional applications in a secure way and to provide support for their future security needs. For example, access to further medical data not covered by the current specifications of the eHC may require some kind of authentication either by a Health Professional or by the Cardholder.

133 **OSP.Electronic_Prescriptions** Access to electronic prescriptions

134 • Access to electronic prescriptions in the eHC must only be possible after authentication.

135 • Creation or modification of these data in the eHC must only be possible in connection with a HPC.

136 • The Cardholder has the following rights: He can read and also delete an electronic prescription.

137 • Access to data on an eHC for personnel without HPC may be authorized by the holder of a HPC. Such access must be logged securely.

138 • Unauthorized access or modification of these data during transport and storage must be prevented.

139 **OSP.Legal_Decisions** Legal responsibility of authorised persons

140 The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorised to deal with the data. The same holds for the decision, when data need to be deleted.

141 Note: The eHC itself cannot decide about the legal relevance and medical correctness of data stored in it.

142 **OSP.Services** Services provided by the card

143 The eHC shall provide the following services:

144 • Service_Asym_Mut_Auth_w/o_SM,

145 • Service_Asym_Mut_Auth_with_SM,

146 • Service_Sym_Mut_Auth_with_SM,

147 • Service_User_Auth_PIN and Service_User_Auth_PUC,

148 • Service_Privacy,

149 • Service_Client_Server_Auth,

150 • Service_Data_Decryption,

151 • Service_Card_Management and

152 • Service_Logging,

153 as described in section 1.2.2.

154 Note: The eHC also provides electronic signature services, however this is to be evaluated according to security requirements for electronic signüatures, e. g. from another PP. Annex 7.1 gives guidance how to combine such PP with the eHC-PP.

155 **OSP.Logging** Logging of access to medical data

156 All access to medical data (except reading access by the Cardholder himself) must be logged. Access to the log file must be protected.

3.3 Threats

157 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in the TOE.

158 Threats will be defined in the following form:

T.name Short Title

Description, for example starting “An attacker tries to...”.

3.3.1 Threats mainly addressing TOE_ES and TOE_APP

159 The TOE shall avert the threats, which are application and operating system oriented, as specified below. As potential attackers all kinds of subjects as listed in Table 3 are considered, as far as they

160 • try to perform actions, which they are not allowed by their access rights as defined in this PP and

161 • may have expertise, resources and motivation as expected from an attacker with high attack potential.

162 **T.Compromise_Internal_Data** Compromise of confidential User or TSF data

163 An attacker with high attack potential tries to compromise confidential user data or TSF data through the communication interface of the TOE by sending commands or by listening to the communication between a terminal and the TOE.

164 This threat comprises several attack scenarios e.g. guessing of the user authentication data (PIN) or reconstruction of the private decipher key using the response code for chosen cipher texts (like Bleichenbacher attack for the SSL protocol implementation).

165 **T.Forge_Internal_Data** Forge of User or TSF data

166 An attacker with high attack potential tries to forge internal user data or TSF data.

167 This threat comprises several attack scenarios of smart card forgery. The attacker may try to alter the user data e.g. to add keys for decipherment of documents. The attacker may misuse the TSF management functions to change the user authentication data to a known value.

168 **T.Misuse** Misuse of TOE functions

169 An attacker with high attack potential tries to use the TOE functions to gain access to the assets without knowledge of user authentication data or any implicit authorization.

170 This threat comprises several attack scenarios e.g. the attacker may try to circumvent the user authentication to use the DECIPHER command for document keys without authorization. The attacker may try alter the TSF data e.g. to extend the user rights after successful card-to-card authentication.

171 **T.Intercept** Interception of Communication

172 An attacker with high attack potential tries to intercept the communication between the TOE and an SMC, HPC, Download Service Provider or Health Insurance Agency Service Provider in order to read, to forge, to delete or to add other data to transmitted data classified as assets.

173 This threat comprises several attack scenarios. A health professional reads from and writes onto eHC patient's data like medication or medical data, which an attacker may read or forge during transmission. Attacker may try to read the document keys output by the TOE as DECIPHER command response. Attackers may try to manipulate card management processes.

3.3.2 Threats mainly addressing TOE_ES and TOE_IC

174 The TOE shall avert the threats, which are operating system and hardware oriented, as specified below.

175 **T.Phys_Tamper** Physical Tampering

176 An attacker with high attack potential may perform physical probing of the IC in order (i) to disclose User Data, (ii) to disclose/reconstruct the IC Embedded Software or (iii) to disclose TSF data. An attacker may physically modify the IC in order to (i) modify security features or functions of the IC, (ii) modify security functions of the IC Embedded Software, (iii) to modify User Data or (iv) to modify TSF data.

177 The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the document decipherment key) or TSF Data (e.g. authentication key of the smart card) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the IC internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

178 **T.Information_Leakage** Information Leakage from TOE's chip

179 An attacker with high attack potential may exploit information, which is leaked from the TOE during its usage in order to disclose confidential data (User Data or TSF data). The information leakage may be inherent in the normal operation or caused by the attacker.

180 Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contact less interface (emanation) or direct measurements (by contact to the chip still available even for a contact less chip) and can then be related to the specific operation being performed. No direct contact with the IC internals is required here. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA).

181 **T.Malfunction** Malfunction due to Environmental Stress

182 An attacker with high attack potential may cause a malfunction of TSF or of the IC Embedded Software by applying environmental stress in order to (I) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify security functions of the IC Embedded Software.

183 This may be achieved e.g. by operating the IC outside the normal operating conditions, exploiting errors in the IC Embedded Software or misuse of administration function. To exploit this an attacker needs information about the functional operation.

184 **T.Abuse_Func** Abuse of Functionality

185 An attacker with high attack potential may use functions of the TOE which shall not be used in TOE operational phase in order (I) to disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or manipulate TSF Data.

186 This threat address attacks using the IC as production material for the smart card and using function for personalization in the operational state after delivery of the smart card.

3.4 Assumptions

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

188 The format for assumptions will be as follows:

A.name short title

Description.

189 The following assumptions hold for the usage environment:

190 **A.Users** Adequate usage of TOE and IT-Systems in the environment.

191 The Cardholder of the TOE uses the TOE adequately. In particular he doesn't tell the PIN (or PINs) of the eHC to others and doesn't hand the card to unauthorised persons. Other actors (see subjects defined in section 3.1.2) use their data systems according to the overall system security requirements.

192 The Cardholder of the eHC needs to be informed clearly about secure usage of the product.

193 Note: In order to use the eHC securely the user needs this information. This is also required by privacy legislation.

194 **A.Perso** Secure handling of data during personalisation and additional personalisation

195 All data structures and data on the card produced during personalisation or additional personalisation steps during the end-usage phase are correct according to the specifications and are handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the eHC) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which he uses to personalize authentic smart cards, in order to prevent counterfeit of the TOE.

196 The same requirements hold for all activities belonging to Phase 5 "Initialisation", if they are executed after TOE delivery. This holds for example if the Personalisation Service Provider also sends the initialisation data to the TOE or if the TOE is delivered by the TOE Manufacturer in form of smart card modules, which are then inserted into the plastic cards at a later stage.

4 Security Objectives

197 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development and production environment and security objectives for the operational environment.

4.1 Security Objectives for the TOE

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

199 Objectives for the TOE will be defined in the following form:

OT.name short title

Description of the objective.

200 In order to support developers, who want to reuse results of a IC (hardware) evaluation or an evaluation of the card operating system, the security objectives are grouped according to the parts of the TOE.

201 **Application note 4**: The structuring described in the preceding paragraph does not imply that the developer of a Security Target for a specific eHC needs to follow this distinction. In other words: If for example an objective, which is listed here as TOE_ES oriented, is covered by the hardware level or by the application level of a specific card, or by a combination of these, then this is of course acceptable. The developer doesn't even need to explicitly distinguish the levels in the same way.

4.1.1 Security objectives, which are mainly TOE_App oriented

202 **OT.Access_Rights** Access control policy for data in the TOE

203 In the End Usage Phase the TOE shall implement the access control policy **SFP_access_rules**, which is defined in the following table:

SFP_access_rules

The following subjects may interact with the TOE (see also section 3.1.2, Table 3):

Cardholder, Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, TOE Manufacturer, Personalisation Service Provider, Download Service Provider, Combined Services Provider, Other Person

The following objects are covered by the policy (see also section 3.1.1, Table 2):

Personal and health insurance data (open), Personal and health insurance data (protected), electronic prescription, VAD (eHC), RAD (eHC), logging data, Card Authentication Private Key, Card Verifiable Authentication Certificates, Client-Server Authentication Private Keys, Decipher Private Keys, Display Message, X.509 Certificates, Public Keys for CV Certificate Verification, SK.VSD, SK.CMS, permission data, reference data (voluntary application), emergency data.

Note: initialisation data and personalisation data are terms used for data written during the corresponding life cycle phases. For the End Usage Phase all assets are covered by the data already listed above.

The following authentication methods are covered by the policy:

The services Service_Asym_Mut_Auth_w/o_SM, Service_Asym_Mut_Auth_with_SM, Service_Sym_Mut_Auth_with_SM, Service_User_Auth_PIN, Service_User_Auth_PUC as defined in chapter 1.2.2 “TOE description”.

The following security attributes for subjects are maintained by the TOE:

For every authentication method the TOE maintains the status of successful authentication (successful PIN verification, successful mutual authentication). (These are security attributes for the connected subject, because the TOE derives the access rights from these attributes).

SFP_access_rules

The following access methods are maintained by the TOE:

Access is allowed only using the defined command interface of the TOE. In other words: A subject sends a command APDU as defined in the eHC specification to the TOE and the TOE processes it.

Access to eHC data is not allowed via a contact-less interface.

Requirements for encryption or MAC-protection (Using Secure Messaging) will be included in addition for access to some of the data.

The following types of access are used in the rules below:

“Read”, “write”, “delete”, “deactivate” (this means making data invisible for other subjects, but without deleting them), “activate” (making deactivated data visible again), “use” (a command is called, which uses data internally, this is relevant for cryptographic keys).

As specific variants of the write access the following terms are used: “Modify” means to change existing data. “Append” means to add data at the end of existing data. “Create” means to create new data structures.

The following access rules are defined for the TOE’s objects:

For all files and other security relevant data (PINs, keys) the TOE maintains the following access rules as defined in the eHC specification, Part 2. Note, that these rules hold for the End Usage Phase of the TOE.

Rule_1:

Personal and health insurance data (open) may be read by all subjects and written only by the Health Insurance Agency Service Provider or Combined Services Provider. Writing of these data requires secure messaging with MAC. The Download Service Provider and the Combined Services Provider have the right to delete the data. The commands used for this require protection by secure messaging with MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).

