Federal Office
for Information Security

Common Criteria Protection Profile

Mobile Card Terminal
for the German Healthcare System (MobCT)

BSI-CC-PP-0052

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Change history

Version	Date	Reason	Remarks
0.1	2nd July 2008	Initial version	
0.2	7th July 2008	Minor changes	
0.3	14th September 2008	Update due to gematik comments and specification update, OSP added, further improvements	
0.7	29th September 2008	Update due to comments from the evaluation body, further improvements	
0.8.1	7th October 2008	Appendix A has been added	
0.8.4	14th November 2008	Updates due to comments from the evaluation body and gematik.	
0.8.5	3rd December 2008	Updates due to comments from the gematik	
0.8.6	5th December 2008	Updates due to BSI	
0.8.7	6th January 2009	Updates due to comments from T-Systems	
0.9.0	31st July 2009	Updates due to fine-tuning between PP Specification	
0.9.5	06th August 2009	Appendix A has been rewritten. Minor changes due to transition to CC 3.1 R3	
0.9.8	16th September 2009	Updates due to comments from T-Systems	
0.9.9	10th February 2010	Updates due to comments from BSI	
1.0.0	25th February 2010	Updates due to comments from BSI	
1.0.1	25th September 2012	Updates due to changes of the gematik specification, see [5]	
1.0.2	04th December 2012	Updates due to comments of the gematik associates	
1.0.3	06th December 2012	Updates due to comments of the gematik	
1.0.4	01st March 2013	Updates due to comments of the gematik	
1.0.5	08th April 2013	Updates due to comments of the gematik	
1.1	30th May 2013	Updates due to comments of the gematik	
1.2	17th April 2014	Update due to a gematik specification update	
1.3	15th July 2014	Update due to a gematik specification update	
1.4	24th September 2014	Updates due to comments from T-Systems	

Last Version: (1.4, 24th September 2014)

Name	Value	Display
File name and sizes	Set automatically	MobCT_PP_1.4_FINAL (1537536 Byte)
Last Version	1.4	1.4
Date	24th September 2014	24th September 2014
Classification	Unclassified	Unclassified
Authors	Jürgen Blum, Marion Brinkkötter	Jürgen Blum, Marion Brinkkötter

Table of Content

1 PP Introduction

1.1 PP Reference

Titel:	Common Criteria Protection Profile – Mobile Card Terminal for the German Healthcare System (MobCT)
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Editor(s):	Jürgen Blum, Marion Brinkkötter, Bundesamt für Sicherheit in der Informationstechnik
CC Version:	3.1
Assurance Level:	EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5
Version number:	1.4
Date:	24th September 2014
Registration-ID:	BSI-CC-PP-0052
Keywords:	Protection Profile, Mobile Card Terminal, Electronic Health Card

1.2 PP Overview

1.2.1 TOE Overview

The Mobile Card Terminal (MobCT) is a **smart card terminal** (= TOE type); used for the German healthcare system. It is used by medical suppliers during visits to read out health insurance data and emergency data[1] from a *user card*[2] of a health insured person. The data may further be viewed on a display or printed by the medical supplier.

For accessing protected data on a user card the medical supplier needs an *authorised card*[3] and a corresponding PIN to unlock the authorised card (*card holder PIN*). The PIN is acquired by the TOE and then relayed to the authorised card. Once the authorised card is unlocked, the medical supplier can plug in a user card. The authorised card then unlocks the user card via card-to-card (C2C) authentication. Afterwards, the TOE is able to read data from the user card. Unprotected data on the user card can be read without the unlock process.

The TOE provides functionality to store the data records in its own persistent storage after the data has been read from a user card. All data records are encrypted using symmetric AES encryption while residing in the storage. The symmetric encryption key is generated by the TOE using the random number generator of the authorised card. The key is also encrypted while in the storage of the TOE. For the encryption and decryption of the symmetric key, the

[1] The storage of emergency data on the user card is currently not foreseen. Therefore any requirements referring the handling of emergency data can be obliged at the moment. Requirements referring the insurance data have to be fulfilled.

[2] See chapter 1.2.4 for a description of user cards.

[3] See chapter 1.2.3 for a description of authorised cards.

TOE uses the functionality of the authorised card. When the authorised card is unlocked and the symmetric key is decrypted by the authorised card, the TOE is in the *authenticated state* for a medical supplier session. While the TOE is in this authenticated state, sensitive data like the symmetric encryption key may reside in the volatile memory of the TOE in clear text. Once the authenticated state has been dropped, all unencrypted sensitive information will be deleted from memory. Another kind of *authenticated state* is obtained after an administrator login (administrator authentication for an administrator session).

The TOE may be used by more than one medical supplier. However, decryption of the data records is only possible with the help of the authorised card that was used to encrypt the data.

The medical supplier is able to transfer the stored data to a Data Management System for a practice or hospital (DMS) for accounting. After a data record has been transferred, the TOE deletes the record from the storage. Data records can also be deleted manually by the medical supplier at the TOE without storing the data records in the DMS.

This PP does only represent a part of the approval process of the gematik for a MobCT. For more information see [7].

The body of the MobCT will be sealed. The sealing has to be compliant to the requirements of BSI – TR 03120, see [8].

Figure 1 gives an overview of the TOE components:

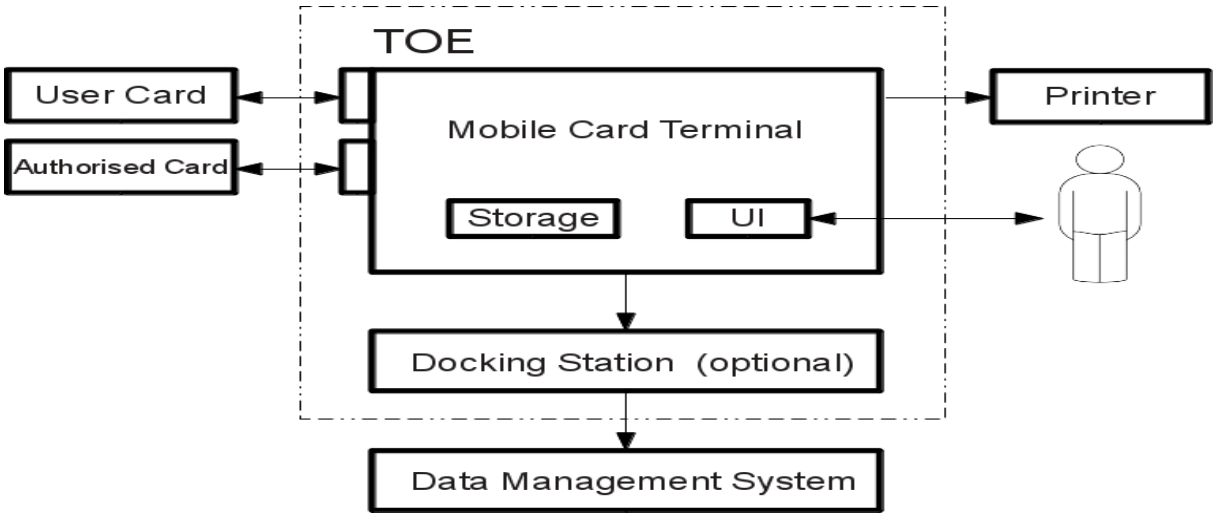


Figure 1: TOE demarcation

1.2.2 Operational environment of the TOE

This Protection Profile specifies the security needs for the MobCT in a secure operational environment where protection against physical manipulation of the TOE is covered by the TOE environment (see also chapter 3.1). If the ST author decides to weaken the assumptions on the environment, then the instructions in the supplement “Mobile Card Terminal for the German Healthcare System: Additional security functionality for physical protection” ([11]) shall be used to add further security functionality.

The TOE will be locked in a secure area whenever it is not used. The secure area is only accessible for the medical supplier and persons authorised by them. Intrusion to the secure

area for the TOE will be easily detectable by the medical supplier. In such a case the device will not be used anymore and will have to be replaced.

The medical supplier is considered to know the user guidance for his TOE and operate it accordingly.

1.2.3 Authorised cards

The following smartcards are authorised cards in the context of this PP:

Authorised card	Description
Healthcare Professional Card (HPC)	The HPC is the personal authorised card for a specific medical supplier and is used with the MobCT to unlock the eHC via Card-to-card authentication (C2C). Before functionality of this card can be used, the medical supplier has to unlock the HPC with the card holder PIN.
SMC-B	The SMC-B is the authorised card for an institution/organisation and is also used with the MobCT to unlock the eHC via Card-to-card authentication (C2C). Before functionality of this card can be used, an authorised medical supplier has to unlock the SMC-B with the card holder PIN. SMC-Bs may be used by more than one medical supplier and the card holder PIN is known to all medical suppliers which are authorised to use the card. The institution/organisation keeps records stating time and identity of the authorised medical supplier using the SMC-B at any time.

Table 1: Authorised cards

1.2.4 User cards

The following smartcards are cards that can be read by the MobCT with the use of authorised cards:

User card	Description
Krankenversichertenkarte (KVK)[4]	The KVK contains health insurance data of a health insured person. This card does not need to be unlocked as it enforces no access control.
electronic Health Card (eHC)	The eHC contains health insurance data and emergency data[1] of a health insured person. In order to read out emergency data and protected health insurance data the card needs to be unlocked by an authorised card. The eHC carries a container for access logs. Access log entries are created by the MobCT when data is accessed.

Table 2: User cards

4 See also [5]

1.2.5 Physical scope of the TOE

The TOE comprises the following physical components:

- At least two card slots for one authorised card and one user card
- A PIN pad for entry of a PIN (part of UI)
- One or more displays for user interaction during the PIN entry, for showing emergency data, and for management of the TOE (part of UI)
- Further user interface (e.g. keyboard) to allow the user to start operations and navigate through menus (part of UI)
- A persistent storage to store data records
- A body which integrates all the above mentioned components and is physically protected by sealing, so that the medical supplier can detect if the device has been tampered with.
- Optionally: a docking station for data transfer to the DMS.

The following components are important in the context of this PP but are not part of the TOE:

- Smartcards (HPC, SMC-B, KVK, eHC)
- Printer
- Data Management System of a practice or hospital (DMS)
- External display that is used to display emergency data (if not included in the TOE)

1.2.6 Logical scope of the TOE

The logical scope of the TOE can be defined by its security functionality:

- Access control for stored health insurance data and emergency data[1]
- Information flow control for the card holder PIN, PIN for the management interface, health insurance data and emergency data[1]
- Cryptographic support for encryption of persistent storage
- Integrity protection of emergency data[1]
- Residual information protection
- Self testing
- Logging accesses to the eHC (not KVK)
- Protocol generation for stored data records
- Restricting transfer of data records to DMS
- Identification and authentication for administrators
- Management functionality including a secure firmware update

The following security functionality is provided by the operational environment of the TOE:

- Card-to-card authentication (authorised card authenticates and unlocks the eHC)

- Identification and authentication of medical suppliers (done by the authorised card via card holder PIN)
- Encryption/decryption of symmetric key (done by the authorised card)
- Physical protection and secure storage of the TOE
- Signature generation for emergency data[1] on the eHC (done by an authorised card that is out of scope of this PP)

1.2.7 Physical Protection of the TOE

The TOE cannot counter physical attacks concerning manipulation of the device which have to be considered due to the augmentation of AVA_VAN.5. Therefore the physical protection is mainly provided by the TOE environment. This specifically covers the following scenarios:

- The TOE is stolen and manipulated or simply replaced by an attacker. This would allow an attacker to foist a "hostile" device upon the medical supplier which in turn could compromise all assets from this point on (e.g. card holder PIN, health insurance data, emergency data).
- The card holder PIN is transferred in clear text to the card slot of the HPC but the card slot is a point of the TOE which is not completely physically protected against manipulation by the TOE itself. An attacker could manipulate the card slot in order to intercept the PIN transfer at a later point, or manipulate the TOE internals.
- During the transfer of data records from the MobCT to the DMS an attacker could intercept the transfer and read out unencrypted data.

In this Protection Profile the environment is assumed to completely counter the threat of physical manipulation of the TOE as such threats can not be diminished by the TOE with reasonable efforts. However, if a manufacturer wants (needs) to weaken the assumptions about the environment and is able to provide physical protection by the TOE, then the ST author shall use the instructions presented in the supplement [11].

1.2.8 Assets

A series of user and TSF data are used for and generated during the operation of the TOE. They are described subsequently. So far as they are assets which need to be protected by the TOE and its operational environment the descriptions include the required kind of protection (e.g. integrity).

1.2.8.1 User data

Data	Description
Card holder PIN	The TOE acquires a PIN from the medical supplier and passes it to the authorised card in one of the card slots. The card holder PIN shall be held confidential.
Data records	The term "data records" refers to health insurance data as well as emergency data stored on the TOE. The data records shall be held confidential and integer.

Health insurance data	The TOE reads out protected and unprotected health insurance data from the eHC (or unprotected health insurance data from the KVK), encrypts and stores it, decrypts and displays it, and sends it to the DMS. Stored health insurance data shall be held confidential and integer.
Emergency data[1]	The TOE reads out protected emergency data from the eHC, encrypts and stores it, displays it, and transfers it to the DMS. Emergency data is equipped with a cryptographic signature and a public key of the authorised card that created the signature. Stored emergency data shall be held confidential and protected against modification.
Firmware updates	The administrator is able to perform firmware updates for the TOE. New firmware is considered to be user data (as long as the data has only been received but not yet used for an update) and its authenticity and integrity shall be ensured.
eHC access logs (also referred to as: access logging data)	Accesses to the eHC are logged. The log entry is written to the eHC by the TOE.
Protocol data	For every time the TOE reads out and stores health insurance and emergency data, it generates protocol data. All protocol data entries are later transmitted to the DMS alongside the data.

Table 3: User data

1.2.8.2 TSF data

Data	Description
Administrator credentials (also referred to as: PIN for the management interface, i.e. Administrator PIN and, if applicable, TOE Reset PIN)	The TOE stores references of the administrator credentials (i.e. a PIN) for the management interface of the TOE. This data shall be held confidential and integrity protected. The administrator PIN shall have the attribute "administrator PIN validity", which indicates whether the current PIN is valid. The PIN is only invalid directly after delivery and after or during a reset to factory defaults. Under these circumstances the attribute ensures that the TOE forces the administrator to set a valid management interface PIN in order to prevent an attacker from gaining easy access to management functionality. The modification of the validity of the management interface PIN is tied to the change of the management interface PIN. By setting the PIN, the administrator changes the validity of the PIN to valid. The TOE has to offer an additional TOE reset mechanism (fallback) in case that administrator credentials are lost. The authentication mechanism for this fallback has to be described in the ST. Its usage causes a reset to factory defaults. Subsequently the administrator must set a new administrator PIN. It is recommended to implement the fallback mechanism by a TOE Reset PIN which is an additional PIN that may be used by the administrator if he has forgotten the administrator PIN. The developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator's authenticity.
User ID (for the management interface)	The TOE may implement a user ID for the management interface, e.g. in order to support multiple administrators.
Symmetric encryption key for the encryption of the data records within the persistent storage (encrypted)	The encrypted symmetric keys for encryption of data records reside in the persistent storage. They are encrypted using the functionality of the authorised card of the respective medical supplier storing the data records.
Symmetric encryption key for the encryption of the data records within the persistent storage (unencrypted)	The decrypted symmetric key is stored in the volatile memory of the TOE, while the TOE is used by the medical supplier to encrypt or decrypt data records. The decrypted symmetric key shall be held confidential and its authenticity shall be ensured.
Public key for firmware signature check	In order to assure the integrity of new firmware, the TOE checks the signature of the firmware using a public key. The public key is part of the installed firmware. This data shall be protected against modification.
Cross CVC	Cross CVCs are used for the card-to-card authentication between cards of different roots.

Installed firmware	The TOE firmware shall be protected against modification. The firmware shall have the attribute firmware version, which allows the TOE to differentiate between different firmware releases. The firmware can be resetted to factory defaults. This will cause all device settings (device configuration) and data stored by the TOE to be lost.
Time settings	Two kinds of "time settings" are used: A) The TOE has an internal clock, the setting of which is the responsibility of the administrator. The time settings (which include date and time) of this clock provide a reliable timestamp for the following purposes: • logging of eHC accesses, • generation of protocol data, • the checking of the validity period of card certificates B) The administrator sets the session time-out of the medical supplier session.

Table 4: TSF Data

1.2.9 External entities and subjects

The following external entities interact with the TOE:

Entity	Description
User	The medical supplier and the administrator are summarized under the term user.
Medical supplier[5]	The medical supplier (or authorised persons acting on behalf) is the main user of the TOE. Using the authorised card they are able to read out and display data from a user card of an insured person and transfer the data to their DMS. The medical supplier is responsible for the secure operation of the TOE as they are for the safe operation of medical devices, the adherence of data protection, and the safe storage of drugs.

[5] Note that in case an SMC-B is used, the medical supplier is an institution/organisation or a person acting on behalf of that institution/organisation.