Rule_2:

Personal and health insurance data (protected) can be read by: Cardholder, Health Professional, Medical Assistant, Security Module Card (health care) (Role ‘7A’ requires additional authentication of the Cardholder with PIN.CH), Combined Services Provider and Health Insurance Agency Service Provider. They can be written by the Health Insurance Agency Service Provider and Combined Services Provider. Writing of these data requires secure messaging with encryption and MAC. Reading data also requires secure messaging with encryption (of the response) and MAC in the case of Health Insurance Agency Service Provider or Combined Services Provider.

Rule_3:

Data of type electronic prescription can be read or deleted by Health Professional, Medical Assistant, Security Module Card (health care) with one of the Role IDs ‘2A’, ‘3A’, ‘5A’, '6A' and ‘9A’ (the last one only in connection with PIN.CH.

The Cardholder can read the data and he has the following rights: He can deactivate or activate and also delete an electronic prescription.

Only Health Professional, Medical Assistant and Security Module Card (health care) with one of the Role IDs ‘2A’, ‘3A’, ‘5A’ or

SFP_access_rules
'6A' can write these data. Note: Technically the ability of the Cardholder to delete an electronic prescription is realised by the right to modify EF.eVerordnungsTicket. The confidentiality of the contents of the electronic prescription is ensured by encryption of the EF.eVerordnungsContainer with a key stored in EF.eVerordnungsTicket. The Download Service Provider and the Combined Services Provider have the right to delete EF.eVerordnungsContainer. The commands used for this require protection by secure messaging with MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).
Rule_4: Data of type RAD (eHC): The PIN.CH and PIN.home may be modified by the Cardholder, the resetting code (PUC) cannot be modified. Both data can not be read by anyone. The retry counter for the PIN can be reset by the Cardholder after authentication with the PUC. Note: VAD (eHC) stands for PIN or resetting code values, which are entered by the Cardholder in clear text and therefore require no specific rules by this policy.
Rule_5: The logging data can be written by Health Professional, Medical Assistant, Security Module Card (health care) and by the Self Service Terminal (the last case requires additional authentication with PIN.CH). Only new entries can be appended, existing entries can not be modified (however, when fifty entries are full, the oldest entry is deleted, when adding a new one). The data can be read by the Cardholder.
Rule_6: The Card Authentication Private Key can never be read or written. It can be used in the services Service_Asym_Mut_Auth_w/o_SM and Service_Asym_Mut_Auth_with_SM. These services include the verification of a CV certificate for the card or security module, with which the TOE interacts during the service.
Rule_7: The Card Verifiable Authentication Certificate can always be read and never written.
Rule_8: The Client-Server Authentication Private Keys and the Decipher Private Keys cannot be read or written, they can only be used in the corresponding services Service_Client_Server_Auth and Service_Data_Decryption. For the keys PrK.CH.AUT and Prk.CH.ENC respectively both services are possible only after authentication by the Cardholder (either with PIN.home or with PIN.CH combined with one of the roles '1A', '2A', '3A', '4A', '5A', '6A', in case of PrK.CH.Aut also PIN.CH combined with role '9A'). For the second authentication key PrK.CH.AUTN the service Service_Client_Server_Auth is allowed for the Cardholder or after authentication by Health Professional, Medical Assistant, Security Module Card (health care), all of these with Role ID

SFP_access_rules
'2A', '3A', '4A', '5A', '6A', '8A', '9A'. For the second decryption key PrK.CH.ENCV the service Service_Data_Decryption is allowed for the Cardholder or after authentication by Health Professional, Medical Assistant, Security Module Card (health care) all of these with Role ID '2A', '3A', '4A', '5A', '6A'. In addition it is allowed for Role ID '9A' in connection with PIN.CH.
Rule_9: The Public Keys for CV Certificate Verification can never be written. It can be used for verification of certificates. Note: Additional Public keys may be stored temporarily in case of cross-certification. The above rule holds for the "root" key of the eHC.
Rule_10: The symmetric keys SK.VSD, SK.VSDCMS and SK.CMS cannot be read or written. They can be used for establishment of trusted channels by the service Service_Sym_Mut_Auth_with_SM.
Rule_11: Files and other data structures necessary for additional applications can be created by the Download Service Provider or the Combined Services Provider. The commands used for this require protection by secure messaging with encryption (of the command message) and MAC.
Rule_12: The Download Service Provider and the Combined Services Provider have the right to deactivate the complete health care application, which means that the card isn't usable as an eHC any more. They can also re-activate the application. The commands used for this require protection by secure messaging with MAC (and therefore authentication by the service Service_Sym_Mut_Auth_with_SM).
Rule_13: The Display Message can be written only by the Cardholder. It can be read only by use of secure messaging, which requires authentication using the service Service_Asym_Mut_Auth_with_SM or Service_Sym_Mut_Auth_with_SM. Note: This allows to demonstrate the establishment of a secure channel to the cardholder.
Rule_14: The X.509 Certificates EF.C.CH.AUT and EF.C.CH.ENC can be read by everybody. Reading EF.C.CH.AUTN and EF.C.CH.ENCV is allowed for the Cardholder, the Download Service Provider and the Combined Services Provider and for entities authenticated as one of the Role Ids '2A', '3A', '4A', '5A', '6A'. In addition EF.C.CH.AUTN can be read for Role IDs '8A' and '9A', while EF.C.CH.ENCV can be read for Role ID ')A' in connection with PIN.CH. All of the X.509 Certificates can be written by the Download Service Provider and the Combined Services Provider. Reading and writing by these entities requires protection by secure messaging with encryption for EF.C.CH.AUT and EF.C.CH.ENC and MAC for all of them.

SFP_access_rules
Rule_15: The permission data can be read by the Cardholder (using PIN.home or PIN.CH in combination with a Self Service Terminal), and by those Health Professional, Medical Assistant, Security Module Card (health care), who have Role Ids ‘2A’, ‘3A’, ‘4A’ or '6A'. They can be written by those Health Professional, Medical Assistant and Security Module Card (health care) with Role ID ‘2A’, ‘3A’ or ‘4A’. Reading and writing requires additional authentication using PIN.CH (except if the Cardholder reads or writes using PIN.home). They can be deactivated and activated by the Cardholder in connection with a Self Service Terminal and by authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’ in combination with PIN.CH.
Rule_16: The reference data (voluntary application) can be read by the Cardholder and by all authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’, ‘6A’, ‘9A’ in combination with PIN.CH. They can be written by the Cardholder and by Health Professional, by Medical Assistant and by Security Module Card (health care) with specific Role IDs ‘2A’, ‘3A’, ‘4A’ or ‘9A’ together with the Cardholder (using PIN.CH). They can be deactivated and activated by the Cardholder in connection with a Self Service Terminal and by authenticated subjects with role ID ‘2A’, ‘3A’, ‘4A’ in combination with PIN.CH.
Rule_17: The emergency data can be written by Health Professional, Medical Assistant and Security Module Card (health care) with Role ID '2A' but only together with the Cardholder (PIN.CH). They can be read by all Health Professional, Medical Assistant, Security Module Card (health care) with one of the Role Ids ‘2A’, ‘7A’, '3A' or '4A', but for the last two IDs only together with the Cardholder (PIN.CH). They can be deactivated or activated by the Cardholder.

Table 4: Access Control Policy for Usage Phase

204 **Application note 5**: The specifications [5] and [6] of the card may be replaced by further versions in future. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications. For the access control policy “SFP_access_rules” this is interpreted as follows: If newer versions of the specifications define the access conditions more restrictively then the SFP above (for example allow access to a specific asset for fewer roles then defined above), this will be acceptable and an ST author may modify the SFP in this way.

4.1.2 Security Objectives, which are mainly TOE_ES oriented

205 The TOE security objectives in this section are those, which will probably be addressed by the TOE operating system.

206 The following objectives all refer to the specifications of the eHC:

207 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

208 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

209 The following objectives shall be upheld by the TOE:

210 **OT.AC_Pers** Access control for personalization

211 The TOE must ensure that the personalisation data can be written by an authorized Personalisation Service Provider only.

212 **OT.Additional_Applications** Protection of additional Applications

213 • The TOE shall provide the possibility to authorised parties to load data for additional applications to the card. Loading of additional executable code shall not be possible.

214 • The TOE shall separate existing applications from additional applications. This means that data structures, access rights and data contents of such additional applications can not modify the security properties, in particular access control, for the existing applications.

215 • By defining access rights to the files belonging to additional applications suitably it shall be possible to provide access control to such files using the mutual authentication services or the PIN authentication services as defined in section 1.2.2.

216 **Application note 6**: This objective is designed to provide the functionality to add additional applications in a secure way and to provide support for their future security needs.

217 **OT.Services** Services provided by the Card

218 The eHC shall provide the following services:

219 • Service_Asym_Mut_Auth_w/o_SM,

220 • Service_Asym_Mut_Auth_with_SM,

221 • Service_Sym_Mut_Auth_with_SM,

222 • Service_User_Auth_PIN and Service_User_Auth_PUC,

223 • Service_Privacy,

224 • Service_Client_Server_Auth,

225 • Service_Data_Decryption,

226 • Service_Card_Management and

227 • Service_Logging

228 as described in section 1.2.2.

229 Note: The eHC also provides electronic signature services, however this is to be evaluated according to security requirements for electronic signatures, e.g. from another PP. Annex 7.1 gives guidance how to combine such PP with the eHC-PP.

230 **OT.Cryptography** Implementation of cryptographic algorithms

231 The cryptographic algorithms required by the eHC specifications, Part 1, (see [5]) are implemented according to their definition.

232 These algorithms are not explicitly listed in this PP in order to allow future development of the specifications.

4.1.3 Security Objectives, which are mainly TOE_IC oriented

233 The following TOE security objectives are drawn from BSI-PP-0002 [11] and address the protection provided mainly by TOE_IC (however it may use support by the other components of the TOE) and independent off the TOE environment.

234 **Application note 7**: This should allow a developer to use the method of composite evaluation with a hardware already evaluated according to BSI-PP-0002.

235 **OT.Prot_Inf_Leak** Protection against Information Leakage

236 The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the TOE's chip

237 • by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

238 • by forcing a malfunction of the TOE and/or

239 • by a physical manipulation of the TOE.

240 **Application note 8:** This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

241 **OT.Prot_Phys_Tamper** Protection against Physical Tampering

242 The TOE must provide protection the confidentiality and integrity of the User Data, the TSF Data, and the chip Embedded Software. This includes protection against attacks with high attack potential by means of

243 • measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

244 • measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

245 • manipulation of the hardware and its security features, as well as

246 • controlled manipulation of memory contents (User Data, TSF Data).

247 with a prior

248 • reverse-engineering to understand the design and its properties and functions.