Administrator	The administrator is responsible for installation, configuration and maintenance of the TOE. This includes but is not limited to the following actions: • Firmware update • Import of Cross CVCs • Management of time settings • Reset to factory defaults • Management of login credentials It should be noted that medical supplier and administrator may be the same person.
Developer	The TOE may provide additional management functionalities specifically for the developer.
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify security relevant data.
Data Management System (DMS) for a practice or hospital	The DMS is the main system of the medical supplier (e.g. at an office or at a hospital). The medical supplier is able to transfer stored data records from the TOE to the DMS via a local interface.
Smart cards	The TOE communicates with smart cards like the HPC and the eHC placed in card slots. All of these smart cards hold an X.509 certificate which provide their card identity.
Authorised Card	An authorised card is a smart card which is authorised to unlock the eHC. This smart card is used by the medical supplier and can either be an HPC or an SMC - B.
User Card	A user card is a smart card or a memory card which contains health insurance data. It is used by a health insured person and can either be an eHC or a KVK.

Table 5: External entities

The following subjects are active entities in the TOE:

Entity	Description
Docking Station	The TOE may use a docking station to transfer data to the DMS. The docking station is an optional part of the TOE.
TOE routine for DMS data transfer	A TOE routine implementing the data transfer from the persistent storage to the DMS.
TOE logging routine	A TOE routine implementing the logging of data access on the eHC.
TOE routine for generation of protocol data	A TOE routine implementing the generation of protocol data for the data records in the persistent storage.

Table 6: Subjects

2 Conformance Claim

2.1 Common Criteria Conformance Claim

The Common Criteria (CC) version in use is Common Criteria, Version 3.1 R4 [1], [2] and [3].
This PP is

- CC Part 2 extended
- CC Part 3 conformant, and
- Package conformant to EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5.

2.2 PP Claim, Package Claim

The PP does not claim conformance to any other PP or Package.

2.3 Conformance Rationale

No conformance rationale is needed as the PP does not claim conformance to any other PP or Package.

2.4 Conformance Statement

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

3 Security Problem Definition

The security problem definition defines the assumptions about the environment, the threats against the TOE, and the organisational security policies.

3.1 Assumptions

The following assumptions need to be made about the environment of the TOE to allow the secure operation of the TOE and to protect the assets named in chapter 1.2.8.

Assumption	Description
A.MEDIC	The medical supplier is assumed to be non hostile, always act with care and read the existing guidance documentation of the TOE. The medical supplier ensures that the rules for the operational environment of the TOE are adhered to as required by the guidance. The medical supplier will be responsible for the secure operation of the TOE. This responsibility is equivalent to their responsibility for the safe operation of medical devices, the adherence with data protection, and the safe storage of drugs.[6] It is assumed that if the medical supplier uses an SMC-B for an authorised card, the medical supplier does not hand over the TOE to any other user (medical supplier or administrator) before the data stored within the terminal has been transferred to the DMS.[7] Further, the medical supplier will ensure that • they never disclose the card holder PIN, • they are not observed while entering the card holder PIN, • they are not observed while reading insurance and emergency data from the display (with one exception: the medical supplier may show a patient his insurance and emergency data); • the authorised card is pulled from the card slot or the authenticated state of the TOE is dropped manually when the TOE is no longer in use; • they check the local connection to the DMS before and while transferring data to prevent wiretapping; • they check that the sealing and the body of the TOE are undamaged every time the device is used and • they request the administrator to set the time-out value for

[6] The medical supplier needs to be aware of the fact that even if the TOE is the property of e.g. a hospital the medical supplier accepts this responsibility by using the TOE. Thus, should the medical supplier be one of many to have access to the TOE, the medical supplier has to ensure before using the TOE that the e.g. hospital security policy is in accordance with the requirements depicted in the guidance and thus only trusted and authorised personnel (medical suppliers and administrators) handle the TOE.

[7] A medical supplier using an SMC-B may otherwise accidentally access stored data records from a different medical supplier using the same SMC-B.

Assumption	Description
	medical supplier inactivity as low as possible.
A.ADMIN	The administrator is assumed to be non hostile, always act with care, read the existing guidance documentation of the TOE and adhere to the rules of the TOEs environment. The administrator will ensure that • the time of the TOE is set correctly, • the firmware is only updated to certified versions, • they set the new administrator PIN immediately upon performing the reset to factory defaults, • they set the time-out value for the medical supplier inactivity during the initial start-up and afterwards, • they never disclose the PIN for the management interface and • they are not observed while entering the PIN for the management interface.
A. Developer	The developer is assumed to be non hostile, always act with care and knows the existing guidance documentation of the TOE. The developer provides an additional TOE reset mechanism (fallback) and describes it in the ST. If the fallback mechanism is implemented by a TOE Reset PIN, the developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator's authenticity. The request is documented by the developer. If the fallback mechanism is implemented by a challenge response mechanism the developer stores the device-specific shared secret in a safe way and tells the administrator the response to a challenge on his request after the successful verification of the administrator's authenticity. The request is documented by the developer.
A.CARDS	The authorised cards and the eHC are smart cards that comply with the specifications of the gematik as referenced in [5]. The authorised card will provide the following functionality to the TOE: • Identification and authentication of medical suppliers using a PIN • Unlocking of eHCs via card-to-card authentication • Generation of random numbers with at least 100 bit of entropy for the generation of symmetric keys as specified in [4]. • Asymmetric encryption/decryption of symmetric keys which are used to encrypt the persistent storage of the TOE. • Emergency data[1] on the eHC will be signed by an authorised card that created the data records on the eHC to allow the TOE to verify the integrity of that data.

Assumption	Description
A.DMS[8]	The TOE is assumed to be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier. Furthermore, the connection between the TOE and the DMS is assumed to be: • established using a cable (USB, RS-232, etc.), • easy to survey for the medical supplier and • under the sole control of the medical supplier. Network interfaces (e.g. Ethernet) will not be used.
A.PHYSICAL[9]	The secure TOE environment is assumed to protect the TOE against physical manipulation[10]. Specifically, the environment will assure that • the card holder PIN cannot be intercepted during transfer to the authorised card, and • data records can not be intercepted during transfer from the TOE to the DMS. The TOE is assumed to have no unnecessary electronic contacts and no obvious constructional defects.
A.ENVIRONMENT	While the TOE is in use by either the medical supplier or the administrator, they always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE is not in use, it is kept in a secure area. • The secure area is checked for physical manipulation before the TOE is taken from it and used. • A breach of this secure area by an attacker must be detectable. In this case the TOE has to be replaced, regardless of whether there is any visible sign of manipulation of the TOE.

Table 7: Assumptions

3.2 Threats

This section describes the threats which have to be countered by the TOE and its operational environment.

[8] In case the TOE realises the (optional) docking station, A.DMS also encompasses the docking station. If the docking station realises part of the flow control or any other TOE functionality, this functionality has to be analysed and tested as any other TOE functionality. Only the physical protection of the docking station is covered by A.DMS.

[9] This assumptions resp. its corresponding security objective OE.PHYSICAL counters the threat T.MAN_HW. If the ST author decides to provide physical protection by the TOE (and weaken the assumption), supplement [11] shall be considered for further security functionality.

[10] Note that in the environment that is characterized by this assumption, stealing the TOE is considered to be possible.

Threat	Description
T.MAN_HW[11]	An attacker could gain access to the TOE in order to manipulate the hardware and modify the functionality of the TOE. Further usage by the medical supplier could then reveal the card holder PIN or data records that are transferred from the TOE to the DMS. The attacker needs to have knowledge on the TOE and how to manipulate electronic devices.
T.DATA	An attacker may try to release or modify protected assets from the TOE. These assets are • the authorised card PIN, • Health insurance data and emergency data that has been received from eHCs and stored in the storage of the TOE, • TSF data (e.g. symmetric encryption key) Specifically an attacker may use any interface that is provided by the TOE. The attacker needs to have knowledge on the TOE.
T.ACCESS	An attacker could try to access stored data records by using an authorised card different from the one that was used to store the data. The threatened assets in this case are health insurance data records and emergency data records stored in the persistent storage of the TOE.
T.AUTH_STATE	An attacker could steal the TOE with a plugged authorised card while the TOE is in an authenticated state. Thereby, the attacker could access stored health insurance data and emergency data. The threatened assets are health insurance data and emergency data residing in the persistent storage. The attacker needs to have basic knowledge on the TOE.
T.ADMIN_PIN	An attacker may try to acquire the administrator PIN or credentials for the TOE reset mechanism (e.g. the TOE Reset PIN or the shared secret in case of a challenge response authentication mechanism) by guessing or predicting. An attacker may try to spy out the administrator PIN or credentials for the TOE reset mechanism via the display.
T.FIRMWARE	An attacker may try to install malicious firmware updates, to alter the behaviour of the TOE. In this case all assets of the TOE are threatened. The attacker needs to have knowledge on the TOE and how to create firmware.

[11] The threat T.MAN_HW is completely covered by security objectives for the TOE operational environment and could therefore be removed from the security problem definition. However, to emphasize the importance of countering this threat by the operational environment of the TOE it is left in this Protection Profile. Furthermore, the threat needs to be considered by the ST author if the informational supplement [11] is used to address physical protection to be provided by the TOE.

Table 8: Threats

3.3 Organisational Security Policies

The TOE shall be implemented according to the following specifications:

Policy	Description
OSP.LOG_CARDS	Health insured persons need to have the opportunity to control who accessed data on their eHC. Therefore, accesses to eHCs shall be logged on the cards itself. At least the following information shall be logged according to [5]: • the timestamp, • the accessed data, and • the identity of the authorised card which was used to access the eHC. Furthermore the write access to the eHC shall be limited to the access logging and no write access shall ever be performed on the KVK.
OSP.LOG_DATA	The TOE shall generate a protocol entry containing the following information whenever health insurance data or emergency data is written to the persistent storage of the TOE: • the timestamp, • the approval number of the TOE as specified in [5]. Additional information may be added to this a protocol entry, as long as no patient information is revealed within or by the protocol entry (e.g. information for the internal administration of the data, for example an search index to accelerate search operations).
OSP.TRANSFER	The TOE shall enable the medical supplier to transfer data records to the DMS only. The TOE shall never transmit health insurance data or emergency data to card slots. Additionally the integrity of the data records is to be protected during transmission by an EDC as specified in [5].
OSP.DMS_CONNECTION	The TOE shall not permit access to the KVK or eHC while the TOE is connected to the DMS. If the TOE uses a docking station, this docking station shall transmit health insurance data and emergency data to the DMS only. It shall never store either indefinitely.
OSP.C2C	The TOE shall initiate the card-to-card authentication between the authorised card and the eHC right before the TOE reads/writes data from/to the eHC. If the authentication

	did not succeed, no access shall be performed by the TOE[12]. This OSP prevents that faked eHC can be used by the TOE.
OSP.TIME	The TOE shall provide a reliable timestamp for the following purposes: • logging of eHC accesses, • generation of protocol data, • the checking of the validity period of card certificates. The TOE shall not allow the setting of the date while health insurance data is still in the persistent storage of the TOE.
OSP.SEALING	The body of the TOE shall be equipped with a seal by the manufacturer. The seal protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The sealing shall be compliant to BSI – TR 03120 ([8]) and has been tested accordingly[13].
OSP.SELFTESTS	The TOE shall be able to perform self tests to verify the correct operation of its security functionality and the integrity of the firmware. The self tests shall run at least during initial start-up.
OSP.EMERGENCY_DATA[1]	The TOE shall verify the integrity of the emergency data after receipt and protect the integrity of the emergency data while it resides inside the TOE, in order to ensure correct visualisation of the data.

Table 9: Organisational Security Policies

[12] Note that the TOE has to support cross CVCs, see [5]. Cross CVCs are used for the card-to-card authentication between cards of different roots.

[13] The testing shall encompass an attestation that the seal fulfils the structural requirements of BSI – TR 03120 ([8]) and an analysis of the seals placement by the evaluator. The evaluator's analysis must determine whether the seal's placement complies with the requirements of BSI – TR 03120 for protection (placement must be such that the casing can not be opened without damaging the seal), visibility (the seal must be easy to perceive by the user, so that damages to the seal are easily recognisable), durability (the placement must take the wear resistance of the seal into account) and user guidance (the user directions for detection of seal tampering provided by the guidance must enable an inexperienced user to detect damaged seals).

4 Security Objectives

This chapter describes the security objectives for the TOE (in section 4.1) and the security objectives for the environment of the TOE (in section 4.2).

4.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE

Objective	Description
O.PIN	The TOE shall serve as a secure pin entry device for the user. Thus the TOE has to provide the user with the functionality to enter an authorised card PIN and ensure that the PIN is never released from the TOE and only relayed to the card slot where the authorised card is plugged in. The TOE shall accept the result of the authentication of the medical supplier to the authorised card for the authentication of the medical supplier role to the TOE.
O.RESIDUAL	The TOE shall delete all security relevant data from volatile memory in a secure manner when it is no longer used. This applies to: • the card holder PIN of the medical supplier, • the PIN for the management interface. • the health insurance data, • the emergency data, as well as • for unencrypted TSF data but the installed firmware.
O.SELFTESTS	The TOE shall be able to perform self tests to verify the correct operation of its security functionality and the integrity of the firmware. The self tests shall run at least during initial start-up.
O.PROTECTION	The TOE shall encrypt data records in the persistent storage[14] using the algorithms specified in [4]. The TOE shall verify that decrypted data records were decrypted with the same authorised card which was used to encrypt the data. The TOE shall not allow encryption keys to leave the TOE. Further, if functionality for emergency data is implemented, the TOE shall assure the integrity of the emergency data upon receipt from the eHC by mathematically verifying the digital signature of the emergency data and protect the integrity of the emergency data while it resides inside the TOE. This includes secure storage and correct visualisation of the data.
O.AUTH_STATE	The TOE shall drop the authenticated state for a medical supplier

[14] The symmetric key shall be encrypted using the functionality of the authorised card (see A.CARDS).

Objective	Description
	session and thereby delete all unencrypted sensitive information from memory in the following situations: • The HPC has been pulled from its card slot or otherwise loses its authenticated state. • After an adjustable time of [1 – 60] minutes of medical supplier inactivity[15] • The medical supplier forces to drop the state manually. • Power loss. The TOE shall drop the authenticated state for a administrator session and thereby delete all unencrypted sensitive information from memory in the following situations: • 15 minutes of administrator inactivity after administrator authentication. • The administrator forces to drop the state manually (by logging off). • Power loss.
O.I&A	The TOE shall provide an authentication mechanism (e.g. PIN based) for administrators. The TOE shall enforce the following quality metrics for secrets used for the management authentication mechanism: • at least 8 digits for a PIN, • the user ID shall not be a part of the PIN. The TOE shall not display the PIN during the authentication process. The TOE shall not allow the PIN to leave the TOE. The TOE shall force the administrator to set an administrator PIN during initialisation (first initialisation or after reset to factory defaults). The TOE shall lock an account after a specified number of unsuccessful authentication attempts for a specified period of time. The TOE shall provide an additional TOE reset mechanism (fallback) called "TOE reset with authentication". If the fallback mechanism is implemented in the recommended way by a TOE Reset PIN: The TOE contains for the TOE reset mechanism an initial, unpredictable device-specific TOE Reset PIN which is set by the developer before the delivery to the user. The TOE Reset PIN is changeable by the administrator in order to allow that in case of an administrator switch the former TOE Reset PIN is invalid. If the fallback mechanism is implemented by a challenge response mechanism: The TOE uses a challenge response mechanism for the TOE reset mechanism. It contains an unpredictable device-specific

[15] The maximum time of 60 minutes between the beginning of medical supplier inactivity and dropping the authenticated state will be tested within a trial phase. It must be possible to change this value with a firmware update.

Objective	Description
	shared secret which is set by the developer before the delivery to the user. The TOE shall lock an account after a specified number of unsuccessful authentication attempts for a specified period of time. Optionally the TOE may offer another additional TOE reset mechanism called "TOE reset without authentication" which does not request for the administrator's credentials before performing a TOE reset to factory defaults. If implemented, the functionality shall be turned off as factory default. Performing such a TOE reset shall not be accidentally possible. The TOE shall notify its medical suppliers before the first usage after a TOE reset without authentication. The message shall be acknowledged by the medical suppliers[16].
O.MANAGEMENT	The TOE shall provide the following management functionality to an authenticated administrator: • Firmware update • Import of Cross CVCs • Management of time • Management of login credentials • Reset to factory defaults[17]. In addition the TOE may also provide the management functionality "Reset to factory defaults" to the developer. A firmware consists of two parts: firstly the so-called "firmware list" and secondly the "firmware core" which includes the whole firmware except the firmware list. Firmware lists and cores have to versioned independently. The firmware list states all firmware core versions to which a change is allowed: An update of the firmware core is only allowed if the core version is included in the firmware list. In case of a downgrade of the firmware core the TOE must warn the administrator before the installation that he is doing a downgrade, not an upgrade. The TOE must offer him the chance to cancel the installation. An update of the firmware list is only allowed to newer versions. Both, updates of firmware core and list are only allowed if their integrity and authenticity is ensured. They can be updated independently. The TOE shall notify the medical suppliers before their first TOE

16 All medical suppliers using the TOE have to be notified.

17 When the device is reset to factory defaults, all data in the persistent storage except the firmware plus the information whether the reset was triggered by a TOE reset without authentication and, if applicable, the TOE reset credentials, are securely deleted and the login credentials for the management interface are set back to initial values and require changing.