249 **Application note 9:** In order to meet the security objectives OT.Prot_Phys_Tamper the TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

250 **OT.Prot_Malfunction** Protection against Malfunctions

251 The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

252 **Application note 10:** A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys_Tamper) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

253 **OT.Prot_Abuse_Func** Protection against Abuse of Functionality

254 The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (I) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Softcoded Smartcard Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

4.2 Security Objectives for the Operational Environment

255 **OE.Users** Adequate usage of TOE and IT-Systems in the environment

256 The Cardholder of the TOE needs to use the TOE adequately. In particular he mustn't tell the PIN (or PINs) of the eHC to others and mustn't hand the card to unauthorised persons.

257 **OE.Legal_Decisions** Legal responsibility of authorised persons

258 The decision, which data are legally feasible for storage on the eHC has to be made by the persons authorised to deal with the data. The same holds for the decision, when data need to be deleted. These persons must use their IT systems according to the legal requirements.

259 This objective holds for all subjects (or the persons controlling them, if the subjects themselves are technical devices) listed in section 3.1.2, Table 3, except the Cardholder (who's behaviour is covered by other objectives) and the category "Other Person", which includes attackers.

260 **OE.Data_Protection** Protection of sensitive data outside of the eHC

261 The persons responsible for the handling of sensitive data outside of the eHC (this includes medical data, PINs, cryptographic keys and sensitive personal data, see the definition of assets in Table 1) use adequate protection for confidentiality and integrity of these data.

262 **OE.Perso** Secure handling of data during personalisation and additional personalisation

263 All data structures and data on the card produced during personalisation or additional personalisation steps during the end-usage phase must be correct according to the specifications and must be handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for the eHC) and their confidential handling. The Personalisation Service Provider must control all materials, equipment and information needed to personalize authentic smart cards in order to prevent counterfeit of the TOE.

264 The same requirements hold for all activities belonging to Phase 5 "Initialisation", if they are executed after TOE delivery. This holds for example if the Personalisation Service Provider also sends the initialisation data to the TOE or if the TOE is delivered by the TOE Manufacturer in form of smart card modules, which are then inserted into the plastic cards at a later stage.

265 **Application note 11:** The security objectives for the environment are very important for the security of the system, in which the eHC is used. According to the requirements defined in the assurance class AGD the user guidance of the TOE will therefore

contain more detailed information about measures to support these objectives. The following considerations may be helpful for this:

266 • If communication between the TOE and another device is done across insecure networks, only services secured by secure messaging must be used. A typical example would be an internet apothecary. The end user must be informed about his possibilities to check this (e. g. how to use the Display Message in order to see that a secure channel was established).

267 • The concept of the two PINs PIN.CH and PIN.home have to be made clear to the Cardholder, in particular he needs to be informed, that the PIN.home must only be used in his private environment or at a Self Service Terminal. In any other IT system of a medical practice or apothecary only PIN.HC must be used. If the Cardholder wants to make real use of the privacy features like activation or deactivation of certain data, he needs to make sure that PIN.CH and PIN.home have distinct values.

268 • The procedures used by the card issuer in order to deliver the eHC as well as PINs and PUCs to the Cardholder must be suitable to prevent attackers from successfully intercepting and using the eHC and the PIN and/or PUC. The requirements defined by gematik in the document [7] (in the version valid at the time of evaluation) will have to be fulfilled and the guidance documentation (e.g. for the Personalisation Service Provider) will have to describe the procedures adequately.

269 • The environment, where the Cardholder enters his PIN, must make sure that the PIN is not intercepted on the line between the device, where the PIN is entered and the TOE.

270 • Similarly, all environments, where authentication (e. g. of a HPC) without secure messaging is used, must ensure that interception or modification of the sensitive data is not possible on the line between the TOE and other devices. They must also prevent unauthorised persons from sending card commands to the TOE after such type of authentication.

271 • If the Service_Data_Decryption is used the environment must ensure that the deciphered data (usually document encipherment keys) are not intercepted during transport outside of the TOE.

272 • If medical data are stored outside of the eGK, for example on a Server, then appropriate access control needs to be in place to prevent unauthorised read or write access to these data.

273 • Of course all parties, which have management access to the TOE (Health Insurance Agency Service Provider, Personalisation Service Provider, Download Service Provider) must ensure that their activities maintain the security of the TOE and its data.

4.3 Security Objectives Rationale

274 The following table shows, which Objectives for the TOE and the environment support which OSP, help to avert which threat and correspond to which assumption. The table shows, that for every OSP, threat and assumption there is at least one objective and vice versa.

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func	OE.Users	OE.Legal_Decisions	OE.Data_Protection	OE.Perso
OSP.eHC_Spec	X	X	X	X	X								
OSP.Additional_Applications			X										X
OSP.Electronic_Prescriptions		X									X	X	
OSP.Legal_Decisions											X		
OSP.Services				X									
OSP.Logging		X		X							X		
T.Compromise_Internal_Data	X	X		X	X						X	X	
T.Forge_Internal_Data	X	X		X	X						X	X	
T.Misuse	X	X		X	X						X	X	
T.Intercept	X	X		X	X						X	X	
T.Phys_Tamper							X						
T.Information_Leakage						X							
T.Malfunction								X					
T.Abuse_Func									X				
A.Users										X			
A.Perso													X

Table 5: Mapping of objectives to OSPs, threats, assumptions

275 The following text describes for every OSP, Threat and Assumption, how they are covered by Security Objectives.

276 The organizational security policy **OSP.eHC_Spec** "Compliance to eHC specifications" is implemented by the following TOE security objectives:

277 • OT.Services requires that the TOE provides the security services, which are realised by the commands defined in the specification.

278 • OT.Cryptography requires that the cryptographic algorithms as defined in the specification are implemented.

279 • OT.Access_Rights requires that the access rights are defined according to the policy SFP_access_rules. These rules are chosen according to the access rights defined in the eHC specification, part 2.

280 • OT.Additional_Applications requires rules for the loading of additional applications, which is also compatible to the definitions in the specifications.

281 • The objective for the TOE environment OE.Perso "Secure personalization" (together with OT.AC_Pers "Access control for personalization" protecting the personalization functions of the TOE) ensure that the Personalisation Service Provider will provide a genuine TOE initialized and personalized according to the specification to the Cardholder.

282 **OSP.Additional_Applications** is fully covered by OT.Additional_Applications, which is essentially identical to OSP.Additional_Applications. In addition it is supported by OE.Perso because this security objective requires adequate organisational security, when loading additional applications during the operational phase.

283 **OSP.Electronic_Prescriptions** is covered by the combination of

284 • OT.Access_Rights, which restricts the access rights to the data in the card as required by OSP.Electronic_Prescriptions (see rule for the asset "electronic prescription").

285 • OE.Data_Protection, which requires adequate protection of the medical data, when handled outside of the card.

286 • OE.Legal_Decisions, which requires use of IT systems according to legal requirements by authorised persons. This in particular implies that the access possibilities by HPC or SMC cards to data in the eHC is used according to the legal requirements.

287 **OSP.Legal_Decisions** is fully covered by OE.Legal_Decisions, which is essentially identical to OSP.Legal_Decisions.

288 **OSP.Services** is fully covered by OT.Services, which is essentially identical to OSP.Services.

289 **OSP.Logging** is realised in cooperation between the TOE and its operational environment:

290 • According to OT.Services the TOE provides the service “Service_Logging”. This service allows authorised users to write logging data into the card.

291 • According to OE.Legal_Decisions all authorised users are responsible for the correctness of the logging data, they write into the card. This compensates for the fact that the card cannot control the content of this file.

292 • According to OT.Access_Rights, access to the log file is protected.

293 The threats **T.Compromise_Internal_Data**, **T.Forge_Internal_Data**, **T.Misuse** and **T.Intercept** are all countered by the following combination of objectives:

294 • OT.Access_Rights (supported by OT.Services, OT.Cryptography) implies that data in the TOE can only be read, written or modified according to the access rules as defined in the access control policy SFP_access_rules, which was defined in OT.Access_Rights. The support by OT.Services is needed since several rules of SFP_access_rules restrict the access to certain subjects (Cardholder, Health Professional, etc.) the authenticity of which is made sure by services required by OT.Services (e. g. Service_User_Auth_PIN, Service_Sym_Mut_Auth_with_SM, Service_Asym_Mut_Auth_with_SM, cf. section 1.2.2). The support by OT.Cryptography is needed since several services required by OT.Services rely on cryptographic mechanisms required by OT.Cryptography (e. g. a symmetric encryption algorithm is needed for Service_Sym_Mut_Auth_with_SM, an asymmetric algorithm for Service_Asym_Mut_Auth_with_SM).

295 • OT.AC_Pers protects the personalization functions of the TOE against unauthorised use.

296 • OE.Legal_Decisions and OE.Data_Protection imply that authorised persons, who are allowed to read, write or modify data in the card, use these rights only in an environment, where unauthorised access to these data is prevented by the environment.

297 An example for this is as follows: The service Service_Asym_Mut_Auth_w/o_SM allows Health Professionals to access electronic prescriptions in the card. This is allowed only in a closed environment, where attackers cannot access the data transmitted between eHC and the health professionals IT equipment. For the case of transmission over insecure lines the service Service_Asym_Mut_Auth_with_SM is provided and the objectives for the environment imply that health professionals use these services adequately.

298 The threat **T.Phys_Tamper** “Physical Tampering” is averted directly by the security objective OT.Prot_Phys_Tamper “Protection against physical tampering”.

299 The threat **T.Information_Leakage** “Information Leakage from smart card chip” is averted directly by the security objective OT.Prot_Inf_Leak “Protection against information leakage” addressing the protection against disclosure of confidential data

(User Data or TSF data) stored and/or processed in the TOE by attacks including but not limited to use of side channels, fault injection or physical manipulation.

300 The threat **T.Malfunction** “Malfunction due to Environmental Stress” is averted directly by the security objective OT.Prot_Malfunction “Protection against Malfunctions”.

301 The threat **T.Abuse_Func** “Abuse of Functionality” is averted directly by the security objective OT.Prot_Abuse_Func “Protection against abuse of functionality” preventing the use of TOE functions which are intended for the testing, the initialization and the personalization of the TOE and which must not be accessible after TOE delivery.

302 The security objective for the environment OE.Users “Adequate usage of TOE and IT-Systems” implements directly the assumption **A.Users** “Adequate usage of TOE and IT-Systems”.

303 The security objective for the environment OE.Perso “Secure personalization” implements the assumption **A.Perso** “Personalization of the Smart Card”.

5 Extended Components Definition

304 This protection profile uses components defined as extensions to CC part 2. Some of these components are defined in [11], other components are defined in this protection profile.