Objective	Description
	usage and after firmware updates. The messages shall be acknowledged by the medical suppliers[16].
O.LOG_CARDS	The TOE shall log accesses to eHCs on the cards itself. The following information shall be logged according to [5] • the timestamp, • the accessed data, and • the identity of the authorised card which was used to access the eHC. Furthermore the write access to the eHC shall be limited to the access logging and no write access shall ever be performed on the KVK.
O.LOG_DATA	The TOE shall generate a protocol entry containing the following information whenever health insurance data or emergency data is written to the persistent storage of the TOE: • the timestamp, • the approval number of the TOE as specified in [5]. Additional information may be added to this a protocol entry, as long as no patient information is revealed within or by the protocol entry.
O.TRANSFER	The TOE shall enable the medical supplier to transfer data records to the DMS only. The TOE shall never transmit health insurance data or emergency data to card slots. The integrity of the data records is to be protected during transmission by an EDC as specified in [5].
O.DMS_CONNECTION	The TOE shall not permit access to the KVK or eHC while the TOE is connected to the DMS. If the TOE uses a docking station, this docking station shall transmit health insurance data and emergency data to the DMS only. It shall never store either indefinitely.
O.C2C	The TOE shall initiate the card-to-card authentication between the authorised card and the eHC right before the TOE reads/writes data from/to the eHC. If the authentication did not succeed, no access shall be performed by the TOE[12].
O.TIME	The TOE shall provide a reliable timestamp for the following purposes: • logging of eHC accesses, • generation of protocol data, • the checking of the validity period of card certificates. The TOE shall not allow the setting of the date while health insurance data is still in the persistent storage of the TOE.
O.SEALING	The body of the TOE shall be equipped with a seal by the manufacturer. Body and seal protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The body and the sealing shall be compliant to BSI – TR 03120

Objective	Description
	([8])[13].

Table 10: Security Objectives for the TOE

Application Note 1: The ST author shall erase all application notes resp. parts of application notes which are addressed to the ST author, e.g. this one.

Application Note 2: The ST author shall erase the paragraph "Optionally the TOE … by the medical suppliers" in O.I&A if the optional "TOE reset without authentication" is not implemented.

Application Note 3: The ST author may erase the paragraph "The TOE shall … by the medical suppliers" in O.MANAGEMENT if the optional "TOE reset without authentication" is not implemented. Accordingly section 4.3 Security Objectives Rationale has to be aligned.

Application Note 4: The TOE may also provide a management interface for developers. In this case define security objectives and SFR which describe the developer authentication mechanism and the associated rights.

Application Note 5: If the optional printer is implemented the TOE may also provide a management interface for developers. In this case define security objectives and SFRs which describes the developer authentication mechanism and the associated rights.

4.2 Security Objectives for the operational Environment

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

Objective	Description
OE.MEDIC	The medical supplier shall be non hostile, always act with care, and read the existing guidance documentation of the TOE. The medical supplier shall ensure that the rules for the operational environment of the TOE are adhered to as required by the guidance. The medical supplier shall be responsible for the secure operation of the TOE. This responsibility is equivalent to their responsibility for the safe operation of medical devices, the adherence with data protection, and the safe storage of drugs.[6] If the medical supplier uses a SMC-B for an authorised card, the medical supplier shall not hand over the TOE to any other user (medical supplier or administrator) before the data stored within the terminal has been transferred to the DMS.[7] Further, the medical supplier shall ensure that • they never disclose the card holder PIN; • they are not observed while entering the card holder PIN; • they are not observed while reading insurance and emergency data from the display (with one exception: the medical supplier may show a patient his insurance and emergency data); • the authorised card is pulled from the card slot or the authenticated state of the TOE is dropped manually when the TOE is no longer in use; • they check the local interface to the DMS before and while transferring data to prevent wiretapping; • they check that the sealing and the body of the TOE is undamaged every time the device is used by the medical supplier; • they request the administrator to set the time-out value for medical supplier inactivity as low as possible and • they do only use the TOE after consulting with the administrator if “TOE reset without authentication”, “First TOE usage” or “Firmware Update” messages are indicated.

OE.ADMIN	The administrator shall be non hostile, always act with care, knows the existing guidance documentation of the TOE and adhere to the rules of the TOEs environment. The administrator will ensure that • the time of the TOE is set correctly, • the firmware is only updated to certified versions, • they set the new administrator PIN immediately upon performing the reset to factory defaults • they set the time-out value for the medical supplier inactivity during the initial start-up and afterwards, • they never disclose the PIN for the management interface, • they are not observed while entering the PIN for the management interface, • they check that the sealing and the body of the TOE is undamaged every time the device is used by the administrator, • they inform the medical suppliers about firmware updates and "TOE resets without authentication" and • they prevent the further TOE usage in case of a reasonable suspicion of TOE manipulation.
OE. Developer	The developer is assumed to be non hostile, always act with care and knows the existing guidance documentation of the TOE. The developer provides an additional TOE reset mechanism (fallback). If the fallback is implemented in the recommended way by a TOE Reset PIN: The developer sets an initial, unpredictable device-specific TOE Reset PIN for the TOE reset mechanism before delivery to the user. The developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator's authenticity. The request is documented by the developer. If the fallback mechanism is implemented by a challenge response mechanism: The developer sets an unpredictable device-specific shared secret for a challenge response mechanism which is used for the TOE reset mechanism before delivery to the user. The developer stores the shared secret in a safe way and tells the administrator the response to a challenge on his request after the successful verification of the administrator's authenticity. The request is documented by the developer.

OE.CARDS	The authorised cards and the eHC are smart cards that comply with the specification of the gematik as referenced in [5]. The authorised card shall provide the following functionality to the TOE: • Identification and authentication of medical suppliers using a PIN • Unlocking of eHCs via card-to-card authentication • Generation of random numbers for the generation of symmetric keys as specified in [4]. • Asymmetric encryption/decryption of symmetric keys which are used to encrypt the persistent storage of the TOE. • Emergency data on the eHC shall be signed with the use of the authorised card that created the data records on the eHC to allow the TOE to verify integrity.
OE.DMS	The TOE shall only be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier. Furthermore, the connection between the TOE and the DMS shall be: • established using a cable (USB, RS-232, etc.) • be under the sole control of the medical supplier • easy to survey for the medical supplier. Network interfaces (e.g. Ethernet) shall not be used.
OE.PHYSICAL	The secure TOE environment shall protect the TOE against physical manipulation. Specifically, the environment shall assure that • the card holder PIN can not be intercepted during transfer to the authorised card, and • data records can not be intercepted during transfer from the TOE to the DMS. The TOE shall have no unnecessary electronic contacts and no obvious constructional defects.
OE.ENVIRONMENT	While the TOE is in use by either the medical supplier or the administrator, they shall always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE is not in use, it is kept in a secure area. • The secure area is checked for physical manipulation before the TOE is taken from it and used. • A breach of this secure area by an attacker must be detectable. In this case the TOE has to be replaced, regardless of whether there is any visible sign of manipulation of the TOE.

Table 11: Security Objectives for the environment of the TOE

4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage. The following chapters provide a more detailed explanation of this mapping.

	O.PIN	O.RESIDUAL	O.SELFTESTS	O.PROTECTION	O.AUTH_STATE	O.I&A	O.MANAGEMENT	O.LOG_CARDS	O.LOG_DATA	O.TRANSFER	O.DMS_CONNECTION	O.C2C	O.TIME	O.SEALING	OE.MEDIC	OE.ADMIN	OE.CARDS	OE.DMS	OE.PHYSICAL	OE.ENVIRONMENT	OE.DEVELOPER
T.MAN_HW															X	X		X	X	X	
T.ACCESS				X													X				
T.DATA	X	X		X	X	X	X								X		X				
T.AUTH_STATE					X										X	X				X	
T.FIRMWARE		X				X	X														
T.ADMIN_PIN						X										X					X
OSP.LOG_CARDS								X													
OSP.LOG_DATA									X												
OSP.TRANSFER										X											
OSP.DMS_CONNECTION											X										
OSP.C2C												X									
OSP.TIME													X			X					
OSP.SEALING														X							
OSP.SELFTESTS			X																		
OSP.EMERGENCY_DATA				X																	
A.MEDIC															X						
A.ADMIN																X					
A.CARDS																	X				
A.DMS																		X			
A.PHYSICAL																			X		
A.ENVIRONMENT																				X	

Table 12: Security Objective Rationale

4.3.1 Countering the threats

The threat **T.MAN_HW**, which describes that an attacker may try to manipulate the TOE physically, is countered by a combination of *OE.MEDIC*, *OE.ADMIN*, *OE.DMS*, *OE.PHYSICAL* and *OE.ENVIRONMENT*. *OE.MEDIC* describes that medical suppliers are responsible for the secure operation of the TOE and especially that they shall check the TOE for manipulations. Further, the connection to the DMS shall be surveyed by the medical suppliers. *OE.ADMIN* states that the administrator has to adhere to the rules of the operational environment of the TOE while it is under the administrator's control and lists the administrator's scope of duties for a secure operation of the TOE. *OE.DMS* describes that the connection of the TOE to a trusted DMS shall be under the sole control of the medical supplier and easy to survey which prevents an interception of the connection. *OE.PHYSICAL* describes that the environment of the TOE shall generally protect against physical manipulation of the TOE. *OE.ENVIRONMENT* describes the general handling of the TOE in terms of the control the user (medical supplier and administrator) has to exert over the environment of the TOE. The last objective is supposed to cover the main part of the threat. In [11] changes are described which are necessary to provide physical protection of the TOE by the TOE itself if the assumptions on the environment have been weakened.

The threat **T.ACCESS**, which describes that an attacker may try to access data in storage that has been stored with a different authorised card, is countered by a combination of *O.PROTECTION*, and *OE.CARDS*. *O.PROTECTION* describes the access control functionality and cryptographic functionality used for the protection of stored data. *OE.CARDS* describes the functionality of the authorised card which is used to encrypt the data.

The threat **T.DATA**, which describes that an attacker may try to read or modify assets, is countered by a combination of *O.PIN*, *O.RESIDUAL*, *O.PROTECTION*, *O.AUTH_STATE*, *O.I&A*, *O.MANAGEMENT*, *OE.MEDIC*, and *OE.CARDS*. *O.PIN* describes that the PIN shall never be released except to the authorised card. *O.RESIDUAL* describes the residual information protection. *O.PROTECTION* describes the access control functionality and the protection of the data using cryptography. *O.AUTH_STATE* describes that the TOE deletes all unencrypted sensitive information in case of prolonged user inactivity or if the session is terminated manually or by removing the authorised card. *O.I&A* describes that the TOE shall authenticate administrators. *O.MANAGEMENT* describes the management of firmware and time by authenticated administrators. *OE.MEDIC* describes the precautions the medical supplier has to take in order to prevent manipulation of the TOE by an attacker. Finally, *OE.CARDS* describes the necessary functionality which shall be provided by the authorised card.

The threat **T.AUTH_STATE**, which describes that an attacker could steal the TOE with a plugged and unlocked authorised card, is countered by a combination of *O.AUTH_STATE*, *OE.MEDIC, OE.Admin* and *OE.ENVIRONMENT. O.AUTH_STATE* describes the occasions on which the device shall drop the authenticated state. *OE.MEDIC* and *OE.ADMIN* describe that the medical supplier and the administrator shall be responsible for the secure usage of the device and *OE.ENVIRONMENT* describes the general handling of the TOE in terms of the control the medical supplier and the administrator has to exert over the environment of the TOE.

The threat **T.FIRMWARE**, which describes that an attacker could try to alter firmware of the TOE, is countered by a combination of *O.I&A*, *O.MANAGEMENT and O.RESIDUAL*. *O.I&A* describes that the TOE shall authenticate administrators and that medical suppliers shall be notified about TOE resets without authentication. *O.MANAGEMENT* describes the management functionality for updating the firmware including a verification of the firmware's authenticity. Medical suppliers will be notified about firmware updates. *O.RESIDUAL* describes how the TOE protects the administrator PIN by deleting it from volatile memory when it is no longer used.

The threat **T.ADMIN_PIN**, which describes that an attacker may attempt to guess, predict or spy out the administrator PIN or credentials for the TOE reset mechanism is countered by *O.I&A*, *OE.ADMIN* and *OE.Developer*. *O.I&A* describes that the authentication mechanisms for the administrator PIN and credentials of the TOE reset mechanism protect PIN and credentials by various means during PIN entry and processing and through its quality. *OE.ADMIN* describes that the administrator has to protect PIN by ensuring its secrecy. *OE.Developer* describes that credentials for a TOE reset mechanism are stored in a safe way by the developer and that a TOE Reset Pin resp. the answer for challenge response mechanism is only told to the administrator on request after the successful verification of the administrator's authenticity.

4.3.2 Covering the OSPs

The organisational security policy **OSP.LOG_CARDS** is covered by *O.LOG_CARDS* as directly follows.

The organisational security policy **OSP.LOG_DATA** is covered by *O.LOG_DATA* as directly follows.

The organisational security policy **OSP.TRANSFER** is covered by *O.TRANSFER* as directly follows.

The organisational security policy **OSP.DMS_CONNECTION** is covered by *O.DMS_CONNECTION* as directly follows.

The organisational security policy **OSP.C2C** is covered by *O.C2C* as directly follows.

The organisational security policy **OSP.TIME**, which describes that the provides a reliable time stamp for various purposes, is covered by *O.TIME* as directly follows and by *OE.ADMIN*. *OE.ADMIN* describes that the administrator is responsible for ensuring that the time settings of the TOE are correct.

The organisational security policy **OSP.SEALING** is covered by *O.SEALING* as directly follows.

The organisational security policy **OSP.SELFTESTS** is covered by *O.SELFTESTS* as directly follows.

The organisational security policy **OSP.EMERGENCY_DATA**, which describes that the TOE has to verify the integrity and the correct visualisation of the emergency data, is covered by *O.PROTECTION*. *O.PROTECTION* describes that the TOE verifies the integrity of the emergency data by mathematically verifying the signature and that the TOE provides secure storage and secure visualisation of the emergency data.

4.3.3 Covering the assumptions

The assumption **A.MEDIC** is covered by *OE.MEDIC* as directly follows.
The assumption **A.ADMIN** is covered by *OE.ADMIN* as directly follows.
The assumption **A.CARDS** is covered by *OE.CARDS* as directly follows.
The assumption **A.DMS** is covered by *OE.DMS* as directly follows.
The assumption **A.PHYSICAL** is covered by *OE.PHYSICAL* as directly follows.
The assumption **A.ENVIRONMENT** is covered by *OE.ENVIRONMENT* as directly follows.

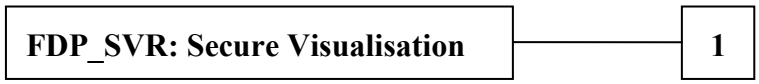
5 Extended Components Definition

5.1 Definition of the family FDP_SVR Secure Visualisation

Family Behaviour

This family describes the requirements for a secure visualisation component for the correct visual representation of the emergency data[1] read for the eHC. The visual representation of this data must be in accordance to the requirements of the data scheme as specified in FDP_SVR.1.1. The entire data shall be displayed if possible; otherwise the user will be notified that the representation of the data is incomplete. Data which can not be unambiguously displayed shall not be displayed at all and the user shall be notified.

Component levelling



FDP_SVR.1 Secure visualisation of data content requires the presentation of data content according to the assigned scheme as specified in FDP_SVR.1.1. The TSF is required to reject visual representation of data which cannot be interpreted unambiguously according to this scheme by the TSF and notify the user. Furthermore it is required that the data is either displayed in its entirety or that the user is notified when the data is displayed incompletely.

Management: FDP_SVR.1

There are no management activities foreseen.

Audit: FDP_SVR.1

There are no auditable activities foreseen.

FDP_SVR.1 Secure visualisation of data content

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SVR.1.1	The TSF shall ensure that the [assignment: *data to be interpreted*] is represented completely and unambiguously according to the [assignment: *data scheme*].
FDP_SVR.1.2	The TSF shall notify the user if the visualisation of the data[18] is incomplete.
FDP_SVR.1.3	The TSF shall reject any visual representation of data which comprises parts which cannot be interpreted or represented unambiguously by the TSF according to the [assignment: *data scheme*] and notify the user.

[18] The term "data" in FDP_SVR.1.2 and FDP_SVR.1.3 refers to the data ("*data to be interpreted*") as assigned in FDP_SVR.1.1.

6 Security Requirements

This chapter defines the functional requirements and the security assurance requirements for the TOE.

Operations for assignment, selection, refinement and iteration have been performed. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

All performed operations from the original text of [2] are written in *italics* for assignments, underlined for selections and **bold** text for refinements. Furthermore the brackets ("[]") from [2] are kept in the text.

All operations which have to be completed by the ST author are marked with the words: "assignment" or "selection" respectively.

Application Note 6: If the PP allows different TOE configurations or optional features the ST author shall refine the SFRs to clarify which TOE configurations and optional features are used.

Application Note 7: The ST author shall specify for all SFRs which contain cryptographic algorithms which algorithms / methods and which parameters (e.g. key sizes) are used. When an SFR in the PP refers to [4] the ST author shall quote the section of [4] he refers to for the selection of a cryptographic algorithm / method and its parameters.

The ST author shall introduce these information by refinements or in the form of an annex to the ST.

6.1 Security Functional Requirements

The TOE has to satisfy the SFRs delineated in the following table. The rest of this chapter contains a description of each component and any related dependencies.