5.1 Definition of the Family FCS_RND

305 To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

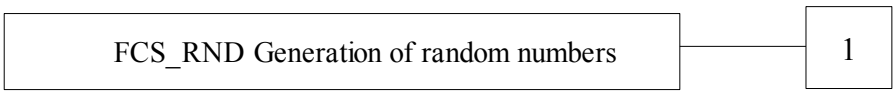
306 The family “Generation of random numbers (FCS_RND)” is specified as follows.

307 **FCS_RND Generation of random numbers**

308 Family behaviour

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

310 Component levelling:



311 FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

312 Management: FCS_RND.1

313 There are no management activities foreseen.

314 Audit: FCS_RND.1

315 There are no actions defined to be auditable.

316 **FCS_RND.1** Quality metric for random numbers

317 Hierarchical to: No other components.

318 Dependencies: No dependencies.

319 FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.2 Definition of the Family FMT_LIM

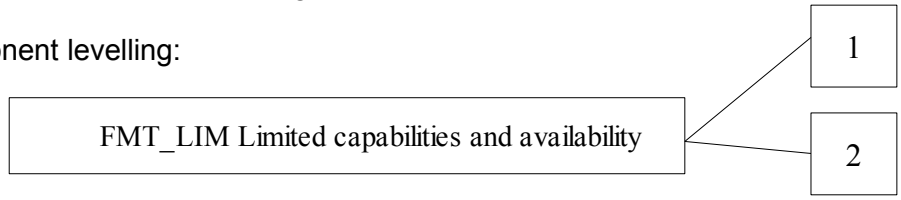
320 The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

321 **FMT_LIM Limited capabilities and availability**

322 Family behaviour

323 This family defines requirements that limits the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

324 Component levelling:



325 FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

326 FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

327 Management: FMT_LIM.1, FMT_LIM.2

328 There are no management activities foreseen.

329 Audit: FMT_LIM.1, FMT_LIM.2

330 There are no actions defined to be auditable.

331 To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

332 The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

333 **FMT_LIM.1** Limited capabilities

334 Hierarchical to: No other components.

335 Dependencies: FMT_LIM.2 Limited availability.

336 FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].

337 The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

338 **FMT_LIM.2** Limited availability

339 Hierarchical to: No other components.

340 Dependencies: FMT_LIM.1 Limited capabilities.

341 FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: *Limited capability and availability policy*].

342 **Application note 12**: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

343 (i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

344 or conversely

345 (ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

346 The combination of both requirements shall enforce the policy.

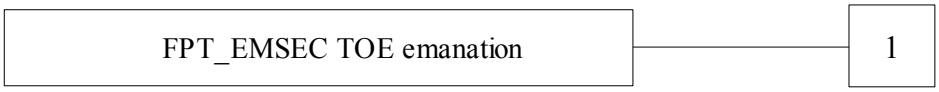
5.3 Definition of the Family FPT_EMSEC

347 The family “TOE Emanation (FPT_EMSEC)” is specified as follows.

348 Family behaviour

349 This family defines requirements to mitigate intelligible emanations.

350 Component levelling:



351 FPT_EMSEC.1 TOE emanation has two constituents:

352 FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

353 FPT_EMSEC.1.2 Interface Emanation requires not emit interface emanation enabling access to TSF data or user data.

354 Management: FPT_EMSEC.1

355 There are no management activities foreseen.

356 Audit: FPT_EMSEC.1

357 There are no actions defined to be auditable.

358 **FPT_EMSEC.1 TOE Emanation**

359 Hierarchical to: No other components.

360 Dependencies: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Requirements

361 The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in Part 2 of the CC. Each of these operations is used in this PP.

362 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is either

- denoted by the word “refinement” in bold text and the added/changed words are in bold text or
- included in text as underlined text and marked by a footnote.

363 In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

364 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*.

365 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*.

366 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

367 This section on security functional requirements (SFR) for the TOE is divided into sub-sections following the main security functionality. They are usually ordered as in CC part 2 [2].

6.1.1 Cryptographic support (FCS)

368 **Application note 13**: In agreement with BSI all explicit references to specific cryptographic algorithms were removed from this PP in order to allow future migration to new algorithms. Instead the authors of conforming STs shall refer to the algorithms defined in the eHC specification, part 1 [5], in the version valid at the time of ST evaluation. The specification will be kept in compliance with the following specific additional documents, which shall be used in the version valid at the time of ST evaluation:

369 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

370 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

371 The TOE shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below (Common Criteria Part 2).

372 **FCS_CKM.1/SM Cryptographic key generation – Secure Messaging Keys**

373 Hierarchical to: No other components.

FCS_CKM.1.1/SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm card-to-card authentication with secure messaging [8] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5] [9].

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

375 **Application note 14:** The Key Generation is done during a mutual authentication with trusted channel establishment. The Authentication Protocol produces agreed parameters to generate the encryption key and the message authentication keys for secure messaging. The algorithm uses random numbers generated by the TSF as required by FCS_RND.1.

[8] [*assignment: cryptographic key generation algorithm*]

[9] [assignment: *list of standards*]

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

377 **FCS_CKM.4 Cryptographic key destruction**

378 Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

379 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]

380 **Application note 15:** The TOE shall destroy the encryption session key and the message authentication session keys for secure messaging after reset or termination of secure messaging session or reaching fail secure state according to FPT_FLS.1.

381 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.

382 **FCS_COP.1/Hash Cryptographic operation – Hash Algorithm**

Hierarchical to: No other components.

FCS_COP.1.1/Hash The TSF shall perform hashing [10] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes none [11] that meet the following: eHC specification, Part 1 [5] [12].

383 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

384 **Application note 16**: This SFR requires the TOE to implement the hash function.

385 **Application note 17**: Depending on the publication of the RegTP on algorithms suitable for electronic signatures [8], additional hash functions may be specified by the author of a Security Target.

[10] [assignment: *list of cryptographic operations*]

[11] [assignment: *cryptographic key sizes*]

[12] [assignment: *list of standards*]

386 **FCS_COP.1/CCA_SIGN Cryptographic operation – Digital Signature-Creation for Card-to-Card Authentication**

387 Hierarchical to: No other components.

FCS_COP.1.1/CCA_SIGN	The TSF shall perform digital signature-creation[13] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][14].

388 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

389 **Application note 18:** This SFR requires the TOE to implement the cryptographic primitive of the digital signature-creation for the card-to-card authentication mechanism according the eHC specification.

390 **FCS_COP.1/CCA_VERIF Cryptographic operation – Digital Signature-Verification for Card-to-Card Authentication**

391 Hierarchical to: No other components.

FCS_COP.1.1/CCA_VERIF	The TSF shall perform digital signature-verification[15] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][16].

392 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

393 **Application note 19:** This SFR requires the TOE to implement the cryptographic primitive of the digital signature-verification for the card-to-card authentication mechanism according to the eHC specification.

13 [assignment: *list of cryptographic operations*]

14 [assignment: *list of standards*]

15 [assignment: *list of cryptographic operations*]

16 [assignment: *list of standards*]

394 **FCS_COP.1/CSA Cryptographic operation – Digital Signature-Creation for Client-Server Authentication**

395 Hierarchical to: No other components.

FCS_COP.1.1/CSA The TSF shall perform digital signature-creation[17] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][18].

396 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

397 **Application note 20:** This SFR requires the TOE to implement the cryptographic primitive of the digital signature-creation for the client-server authentication mechanism according to the eHC specification.

398 **FCS_COP.1/Asym_DEC Cryptographic operation – Asymmetric Decryption**

399 Hierarchical to: No other components.

FCS_COP.1.1/ASYM_DEC The TSF shall perform decryption[19] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][20].

400 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

401 **Application note 21:** This SFR requires the TOE to implement the cryptographic primitive of the asymmetric decryption.

[17] [assignment: *list of cryptographic operations*]

[18] [assignment: *list of standards*]

[19] [assignment: *list of cryptographic operations*]

[20] [assignment: *list of standards*]

402 **FCS_COP.1/Sym Cryptographic operation – Symmetric Encryption / Decryption**

403 Hierarchical to: No other components.

FCS_COP.1.1/Sym The TSF shall perform encryption and decryption[21] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][22].

404 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

405 **Application note 22:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging and for possible other uses of a symmetric encryption algorithm.

406 **FCS_COP.1/MAC Cryptographic operation – MAC**

407 Hierarchical to: No other components.

FCS_COP.1.1/MAC The TSF shall perform generation and verification of message authentication code[23] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: eHC specification, Part 1 [5][24].

408 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

409 **Application note 23:** This SFR requires the TOE to implement the cryptographic primitive for secure messaging.

410 The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified in section 5.1 (Common Criteria Part 2 extended).

21 [assignment: *list of cryptographic operations*]

22 [assignment: *list of standards*]

23 [assignment: *list of cryptographic operations*]

24 [assignment: *list of standards*]

411 **FCS_RND.1 Quality metric for random numbers**

412 Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

413 Dependencies: No dependencies.

414 **Application note 24:** This SFR requires the TOE to generate random numbers used for (i) the authentication protocols as required by FIA_UAU.4, and (ii) the key agreement FCS_CKM.1/SM for secure messaging. The quality metric shall be chosen to ensure the strength of function high.

6.1.2 Identification and Authentication

415 The TOE shall meet the requirement “Authentication failure handling (FIA_AFL.1)” as specified below (Common Criteria Part 2).

416 **FIA_AFL.1/PIN Authentication failure handling – eHC-PIN**

417 Hierarchical to: No other components.

FIA_AFL.1.1/PIN	The TSF shall detect when [selection: [assignment: *positive integer number*], *an administrator configurable positive integer within* [assignment*: range of acceptable values*]] unsuccessful authentication attempts occur related to consecutive failed human user authentication for the health care application[25].
FIA_AFL.1.2/PIN	When the defined number of unsuccessful authentication attempts has been [selection: *met or surpassed*], the TSF shall block the PIN for authentication until successful unblock with resetting code[26].

418 Dependencies: FIA_UAU.1 Timing of authentication.

419 **Application note 25:** The component FIA_AFL.1/PIN addresses the human user authentication by means of the PINs (PIN.CH and PIN.home) for the health care application. The security target writer shall select the parameters with respect to the high strength of the authentication function, e.g. a PIN length of six and a retry counter value of three are acceptable.

420 **Application note 26:** For the electronic signature service another specific PIN will be used, for which this SFR may be iterated.

[25] [*assignment: list of authentication events*]

[26] [assignment: *list of actions*]

421 **FIA_AFL.1/PUC Authentication Failure Handling – eHC-PIN-unblocking code**

422 Hierarchical to: No other components.

FIA_AFL.1.1/PUC The TSF shall detect when [assignment*: positive integer number]*[27] ~~unsuccessful~~[28] attempts occur related to usage of the eHC-PIN unblocking code[29].

FIA_AFL.1.2/PUC When the defined number of ~~unsuccessful~~[30] authentication attempts has been [selection: *met or surpassed*], the TSF shall [assignment: *list of actions, which at least includes: block the PIN unblocking code*][31].

423 Dependencies: FIA_UAU.1 Timing of authentication

424 **Application note 27:** The component FIA_AFL.1/PUC address the human user authentication by means of the PIN unblocking code for the PINs used for the health care application. The ST writer shall consider the effect for the high strength of the authentication function e.g. a PUC length of eight and a usage counter value of ten are acceptable.

425 The TOE shall meet the requirement “User attribute definition (FIA_ATD.1)” as specified below (Common Criteria Part 2).

426 **FIA_ATD.1 User attribute definition**

427 Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: identity and role[32].

428 Dependencies: No dependencies.

429 **Application note 28:** The component FIA_ATD.1 applies to (i) the human user authentication, i.e. the Cardholder, whose identity is given in the Personal and health insurance data (open), and to (ii) the card-to-card authentication where the identity (i.e. the ICCSN.ICC) and the role (i.e. Role ID) are encoded in the CV certificate.

---

27 *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]*

28 refinement: not only unsuccessful but all attempts shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled

29 [assignment: *list of authentication events*]

30 refinement: not only unsuccessful but all shall be counted here – obviously this refinement is valid, because the original requirement is still fulfilled

31 [assignment: *list of actions*] with refinement of the list of actions – obviously this refinement is valid, because the original requirement is still fulfilled

32 [assignment: *list of security attributes*]

430 **FIA_UID.1 Timing of identification**

431 Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow

(1) reading the ATR,
(2) reading the Card Verifiable Authentication Certificate,
(3) reading the Certificate Service Provider Certificate,
(4) [assignment: *list of TSF-mediated actions*][33]

on behalf of the user to be performed before the user is identified.

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

432 Dependencies: No dependencies.

433 **Application note 29:** This SFR is meant to support the access control policy **SFP_access_rules**. Note, that access rules for initialisation and personalisation phases are defined by management SFRs (FMT_MTD.1, see section 6.1.5 and the corresponding application notes). The ST writer may complete the list of allowed actions by all actions allowed to a non-authorised user according to the specification. This list must be consistent to the security policy **SFP_access_rules** and the other SFRs in this PP.

434 The TOE shall meet the requirement “Timing of authentication (FIA_UAU.1)” as specified below (Common Criteria Part 2).

435 **FIA_UAU.1 Timing of authentication**

436 Hierarchical to: No other components.

[33] [assignment: *list of TSF-mediated actions*]

FIA_UAU.1.1 The TSF shall allow

(1) reading the ATR
(2) reading the Card Verifiable Authentication Certificate
(3) reading the Certificate Service Provider self-signed Certificate
(4) identification by providing the users eHC-PIN
(5) identification by providing the users certificate
(6) **[assignment: *list of TSF-mediated actions*]**[34]

on behalf of the user to be performed before the user is authenticated.

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

437 Dependencies: FIA_UID.1 Timing of identification

438 **Application note 30:** This SFR is meant to support the access control policy **SFP_access_rules**. Note, that access rules for initialisation and personalisation phases are defined by management SFRs (FMT_MTD.1, see section 6.1.5, and the corresponding application notes). The ST writer may complete the list of allowed actions by other actions allowed to a non-identified user according to the specification. This list must be consistent to the security policy **SFP_access_rules** and the other SFRs in this PP.

439 The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

440 **FIA_UAU.4 Single-use authentication mechanisms**

441 Hierarchical to: No other components.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to Card-to-Card Authentication Mechanism[35].

442 Dependencies: No dependencies.

443 **Application note 31:** The Card-to-Card Authentication Mechanism required in this protection profile is based on asymmetric cryptographic primitives as required by FCS_COP.1/CCA_SIGN and FCS_COP.1/CCA_VERIF or on symmetric cryptography using FCS_COP.1/Sym and uses the freshness generated by the TOE random data (see FCS_RND.1) as challenge to prevent reuse of a response generated in a successful authentication attempt.

[34] [assignment: *list of TSF-mediated actions*]

[35] [assignment: *identified authentication mechanism(*s)]

6.1.3 Access Control

444 The Security Function Policy (SFP) **SFP_access_rules,** which as defined in the security objective OT.Access_Rights (section 4.1.1), is used in the requirements "Complete Access Control (FDP_ACC.2)", "Security attribute based access control (FDP_ACF.1)", "Basic data exchange confidentiality (FDP_UCT.1)" and "Basic data exchange confidentiality (FDP_UCT.1)".

445 The access control policy **SFP_access_rules** is only defined for the End Usage phase of the TOE. Note, that access rules for initialisation and personalisation phases are defined by management SFRs (FMT_MTD.1, see section 6.1.5), not by an explicit policy.

446 The following SFRs require the TOE to enforce the security policy **SFP_access_rules**. Note that all subjects, objects, security attributes, access methods and access rules are defined already in this policy. Therefore all of the following SFRs simply refer to this policy in all assignments.

447 The TOE shall meet the requirement "Complete Access Control (FDP_ACC.2)" as specified below (Common Criteria Part 2).

448 **FDP_ACC.2 Complete Access Control**

449 Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1 The TSF shall enforce the SFP_access_rules[36] on all subjects and objects defined by SFP_access_rules[37] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

450 Dependencies: FDP_ACF.1 Security attribute based access control

451 **Application note 32:** Keys and other data for creation of qualified signatures are out of scope of this protection profile.

452 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

[36] [assignment*: access control SFP*]

[37] [assignment: *list of subjects and objects*]

454 **FDP_ACF.1 Security attribute based access control**

455 Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the SFP_access_rules[38] to objects based on the following: all subjects and objects together with their respective security attributes as defined in SFP_access_rules[39].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules for all access methods and the access rules defined in SFP_access_rules[40].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none[41].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: rules for all access methods and the access rules defined in SFP_access_rules[42].

456 Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

457 The TOE shall meet the requirement “Residual Information Protection (FDP_RIP.1)” as specified below (Common Criteria Part 2).

458 **FDP_RIP.1 Residual Information Protection**

459 Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from]* the following objects: [assignment: *list of objects at least including: PINs, secret and private cryptographic keys, data in all files, which are not freely accessible]*[43].

38 [assignment: *access control SFP*]

39 [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes*, *or named groups of SFP-relevant security attributes*]

40 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

41 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

42 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

43 [*assignment: list of objects*] with refinement of the list of objects – obviously this refinement is valid, because the original requirement is still fulfilled

460 Dependencies: No dependencies.

461 **Application note 33:** The writer of the Security Target may want to use iterations of FDP_RIP.1 in order to distinguish between data, which must be deleted already upon deallocation and those which can be deleted upon allocation. Note that the SSCD-PP requires to delete secret signature keys upon deallocation and that this is advisable for all PINs and secret/private cryptographic keys in general. For secret user data deletion upon allocation should be sufficient (depending on the resistance of the concrete TOE against physical attacks). Note in this context that the eHC concept allows management of applications during operational use. Therefore it is theoretically possible that a newly created file uses memory areas, which belonged to another file before. Therefore the operating system must ensure that contents of the old file are not accessible by reading the new file.

462 The TOE shall meet the requirement "Stored Data Integrity (FDP_SDI.2)" as specified below (Common Criteria Part 2).

463 **FDP_SDI.2 Stored Data Integrity**

464 Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors[44] on all objects, based on the following attributes: [assignment: *user data attributes – the attributes shall be chosen in a way that at least the following data are included:*

- PINs,
- cryptographic keys,
- security relevant status variables of the card (e.g. authentication status for the PIN or for mutual authenticate),
- input data for electronic signatures,
- user data in files on the card,
- file management information (like access rules for files), and
- *the card life cycle status*][45].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

1. prohibit the use of the altered data
2. inform the connected entity about integrity error[46].

465 Dependencies: No dependencies.

[44] *[assignment: integrity errors]*

[45] *[assignment: user data attributes]* with refinement of the list of user data attributes – obviously this refinement is valid, because the original requirement is still fulfilled

[46] *[assignment: action to be taken]*

466 Application note 34:

- The writer of the Security Target may want to use iterations of FDP_SDI.2, for example in order to distinguish between different types of data (compare the SSCD-PP, where this is done for persistent data on the one hand and other data on the other hand).
- For data, which already contain an integrity protection as part of their format, the TOE does not need to apply additional measures. For example a certificate signed by an external entity and stored in the TOE for presentation to other parties will be rejected by other external entities, if it was modified. In such cases the TOE does not need to monitor the stored certificate for integrity errors.
- The formulation “Prohibit the use of the altered data” means prohibition of active use in security relevant processes, for example use of a cryptographic key in a cryptographic algorithm. It is not necessary to prevent a connected entity, which has the appropriate access rights, from reading stored user data, as long as the entity is informed about the integrity error.

6.1.4 Inter-TSF-Transfer

467 **Application note 35:** FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 require the TOE to protect User Data transmitted between the TOE and a connected device by secure messaging with encryption and message authentication codes after successful authentication of the remote device. The authentication mechanisms as part of the Card-to-Card Authentication Mechanism include the key agreement for the encryption and the message authentication key to be used for secure messaging. The rules for the data transfer are defined in the security policy **SFP_access_rules** defined in objective OT.Access_Rights (section 4.1.1).

468 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

469 **FDP_UCT.1 Basic data exchange confidentiality**

470 Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the SFP_access_rules[47] to transmit and receive[48] user data in a manner protected from unauthorised disclosure.

471 Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

472 **Application note 36**: The TOE supports secure messaging with symmetric encryption (cf. SFR FCS_COP.1/Sym) after card-to-card authentication with secure messaging.

473 The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

474 **FDP_UIT.1 Data exchange integrity**

475 Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the SFP_access_rules[49] to transmit and receive[50] user data in a manner protected from modification, deletion, insertion and replay[51] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data,

47 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

48 [selection*: transmit, receive*]

49 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

50 [selection*: transmit, receive*]

51 [selection: *modification, deletion, insertion, replay*]

whether modification, deletion, insertion and replay[52] has occurred.

476 Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

477 **Application note 37**: The TOE supports secure messaging with MAC (cf. FCS_COP.1/MAC) after card-to-card authentication with secure messaging.

478 The TOE shall meet the requirement “Inter-TSF trusted channel (FTP_ITC.1)” as specified below (Common Criteria Part 2).

479 **FTP_ITC.1 Inter-TSF Trusted Channel**

480 Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT product[53] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for all functions requiring a trusted channel as defined by SFP_access_rules[54].

481 Dependencies: No dependencies.

[52] [selection: *modification*, *deletion, insertion, replay*]

[53] [selection: *the TSF, the another trusted IT product*]

[54] [assignment: *list of functions for which a trusted channel is required*].

6.1.5 Security Management

482 **Application note 38**: The SFR FMT_SMF.1 and FMT_SMR.1 provide basic requirements to the management of the TSF data.