Cryptographic Support (FCS)	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/AES	Cryptographic operation for storage encryption
FCS_COP.1/FW	Cryptographic operation for signature verification of firmware updates
FCS_COP.1/DATA	Cryptographic operation for signature verification of emergency data
User data protection (FDP)	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1/Cards	Subset information flow control for card communication

FDP_IFC.1/DMS	Subset information flow control for communication with DMS
FDP_IFC.1/MSI	Subset information flow control for medical supplier information
FDP_IFF.1/Cards	Simple security attributes for card communication
FDP_IFF.1/DMS	Simple security attributes for communication with DMS
FDP_IFF.1/MSI	Simple security attributes for medical supplier information
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1/FW	Subset residual information protection
FDP_RIP.1/UserData	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_SVR.1	Secure visualisation of data content
Identification and authentication (FIA)	
FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of Authentication
FIA_UAU.5	Multiple authentication mechanism
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of Identification
Security Management (FMT)	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_MTD.3	Secure TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
TOE Access (FTA)	
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
Protection of the TSF (FPT)	
FPT_PHP.1	Passive detection of physical attack
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing

Table 13: Security Functional Requirements for the TOE

6.1.1 Cryptographic Support (FCS)

6.1.1.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [*as specified in [4]*] that meet the following: [*symmetric encryption standards according to [4]*].

Hierarchical to: No other components.

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

Application Note 8: The TOE shall use a hybrid encryption method according to [4]. The cryptographic symmetric key, generated by FCS_CKM.1 shall be used for the symmetric encryption of the emergency data and the health insurance data within the persistent storage of the TOE. The symmetric encryption key is then encrypted via the authorised card.

The generation of the symmetric key is performed using a random number generator which is provided by the authorised card.

6.1.1.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [*cryptographic standards according to [4]*].

Hierarchical to: No other components.

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

6.1.1.3 FCS_COP.1/AES Cryptographic operation for storage encryption

FCS_COP.1.1/AES The TSF shall perform [*symmetric encryption and decryption*] in accordance with a specified cryptographic algorithm [*specified in [4]*] and cryptographic key sizes [*specified in [4]*] that meet the following: [*cryptographic standards according to [4]*].

Hierarchical to: No other components.

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

Application Note 9: The cryptographic functionality in FCS_COP.1/AES and FCS_CKM.1 shall be used to encrypt the emergency data and the health insurance data (protected and unprotected) within the persistent storage of the TOE.

The symmetric key is then asymmetrically encrypted using the functionality of the authorised card. The corresponding protocol data is not encrypted.

6.1.1.4 FCS_COP.1/FW Cryptographic operation for signature verification of firmware updates

FCS_COP.1.1/FW The TSF shall perform [*signature verification for firmware updates*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [*[4]*].

Hierarchical to: No other components.

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

Application Note 10: The functionality for signature verification is used to check the integrity and authenticity of a potential firmware update. Such functionality usually relies on hashing and encryption using a public key. The public key must be part of the installed firmware. Further details on the used cryptographic algorithms need to be specified by the ST author.

6.1.1.5 FCS_COP.1/DATA Cryptographic operation for signature verification of emergency data

FCS_COP.1.1/DATA The TSF shall perform [*signature verification for emergency data*[1]] in accordance with a specified cryptographic algorithm [*as specified in [4]*] and cryptographic key sizes [*as specified in [4]*] that meet the following: *[4]*.

Hierarchical to: No other components.

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

Application Note 11: The functionality for signature verification is used to check the integrity of the emergency data using the public key from the emergency data (see FDP_ITC.1). The functionality is not used to check for a qualified signature according to [9] but to check the mathematical correctness of the signature.

Application Note 12: If a challenge response mechanism is used for a TOE reset mechanism: The ST writer shall add an iteration of FCS_COP.1 for the generation of challenges and calculation of correct answers.

6.1.2 User data protection (FDP)

6.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [*MobCT SFP*] on [
Subjects:

- *authorised card,*
- *user (administrator or medical supplier)*

Objects:

- *card holder PIN,*
- *administrator PIN,*
- [assignment*: credentials for the TOE reset mechanism*],
- *health insurance data,*
- *emergency data,*
- *firmware,*
- *public key for firmware verification,*
- *time settings,*

- *symmetric keys (encrypted and decrypted)*,
- *card slot,*
- *access logging data*
- [assignment: *other objects*]

Operations:

- *Read,*
- *modify,*
- *delete*
- [assignment: *other operations*]].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note 13: Name the kind of credentials which are used for the TOE reset mechanism (e.g. TOE Reset PIN or shared secret for a challenge response mechanism).

6.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [*MobCT SFP*] to objects based on the following: [

Subjects:

- *authorised card,*
- *user (administrator or medical supplier)*

Objects:

- *card holder PIN,*
- *administrator PIN,*
- [assignment*: credentials for the TOE reset mechanism*],
- *health insurance data,*
- *emergency data,*
- *firmware,*
- *public key for firmware verification,*
- *cross CVCs*
- *time settings,*
- *symmetric keys (encrypted and decrypted),*
- *card slot,*
- *access logging data*

Object attributes:

- *firmware version*,
- *administrator PIN validity*,

[assignment: other objects and related attributes or none]].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *Access to health insurance data or emergency data from the storage shall be allowed if the data was decrypted with the help of the same authorised card which was used to encrypt the data.*
- *An update of the firmware of the TOE shall only be allowed by an authenticated administrator:*
  - *A firmware consists of two parts: firstly the so-called "firmware list" and secondly the "firmware core" which includes the whole firmware except the firmware list. The firmware list states all firmware core versions to which a change is allowed. Firmware lists and cores have to be versioned independently.*
  - *An update of the firmware core is only allowed if the core version is included in the firmware list. Firmware lists must only contain version numbers of firmware cores which are certified accordingly this Protection Profile. For the use in the German Healthcare System the named versions must also be approved by the Gematik.*
  - *In case of downgrades of the firmware core the TOE must warn the administrator before the installation that he is doing a downgrade, not an upgrade. The TOE must offer him the chance to cancel the installation.*
  - *Firmware list and core can be updated independently. In case of a common update the TOE has to install the new firmware list at first. The new list is used to decide whether an update to the accompanying firmware core is allowed.*
  - *Updates of the firmware list are only allowed to newer versions. Use higher version numbers to distinguish newer versions.*
  - *Installing of firmware cores and lists are only allowed after the integrity and authenticity of the firmware has been verified using the mechanism as described in FCS_COP.1/FW.*
- *Import of cross CVCs shall only be allowed for an authenticated administrator.*
- *The TOE shall permit the authenticated administrator to modify the date of the time settings only if no data records are stored in the persistent storage of the TOE.*

- *[selection: [The TOE shall permit the authenticated administrator to enable and disable the "TOE reset without authentication" mechanism. The mechanism must be disabled by default. Performing such a TOE reset shall not be accidentally possible.] or none]*.
- *[assignment: other rules or none]*].

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules [

- *No subject shall read out or modify the card holder PIN or symmetric keys, while they are temporarily stored in the volatile memory of the TOE.*
- *No subject shall access any object other than the administrator PIN while the administrator PIN is not valid.*
- *No subject shall read out the administrator PIN.*
- *[selection: [No subject shall read out the TOE Reset PIN], [No subject shall read out the shared secret for a challenge response mechanism], [*assignment: *other rules for the TOE reset mechanism]*,
- *No subject shall modify the public key for the signature verification for firmware updates.*
- *While the TOE is connected to the DMS no subject shall be allowed to access a card slot containing an eHC or KVK,*
- *[assignment: other rules or none]*].

Hierarchical to: No other components.

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

Application Note 14: For FDP_ACF.1.1: Name the kind of credentials which are used for the TOE reset mechanism (e.g. TOE Reset PIN or shared secret for a challenge response mechanism).

Application Note 15: Specific implementations of a TOE compliant to this PP may require more objects that are subject to access control and more granular rules for access control (e.g. for printer control). Therefore, the open assignments in FDP_ACF.1.2 and FDP_ACF.1.4 should allow the ST author to specify the access control policy for the TOE in more detail.

Application Note 16: In FDP_ACF.1.2 "With the help of" refers to the fact that the data is en-/decrypted with the symmetric key which is stored on the TOE and is itself encrypted by the authorised card.

The TOE uses functionality of the authorised card to determine if the

stored data was stored with the help of (and therefore may be accessed with the help of) the authorised card. This means for FDP_ACF.1.2 that the TOE is able to determine if the decrypted data is real data and not data that was decrypted with a false key. In the latter case, access to the data shall be denied by the TOE.

Application Note 17: In FDP_ACF.1.4 "temporarily" refers in regard to the card holder PIN to the duration of PIN entry. The PIN will not be stored longer than it is necessary in order to send the PIN to the authorised card.