483 The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below (Common Criteria Part 2).

484 **FMT_SMF.1 Specification of Management Functions**

485 Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization
2. Personalization
3. the "Service_Card_Management"
4. Modification of the PIN[55].

486 Dependencies: No Dependencies

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

488 **FMT_SMR.1 Security roles**

489 Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider, Cardholder, Download Service Provider, Personalisation Service Provider, TOE Manufacturer[56].

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

490 Dependencies: FIA_UID.1 Timing of identification

[55] [assignment: *list of security management functions to be provided by the TSF*]

[56] [assignment: *the authorised identified roles*]

491 **Application note 39**: The Cardholder, Health Professional, Medical Assistant, Security Module Card (health care), Self Service Terminal, Health Insurance Agency Service Provider, Combined Services Provider and Download Service Provider are authenticated by services defined in this PP. The method, how the TOE authenticates Personalisation Service Provider and TOE Manufacturer may be product specific, because these roles are not relevant during the End Usage phase. In cases, where personalisation is done in the same secure environment as the manufacturing, it is also allowed that the two roles Personalisation Service Provider and TOE Manufacturer are fulfilled by the same persons. In this case it is also accepted that (if for example personalisation is done immediately after initialisation) only one identification/authentication procedure is done to allow both processes instead of requiring two distinct identifications and authentications.

492 **Application note 40**: The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases.

493 The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified in section 5.2 (Common Criteria Part 2 extended).

494 **FMT_LIM.1 Limited capabilities**

495 Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[57].

496 Dependencies: FMT_LIM.2 Limited availability.

497 The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified in section 5.2 (Common Criteria Part 2 extended).

[57] [assignment: *Limited capability and availability policy*]

499 **FMT_LIM.2 Limited availability**

500 Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks[58].

501 Dependencies: FMT_LIM.1 Limited capabilities.

502 The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

503 **FMT_MTD.1/Ini Management of TSF data - Initialisation**

504 Hierarchical to: No other components.

FMT_MTD.1.1/Ini The TSF shall restrict the ability to write[59] the initialisation data[60] to the TOE Manufacturer[61].

505 Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

506 **Application note 41**: As discussed in section 1.3.2 "TOE life cycle" the delivery of the TOE might be organised in a way, that hardware and initialisation data are two separate parts of the TOE during delivery. However, this is allowed only in connection with a method, which makes sure that the initialisation data are not modified by the party, which stores them into the hardware. The method used to guarantee the authenticity of the data implicitly also authenticates the TOE manufacturer as the source of the data. So the SFR FMT_MTD.1/Ini is fulfilled even if the command(s) to write the initialisation data is sent technically by a party different from the TOE manufacturer.

58 [assignment: *Limited capability and availability policy*]

59 [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

60 [assignment: *list of TSF data*]

61 [assignment: *the authorised identified roles*]

508 **FMT_MTD.1/Pers Management of TSF data - Personalisation**

509 Hierarchical to: No other components.

FMT_MTD.1.1/Pers The TSF shall restrict the ability to write[62] the personalisation data[63] to the Personalisation Service Provider[64].

510 Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

511 **Application note 42**: Note, that the management of applications during the end usage phase is not a task for the "Personalisation Service Provider" but for the "Download Service Provider".

512 **FMT_MTD.1/CMS Management of TSF data – Card Management**

513 Hierarchical to: No other components.

FMT_MTD.1.1/CMS The TSF shall restrict the ability to write[65] the

1. File structures for additional Applications,
2. Cryptographic Keys for additional applications,
3. PINs and other user authentication reference data for additional applications and
4. Access Rights for additional applications[66]

to the Download Service Provider[67].

514 Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

62 [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

63 [assignment: *list of TSF data*]

64 [assignment: *the authorised identified roles*]

65 [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

66 [assignment: *list of TSF data*]

67 [assignment: *the authorised identified roles*]

516 **FMT_MTD.1/PIN Management of TSF data – Human User Authentication data**

517 Hierarchical to: No other components.

FMT_MTD.1.1/PIN	The TSF shall restrict the ability to modify and unblock[68] the PIN[69] to the Cardholder[70].

518 Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

519 **Application note 43**: The Cardholder modifies his or her PIN as special case of the User Authentication Reference Data by means of (i) the command CHANGE REFERENCE DATA and providing the old and the new PIN or (ii) the command RESET RETRY COUNTER and providing the PUC and the new PIN. He or she unblocks the PIN by means of (i) the command RESET RETRY COUNTER and providing the PUC and the new PIN or (ii) the command RESET RETRY COUNTER and providing the PUC (without a new PIN).

520 **Application note 44**: The following SFR addresses the protection of the keys as part of the TSF data. Note that other keys are user data under protection according to SFR FDP_ACF.1.

521 **FMT_MTD.1/KEY_MOD Management of TSF data – Key Management**

522 Hierarchical to: No other components.

FMT_MTD.1.1/KEY_MOD	The TSF shall restrict the ability to modify[71] the Public Key for CV Certification Verification[72] to none[73].

523 Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

[68] [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

[69] [assignment: *list of TSF data*]

[70] [assignment: *the authorised identified roles*]

[71] [selection: *change default, query, modify, delete, clear*, [assignment: *other operations*]]

[72] [assignment: *list of TSF data*]

[73] [assignment: *the authorised identified roles*]

6.1.6 General Security Functions

524 The TOE shall prevent inherent and forced illicit information flow for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

527 The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified in section 5.3 (Common Criteria Part 2 extended):

528 **FPT_EMSEC.1 TOE Emanation**

529 Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [assignment: *specified limits*] enabling access to

1. PIN and PUC[74]

and

2. Card Authentication Private Keys,
3. Client-Sever Authentication Private Key,
4. Document Cipher Key Decipher Key,
5. secure messaging keys[75].

[74] [assignment: *list of types of TSF data*]

[75] [assignment: *list of types of user data*]

FPT_EMSEC.1.2 The TSF shall ensure any user[76] are unable to use the following interface smart card circuit contacts[77] to gain access to

1. PIN and PUC[78]

and

2. Card Authentication Private Key,
3. Client-Sever Authentication Private Key
4. Document Cipher Key Decipher Key
5. secure messaging keys[79].

530 Dependencies: No other components.

531 **Application note 45**: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The TOE has to provide a smart card interface with contacts according to ISO/IEC 7816-2 but the integrated circuit may have additional contacts or a contact less interface as well. Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

532 The following security functional requirements address the protection against forced illicit information leakage.

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

534 **FPT_FLS.1 Failure with preservation of secure state**

535 Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

1. exposure to operating conditions where therefore a malfunction could occur,
2. self-test according to FPT_TST.1[80].

[76] [assignment: *type of users*]

[77] [assignment: *type of connection*]

[78] [assignment: *list of types of TSF data*]

[79] [assignment: *list of types of user data*]

536 Dependencies: No dependencies

537 The TOE shall meet the requirement “Resistance to physical attack (FPT_PHP.3)” as specified below (Common Criteria Part 2).

538 **FPT_PHP.3 Resistance to physical attack**

539 Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing[81] to the TSF[82] by responding automatically such that the SFRs are always enforced.

540 Dependencies: No dependencies.

541 **Application note 46**: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

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

545 **FPT_TST.1 TSF testing**

546 Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests [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*]] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF]*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data]*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF]*, *TSF*].

547 Dependencies: No dependencies

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

[81] [assignment: *physical tampering scenarios*]

[82] [assignment: *list of TSF devices/elements*]

548 **Application note 47**: If the chip uses state of the art smart card technology it will run some self tests at the request of the authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of the TSF may be executed in different variants depending on the type of storage. Those parts of the code stored in read only memory may be tested during initial start-up by the "authorised user" Manufacturer in the Phase 2 Manufacturing. Those parts stored in re-writable memory (e. g. EEPROM) may be tested automatically at every start-up of the chip, which means, that the user "everybody" is authorised to start this test. Other self tests may run automatically to detect failure and to preserve a secure state according to FPT_FLS.1 in the Phase 4 Operational Use, e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as countermeasure against Differential Failure Attacks. The security target writer shall perform the operations in the SFR as suitable for the concrete product under evaluation. The vulnerability analysis done during the evaluation of the class AVA for the specific product will show, if the tests are sufficient to maintain a secure state.

6.2 Security Assurance Requirements for the TOE

549 The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the

550 Evaluation Assurance Level 4 (EAL4)

551 and augmented by taking the following components:

552 AVA_VAN.5.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Coverage

553 The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one objective.

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func
FCS_CKM.1/SM				X	X				
FCS_CKM.4				X	X				
FCS_COP.1/Hash				X	X				
FCS_COP.1/CCA_SIGN				X	X				
FCS_COP.1/CCA_VERIF				X	X				
FCS_COP.1/CSA				X	X				
FCS_COP.1/Asym_DEC				X	X				
FCS_COP.1/Sym				X	X				
FCS_COP.1/MAC				X	X				
FCS_RND.1				X	X				
FIA_AFL.1/PIN		X		X					
FIA_AFL.1/PUC		X		X					
FIA_ATD.1		X		X					
FIA_UID.1	X	X		X					
FIA_UAU.1	X	X		X					

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func
FIA_UAU.4				X					
FDP_ACC.2		X		X					
FDP_ACF.1		X		X					
FDP_RIP.1		X	X						
FDP_SDI.2		X							
FDP_UCT.1		X		X					
FDP_UIT.1		X		X					
FTP_ITC.1		X		X					
FMT_SMF.1	X	X	X	X					
FMT_SMR.1	X	X	X	X					
FMT_LIM.1		X	X						X
FMT_LIM.2		X	X						X
FMT_MTD.1/Ini	X	X	X	X					
FMT_MTD.1/Pers	X	X	X	X					
FMT_MTD.1/CMS		X	X	X					
FMT_MTD.1/PIN		X	X	X					
FMT_MTD.1/KEY_MOD		X	X	X					
FPT_EMSEC.1						X			
FPT_FLS.1						X		X	
FPT_PHP.3						X	X	X	

	OT.AC_Pers	OT.Access_Rights	OT.Additional_Applications	OT.Services	OT.Cryptography	OT.Prot_Inf_Leak	OT.Prot_Phys_Tamper	OT.Prot_Malfunction	OT.Prot_Abuse_Func
FPT_TST.1						X		X	

Table 6: Coverage of Security Objectives for the TOE by SFRs

6.3.2 Functional Requirements Sufficiency

554 The security objective **OT.AC_Pers** “Access control for personalization” is implemented by following SFRs:

555 (i) the SFR FMT_SMR.1 defines the Personaliser as known role of the TOE and the SFR FMT_SMF.1 defines personalization as security management function,

556 (ii) the SFR FIA_UID.1 and FIA_UAU.1 require identification and authentication as necessary precondition for the personalization (i.e. this TSF mediated function is not allowed before the user is identified and successfully authenticated),

557 (iii) the SFR FMT_MTD.1/Pers limit right to write personalisation data to the Personalisation Service Provider and

558 (iv) the SFR FMT_MTD.1/INI limiting the right to write any data before personalisation to the TOE Manufacturer, which in particular implies that the Personaliser role shall be created by the TOE Manufacturer.

559 The security objective **OT.Access_Rights** is the central security requirement for the TOE. Therefore it is supported by many of the SFRs. It is mainly implemented by

560 (i) the SFRs FDP_ACC.2 and FDP_ACF.1, which require to implement the access rules defined in the security policy SFP_access_rules as defined in OT.Access_Rights,

561 and supported by

562 (ii) SFRs FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD/PIN, which all support the security of the Cardholders eHC-PIN and PUC.

563 (iii) SFRs FIA_UID.1 and FIA_UAU.1, which support timing of Identification and authentication,

564 (iv) SFRs FDP_RIP.1 and FDP_SDI.2 (as well as all the more low-level oriented SFRs, which are not repeated here) prevent unwanted knowledge of secret data or unauthorised modification of the assets.

565 (v) the SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1 provide the trusted channel for the protection of the confidentiality and integrity of transmitted data, which is required by some of the rules in SFP_access_rules.

566 (vi) the SFRs FMT_MTD.1/Ini, FMT_MTD.1/Pers, FMT_MTD.1/CMS, FMT_MTD.1/KEY_MOD restrict the management of applications to authorised subjects and FMT_LIM.1 and FMT_LIM.2 prevent unauthorised use of management functions. Together they prevent the attempt to use management commands in order to bypass the access control policy.

567 The security objective **OT.Additional_Applications** covers the rules for the download of additional applications into the TOE. Therefore it is mainly supported by

568 (i) FMT_MTD.1/CMS, which restricts download of additional applications to the Download Service Provider (as also required by SFP_access_rules).

569 (ii) The other SFRs on management functions FMT_SMF.1, FMT_SMR.1, FMT_LIM.1, FMT_LIM.2, FMT_MTD.1/Ini, FMT_MTD.1/Pers, FMT_MTD.1/PIN, FMT_MTD.1/KEY_MOD support this, because they restrict other management functions to authorised subjects

570 (iii) A more “low level” support is given by FDP_RIP.1, which require the deletion of secret data before any memory area is re-used. (All hardware-oriented SFRs, which are not repeated here, also support non-bypassability of security functions.)

571 The security objective **OT.Services** addresses the implementation and the access control of the TOE security services. The security services are implemented by the following SFR:

(i) the TOE security service Service_Asym_Mut_Auth_w/o_SM is implemented by the SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/Hash, FCS_RND.1 and FIA_UAU.4.

(ii) the TOE security service Service_Asym_Mut_Auth_with_SM is implemented by the SFR FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/Hash, FCS_RND.1, FCS_COP.1/Sym, FCS_COP.1/MAC and FIA_UAU.4. The trusted channel established by this service is described by SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1.

(iii) the TOE security service Service_Sym_Mut_Auth_with_SM is implemented by the SFR FCS_CKM.1/SM, FCS_CKM.4, FCS_RND.1, FCS_COP.1/Sym, FCS_COP.1/MAC and FIA_UAU.4. The trusted channel established by this service is described by SFRs FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1.

(iv) the TOE security services Service_User_Auth_PIN and Service_User_Auth_PUC are implemented by the SFRs FIA_AFL.1/PIN, FIA_AFL.1/PUC, FIA_ATD.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD/PIN, which all support the security of the Cardholders eHC-PIN and PUC. Also it is supported by FDP_ACC.2 and FDP_ACF.1, because these SFRs require implementation of SFP_access_rules, which involves PIN authentication.

(v) the TOE security service Service_Privacy is implemented mainly by the SFRs FDP_ACC.2 and FDP_ACF.1, because the possibility for the Cardholder to delete electronic prescription data is defined as a rule in SFP_access_rules, which is mainly supported by these two SFRs (in fact all other SFRs supporting OT.Access_Rights, as listed for that objective, also support this service).

(vi) the TOE security service Service_Client_Server_Auth is implemented by the SFR FCS_COP.1/CSA

(vii) the TOE security service Service_Data_Decryption is implemented by the SFR FCS_COP.1/Asym_Dec.

(viii) the TOE security service Service_Card_Management is implemented by the SFRs already listed for the service Service_Asym_Mut_Auth_with_SM, because this service is used for authentication of the Download Service Provider and for the establishment of secure messaging for the trusted channel. Also the SFRs listed for the objective OT.Additional_Applications support this service.

(ix) the TOE security service Service_Logging is implemented by access rules for the asset logging data defined in SFP_access_rules, so it is realised mainly by the SFRs FDP_ACC.2 and FDP_ACF.1 (and in fact all other SFRs supporting OT.Access_Rights, as listed for that objective, also support this service).

572 The human user authentication and the access control for all of these security services is implemented mainly by the SFRs FDP_ACC.1 and FDP_ACF.1, because the policy SFP_access_control includes rules for the use of the services. (This is described in SFP_access_control in the form of rules for the use of the keys, which are relevant for the services.)

573 The TOE security objective **OT.Cryptography** is implemented by the SFRs of the FCS class. They include symmetric algorithms as used for secure messaging, hash functions, asymmetric algorithms and random number generation.

574 The security objective **OT.Prot_Inf_Leak** “Protection against information leakage” is implemented by the following SFR:

575 (i) The SFR FPT_EMSEC.1 protects user data and TSF data against information leakage through side channels.

576 (ii) The SFR FPT_TST.1 detects errors and the SFR FPT_FLS.1 preserves a secure state in case of detected error which may cause information leakage e.g. trough differential fault analysis.

577 (iii) The SFR FPT_PHP.3 resists physical manipulation of the TOE hardware to enforce information leakage e.g. by deactivation of countermeasures or changing the operational characteristics of the hardware.

578 The security objective **OT.Prot_Phys_Tamper** “Protection against physical tampering” is implemented directly by the SFR FPT_PHP.3.

579 The security objective **OT.Prot_Malfunction** “Protection against Malfunctions” is implemented by the following SFR:

580 (i) The SFR FPT_TST.1 detects errors and the SFR FPT_FLS.1 prevents information leakage by preserving a secure state in case of detected errors or insecure operational conditions where reliability and secure operation has not been proven or tested.

581 (ii) The SFR FPT_PHP.3 resists physical manipulation of the TOE hardware controlling the operational conditions e.g. sensors.

582 The security objective **OT.Prot_Abuse_Func** “Protection against abuse of functionality” is implemented by the following SFR:

(i) The SFR FMT_LIM.1 and FMT_LIM.2 prevent the misuse of TOE functions intended for the testing, the initialization and the personalization of the TOE in the operational phase of the TOE.

6.3.3 Dependency Rationale

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/SM	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4, FCS_COP.1/Sym and FCS_COP.1/MAC
FCS_CKM.4	[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.1
FCS_COP.1/Hash	[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	justification The cryptographic algorithm for hashing does not use any cryptographic key. Therefore none of the listed SFR are needed to be defined for this specific instantiation of FCS_COP.1. for non-satisfied dependencies
FCS_COP.1/CCA_SIGN	[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	justification The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/Asym_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1. for non-satisfied dependencies
FCS_COP.1/CCA_VERIF	[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	justification The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/Asym_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1. for non-satisfied dependencies
FCS_COP.1/CSA	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with	justification The SFR FCS_COP.1/CCA_SIGN,

SFR	Dependencies	Support of the Dependencies
	security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/Asym_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1. for non-satisfied dependencies
FCS_COP.1/Asym_DEC	[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	justification The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/Asym_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1. for non-satisfied dependencies
FCS_COP.1/Sym	[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.1, FCS_CKM.4
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_RND.1	-	-
FIA_AFL.1/PIN	FIA_UAU.1 Timing of authentication	fulfilled
FIA_AFL.1/PUC	FIA_UAU.1 Timing of authentication	fulfilled
FIA_ATD.1	-	-
FIA_UID.1	-	-
FIA_UAU.1	FIA_UID.1 Timing of identification	fulfilled

SFR	Dependencies	Support of the Dependencies
FIA_UAU.4	-	-
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	fulfilled
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2, justification The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.3) is necessary here. for non-satisfied dependencies
FDP_RIP.1	-	-
FDP_SDI.2	-	-
FDP_UCT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1 and FDP_ACC.2
FDP_UIT.1	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FTP_ITC.1 and FDP_ACC.2
FTP_ITC.1	-	-
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	fulfilled
FMT_LIM.1	FMT_LIM.2	fulfilled
FMT_LIM.2	FMT_LIM.1	fulfilled
FMT_MTD.1/Ini	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/PIN	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/Pers	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FMT_MTD.1/CMS	FMT_SMF.1 Specification of management	fulfilled

SFR	Dependencies	Support of the Dependencies
	functions, FMT_SMR.1 Security roles	
FMT_MTD.1/KEY_MOD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	fulfilled
FPT_EMSEC.1	-	-
FPT_FLS.1	-	-
FPT_PHP.3	-	-
FPT_TST.1	-	-

Table 7: Dependency rationale overview

583 Justification for non-satisfied dependencies:

584 No. 1: The cryptographic algorithm for hashing does not use any cryptographic key. Therefore none of the listed SFR are needed to be defined for this specific instantiation of FCS_COP.1.

585 No. 2: The SFR FCS_COP.1/CCA_SIGN, FCS_COP.1/CCA_VERIF, FCS_COP.1/CSA and FCS_COP.1/Asym_DEC use keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1.

586 No. 3: The access control TSF according to FDP_ACF.1 uses security attributes which are defined during the personalization and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.3) is necessary here.

6.3.4 Rationale for the Assurance Requirements

587 The EAL4 was chosen to permit 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

588 The TOE shall be shown to be resistant to penetration attacks with high attack potential as described in the threats. Therefore the component AVA_VAN.5 was chosen in order to meet the security objectives.

589 The component AVA_VAN.5 has the following dependencies:

590 • ADV_ARC.1 Security architecture description

591 • ADV_FSP.4 Complete functional specification

592 • ADV_TDS.3 Basic modular design

593 • ADV_IMP.1 Implementation representation of the TSF

594 • AGD_OPE.1 Operational user guidance

595 • AGD_PRE.1 Preparative procedures

596 • ATE_DPT.1 Testing: basic design

597 All of these are met or exceeded in the EAL4 assurance package.

6.3.5 Security Requirements – Mutual Support and Internal Consistency

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

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

600 • The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements.

601 • The dependency analysis for the additional assurance components in section 6.3.4 shows that the assurance requirements are mutually supportive and internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

602 • The dependency analysis in section 6.3.3 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.

603 • The following additional reasons support consistency and mutual supportiveness of the SFRs:

604 • The chosen SFRs of class FCS implement the cryptographic algorithms as required by the eHC specification.

605 • The chosen SFRs of classes FIA and FDP support the access control policy **SFP_access_control** as defined in the objective OT.Access_Rights.

606 • The chosen SFRs of class FMT support the secure management of TSF data in a way, which is consistent to the policy SFP_access_control.

607 • The SFRs of all these classes (FCS, FIA, FDP, FMT) together provide the eHC services as defined in the TOE description (section 1.3).

608 • The remaining SFRs, chosen from class FPT define low level protection of the TOE against any attempt to bypass the security policy **SFP_access_control** or the services defined in the specification.

609 In detail these connections between the SFRs can be seen from section 6.3.2.

610 • 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 section 6.3.3. Furthermore, as also discussed in section 6.3.4, 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 Annexes

7.1 Annex: Guidance on integration of this PP with other PPs in a Security Target

7.1.1 PP conformance

611 The Common Criteria parts 1 [1] and 3 [3] describe how a security target may claim conformance to one or more protection profiles. The rules for a compliance claim may be summarized as follows (for details refer to [1], section 10.4 “Conformance claim” and annex D “PP conformance”, and [3], section 11.2, conformance claims component ASE_CCL.1):

612 (1) The developer shall provide a conformance claim as part of the ST (see ASE_CCL.1.1D) and each claim shall identify the PP for which compliance is being claimed (see ASE_CCL.1.5C).

613 (2) The ST shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed (see ASE_CCL.1.7C).

614 (3) The ST shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed (see ASE_CCL.1.8C).

615 (4) The conformance claim rationale in the ST shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed (see ASE_CCL.1.9C).

616 (5) The conformance claim rationale in the ST shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

617 The following section discuss how a ST may be written claiming compliance to this PP for the eHC and one (or more) of the PPs for SSCD[83], see [10]. The author of the security target should pay intention to the technology independence of the SSCD PPs on the one hand and smart card specific descriptions of the current PP on the other hand. These approaches result in different text of similar security objectives or security requirements.

[83] Note however, that the German Digital Signature Act includes no requirement to claim one of the SSCD PPs in order to evaluate an application for qualified digital signatures. Therefore an ST author may also consider to take relevant contents from one of these PPs without claiming formal conformance.

618 Note that a clarification of the use of PPs claiming strict or demonstrable conformance in an ST is planned by the CC authorities and is is discussed as a “Change Proposal” at the time of writing of this PP. Since additional support for the integration of more than one PP is also expected from this process, the author of an ST should seek guidance on these issues from the responsible CC scheme.

7.1.2 Security Objectives

619 The ST claiming compliance to the PP eHC and one (or more) of the PPs SSCD [10] shall include all security objectives of the respective PPs. Note, these PP contain similar security objectives which should be stated in parallel because the address different assets. Some of them may be combined if appropriate rationale is given.

620 For example, the security objectives OT.AC_Pers in this eHC PP and the security objective OT.Lifecycle_Security in the PP SSCD addresses the security of the initialization and personalization of the TOE. The OT.AC_Pers and OT.Lifecycle_Security limit personalization to authorized users but relates to different data. The PP SSCD allows for safe destruction of the signature-creation data (SCD) which end the SSCD life cycle. The SCD may be re-generated starting a new life cycle.

7.1.3 Security Functional Requirements

621 The ST shall include all security functional requirements (SFR) of all PPs for which compliance is being claimed. The protection profiles eHC and SSCD define almost all SFR with performed operation. The ST writer shall perform all operation which are not performed already in these PP. The instantiations of the SFR components either address different security features of the TOE or describe the same security features in a consistent way.

622 The ST writer should be aware of the different roles and identities handled by the TOE.

623 Note that the roles Cardholder and Signatory will be assigned to the same person but in different context:

624 • The user authenticated for the role Cardholder may use the health application but the can not use the signature-creation data (SCD) in the signature application.

625 • The user authenticated for the role Signatory may use the SCD in the signature application but the can not use the health application.

626 • The ST shall define different authentication reference data for both roles. The values of these authentication reference data may be chosen independent on each other. This is a result of the German signature ordinance and their technical interpretation given by Bundesnetzagentur.

627 The instantiations of components of the families FDP_ACC, FDP_ACF, FDP_UCT and FDP_UIT of the PP eHC and SSCD enforce different security functional policies defined for different subjects, objects and operations:

628 • the SCD/SVD Generation SFP, the Signature-creation SFP and SVD Transfer SFP for SSCD,

629 • this eHC PP enforces the eHC SFP "**SFP_access_rules**".

630 The smart card specific eHC PP assumes to use secure messaging as mechanism to establish the trusted channel. The PP SSCD as being technology independent does not require the TOE to use mechanisms secure messaging.

631 The instantiations SFR components of the class FCS address different cryptographic mechanisms. Note that the PP eHC uses the digital signature-creation for card-to-card authentication and the client-server-authentication where the PP SSCD address the digital signature-creation for electronic signature of the data to be signed (DTBS). These digital signature use specific cryptographic algorithms and keys.

632 The instantiation of the SFR FPT_EMSEC.1 TOE emanation are very similar in the PP SSCD and PP eHC:

633 • they are not operated in respect of the types and limits of emanation,

634 • they list specific sets of user data and TSF data to protect, and

635 • only the PP eHC specifies the smart card circuit interface as the interface of the connection which the ST should use for a smart card as SSCD as well.

636 The FPT_FLS.1 Failure with preservation of secure state is common to the PP SSCD and the PP eHC where the PP SSCD does not completely perform the operation and the PP eHC assigns the exposure of operating condition. Thus the ST writer may use the list of failure defined in the PP eHC or may add other failure in which the TOE preserve a secure state.

7.1.4 Security Assurance Requirements

637 The ST compliant with the PP SSCD and the PP eHC will include at least

- the assurance package EAL4 and as augmentation
- the assurance component AVA_VAN.5 contained in all PPs.

7.2 Glossary and Acronyms

638 Some types of terms are not described here, but at specific places in the text:

639 • The services provided by the TOE are defined in section 1.2.2.

640 • The life cycle phases of the TOE are defined in section 1.3.2.

641 • Assets (sensitive data) protected by the TOE are defined in section 3.1.1.

642 • The subjects interacting with the TOE are defined in section 3.1.2.

7.2.1 Glossary

Term	Definition
Application note	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
IC dedicated software	The part of the TOE's software, which is provided by the hardware manufacturer
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification (IC identification data).
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The eHC's chip is a integrated circuit.
Mutual Authentication	Type of those cryptographic protocols, were two entities mutually verify the authenticity of each other, for smart cards this is realised by suitable sequences of amt card commands and responses
Personalization	The process by which personal data are brought into the TOE before it is handed to the cardholder
Rule_*	Naming convention for access control rules in this PP, defined in SFP_access_rules.
Secure Channel	A connection between two devices, which is secured against interception or modification of the transmitted data. The TOE realises a secure channel to other devices using secure messaging.
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Service_****	Services provided by the TOE (e. g. Service_Privacy) are defined in section 1.2.2.

Term	Definition
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]).

7.2.2 Acronyms

Acronyms	Term
A.***	Naming convention for assumptions in this PP, e. g. A.Users, see section 3.4
BMG	Bundesministerium für Gesundheit (the German Federal Ministry of Health)
BSI-PP-****	Naming convention for Protection Profiles registered by BSI
CC	Common Criteria
CCIMB	Common Criteria Implementation Management Board
COS	Card Operating System
EAL	Evaluation Assurance Level
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card
HEC	Health Employee Card (technically a type of HPC)
HPC	Health Professional Card
MAC	Message Authentication Code
OSP	Operational Security Policy
OSP.***	Naming convention for organisational security policies in this PP, e. g. OSP.User_Information (see section 3.2).
OT.***	Naming convention for security objectives for the TOE in this PP, e. g. OT.Access_Rights (see section 4.1.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUC	PIN Unblocking Code
PP	Protection Profile

Acronyms	Term
RAD	Reference Authentication Data (see [10]).
SAR	Security assurance requirements
SFP	Security Functional Policy
SFP_access_rules	Name of the security functional policy defining the access rights to assets (data) in the TOE. It is defined in OT.Access_Rights (see section 4.1) and used by access control SFRs (see section 6).
SFR	Security functional requirement
SM	Secure Messaging
SMC	Security Module Card
SSCD-PP	Secure Signature Creation Device Protection Profile, see [10]
SSVG-PP	Secure Silicon Vendor's Protection Profile, see [11]
T.***	Naming convention used for naming threats in this PP, for example T.Forge_Internal_Data, see section 3.3.
TOE	Target of Evaluation
TOE_App	Application Part of the TOE
TOE_ES	TOE Embedded Software (operating system of the TOE)
TOE_IC	The integrated circuit of the TOE, the hardware part together with IC dedicated software
TSF	TOE security functions
VAD	Verification Authentication Data
X.509	A certificate format

7.3 Literature

643 **Common Criteria**

644 [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

645 [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

646 [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

647 [4] Common Methodology for Information Technology Security Evaluation CEM, Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

648 **eHC specifications and further documents related to the German eHC**

649 Note: The following specifications may be replaced by further versions in future. This PP allows the evaluation of cards, which are implemented according to such newer versions, as long as the security properties defined in this PP remain valid for those newer versions of these specifications.

650 [5] Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2, 16.09.2008, gematik

651 [6] Die Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.1, 19.06.2008, gematik

652 [7] Beschreibung der zulässigen PIN- und PUK-Verfahren für die eGK, Version 1.4.0, 08.05.2009, gematik;
and
Übergreifendes Sicherheitskonzept der Telematikinfrastruktur, Anhang E – PIN/PUK-Policy, Version 2.4.0, 05.09.2008, gematik
Note: These documents need to be used in the version valid at the time of evaluation, see the web site www.gematik.de for contact.

653 **Cryptography**

654 [8] „Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001“, Bundesnetzagentur, 06.01.2010

655 Note: The newest officially published version of the preceding document shall be used, see http://www.bundesnetzagentur.de. Note that this document is specifically relevant for qualified digital signatures, while the following documents are relevant for other cryptographic algorithms used.

656 [9] BSI TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version: 3.0, Datum: 08.04.2009, Status: Veröffentlichung, Fassung: April 2009

657 Note: The newest officially published version of the preceding document shall be used, see http://www.bsi.bund.de.

658 **Protection Profiles**

659 [10] SSCD-PP according to CC 3.1: "Protection Profiles for Secure Signature Creation Device – Part 2: Device with Key Generation, Version 1.03", reference BSI-CC-PP-0059-2009

660 [11] Smartcard IC Platform Protection Profile, Version 1.0, 15.06.2007; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, also short SSVG-PP

661 [12] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002