6.1.2.3 FDP_IFC.1/Cards Subset information flow control for card communication

FDP_IFC.1.1/Cards The TSF shall enforce the [*Card SFP*] on [

Subjects:

- *TOE logging routine,*
- *TOE routine for generation of protocol data,*
- *medical supplier,*
- *authorised card*
- *electronic health card*

Information:

- *card holder PIN,*
- *X.509 certificate,*
- *health insurance data,*
- *emergency data (including signature and public signature key),*
- *eHC access log entries,*
- *protocol data*

Operation:

- *entering the card holder PIN,*
- *reading out the X.509 certificate,*
- *transferring health insurance and emergency data*
- *writing an access log entry to the logging container of the eHC*
- *generating protocol data for the health insurance data and the emergency data*].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

6.1.2.4 FDP_IFC.1/DMS Subset information flow control for communication with DMS

FDP_IFC.1.1/DMS The TSF shall enforce the [*DMS communication SFP*] on [
Subjects:
- *TOE routine for DMS data transfer,*
- *[selection: docking station or none]*.

Information:
- *health insurance and emergency data records,*
- *protocol data*

Operation:
- *data transfer to DMS*].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

6.1.2.5 FDP_IFC.1/MSI Subset information flow control for medical supplier information

FDP_IFC.1.1/MSI The TSF shall enforce the [*MS information SFP*] on [
Subjects:
- *medical supplier*

Information:
- *first TOE usage (unknown medical supplier),*
- *firmware update,*
- *TOE reset without authentication.*

Operation:
- *notification and acknowledgement*].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

Application Note 18: For the ST author: It is allowed to discard the "MS information SFP" expressed in FDP_IFC.1/MSI and FDP_IFF.1/MSI if the "TOE reset without authentication" mechanism is not implemented. Accordingly section 6.3 Security Requirements Rationale has to be aligned.

6.1.2.6 FDP_IFF.1/Cards Simple security attributes for card communication

FDP_IFF.1.1/Cards The TSF shall enforce the [*Card SFP*] based on the following types of subject and information security attributes: *[none]*.

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

- *Before permitting any other interaction with a card, the TOE shall read out the card's X.509 certificate and check*
  - *whether the card claims to be an authorised card and*
  - *whether the current date given by the TOE falls within the validity period of the certificate.*
- *Card holder PINs entered via the PIN pad shall only be sent to the card slot where the authorised card is plugged in. No PIN must be sent to the card slot where the eHC is plugged in.*
- *The TOE shall only read data from the eHC when the card-to-card authentication between the authorised card and the eHC succeeded recently.*

].

FDP_IFF.1.3/Cards The TSF shall enforce the [*following rule:*

If protected health insurance data or emergency data is read from the eHC, the TOE shall write an access log entry to the logging container of the eHC[19] *including:*

- *the time of access,*
- *the accessed data, and*
- *the identity of the authorised card which was used to access the eHC*

If health insurance data or emergency data read from the eHC is stored by the TOE, the TOE shall generate a protocol data entry and attach it to the health insurance data or emergency data. The protocol data shall include:

- *the time of access,*
- *terminal approval number,*
- *[assignment: further data or none]*

].

FDP_IFF.1.4/Cards The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5/Cards The TSF shall explicitly deny an information flow based on the following rules: [

- *The TOE shall never write data to containers of the eHC other*

[19] The eHC possesses a logging container. Every read-access to the eHC which accesses emergency data or protected health insurance data has to be logged within this container.

than the logging container.

- *The TOE shall never write data to the KVK.*
- *Health insurance data and emergency data shall never be transferred to any card slot.*
- *The TOE shall never include patient specific data within or by its protocol data.*

].

Hierarchical to: No other components.

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

Application Note 19: FDP_IFF.1.2/Cards: Here "recently" means that the C2C authentication shall be initiated every time right before data is read from an eHC. This limits the risk that the eHC can be replaced with a faked eHC to read faked data records.

Application Note 20: FDP_IFF.1.3/Cards: The identity of the authorised card which was used to access the eHC clearly identifies the medical supplier that initiated the operation. However, in case the authorised card is not a personal card but a card of an institution/organisation used by more than one medical supplier, the institution/organisation needs to account which person possessed the card at a specific time.

Application Note 21: FDP_IFF.1.3/Cards and FDP_IFF.1.5/Cards: The developer may add additional information to the protocol data as long as the information does not reveal patient specific data. Patient specific data is any data, which enables the reader to infer which patient the data refers to.

6.1.2.7 FDP_IFF.1/DMS Simple security attributes for communication with DMS

FDP_IFF.1.1/DMS The TSF shall enforce the [*DMS communication SFP*] based on the following types of subject and information security attributes: [*Information attributes: date of data record readout from eHC*].

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

- *The TOE shall enable the medical supplier to transfer data records from the persistent storage to the DMS.*
- *The TOE shall provide the transfer data with error detection as specified in [5].*
- *[selection:*

  The docking station shall transfer the emergency data and the health insurance data to the DMS only. It shall never store either indefinitely.

  or

  no further rules]

].

FDP_IFF.1.3/DMS The TSF shall enforce ~~**the**~~ [*no further rules*].

FDP_IFF.1.4/DMS The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5/DMS The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Hierarchical to: No other components.

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

Application Note 22: FDP_IFC.1.1/DMS und FDP_IFF.1.2/DMS: The selection allows the ST author to specify the transfer to the DMS via a docking station, depending on whether the TOE uses a docking station or not.

6.1.2.8 FDP_IFF.1/MSI Simple security attributes for medical supplier information

FDP_IFF.1.1/MSI The TSF shall enforce the [*MS information SFP*] based on the following types of subject and information security attributes: [*none*].

FDP_IFF.1.2/MSI The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*none*].

FDP_IFF.1.3/MSI The TSF shall enforce [*the following rule:*

The TOE shall notify the medical suppliers immediately after a successful authentication with HPC and PIN in case of

- *their first TOE usage (new / unknown user),*
- *their first TOE usage after firmware updates and*
- *their first TOE usage after a TOE reset without authentication.*

The messages shall be acknowledged by the medical suppliers[16].

].

FDP_IFF.1.4/MSI The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5/MSI The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Hierarchical to: No other components.

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

6.1.2.9 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [*MobCT SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*none*].

Hierarchical to: No other components.

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

Application Note 23: User data in FDP_ITC.1 is the public key of the associated private key that was used to sign the emergency data[1] on the eHC. The public key

is also transferred from the eHC (as part of the data) to the TOE in order to check the signature for mathematical correctness.

6.1.2.10 FDP_RIP.1/FW Subset residual information protection

FDP_RIP.1.1/FW The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**reset to factory defaults and** deallocation of the resource from] the following objects: [*all information in the memory of the TOE except the installed firmware, and [assignment: TOE reset credentials, other objects or none]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 24: The data to be erased includes encrypted health insurance and emergency data in the persistent storage, as well as temporary user data e.g. an unencrypted symmetric encryption key and user settings.

6.1.2.11 FDP_RIP.1/UserData Subset residual information protection

FDP_RIP.1.1/UserData The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**dropping of the authenticated states, power loss and** deallocation of the resource from] the following objects: [*temporary data in the persistent storage of the TOE and in the volatile memory of the TOE i.e.*

- *the unencrypted symmetric encryption key for the storage,*
- *unencrypted health insurance data,*
- *unencrypted emergency data,*
- *card holder PIN of the medical supplier,*
- *PIN for the management interface and*
- *[assignment: other objects or none]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 25: The data to be erased does not include the encrypted data storage of the TOE or user settings.

6.1.2.12 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in ~~**containers**~~ **the persistent storage of the TOE** controlled by the TSF for [*all integrity errors*] on all objects**,** based on the following attributes: [assignment: *user data attributes*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*not use the data, inform the medical supplier, and [assignment: other actions or none]*].

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

Application Note 26: The user data attributes shall be filled in by the ST author, as the integrity check is supposed to be implementation dependent.

Application Note 27: For integrity protection of emergency data[1] it is also necessary that the medical supplier is able to read the data unaltered from the display without loss of information.

It is not necessary to show an emergency data record completely if it exceeds the space on the display, but the medical supplier shall then be informed that there is still some remaining undisplayed data. In that case they shall be able to navigate through the remaining parts of the record using a scroll bar or similar.

Application Note 28: The notification of the medical supplier in case of an integrity error shall be visual.

6.1.2.13 FDP_SVR.1 Secure visualisation of data content

FDP_SVR.1.1 The TSF shall ensure that the [*emergency data[1] and [assignment: further data to be interpreted]*] is represented completely and unambiguously according to the [*scheme specified in [5]*].

FDP_SVR.1.2 The TSF shall notify the user if the visualisation of the data is incomplete.

FDP_SVR.1.3 The TSF shall reject any visual representation of data which comprises parts which cannot be interpreted or represented unambiguously by the TSF according to the [*scheme specified in [5]*] and notify the user.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [3] unsuccessful authentication attempts occur related to [*the last successful authentication attempt via the management interface*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the authentication mechanism for a period of time according to Table 14 depending on the number of consecutive unsuccessful authentication attempts*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

Unsuccessful authentication attempts	Lockout time
3–6	1 minute
7–10	10 minutes
11–20	1 hour
> 20	1 day

Table 14: Lockout times

6.1.3.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following:** [

A PIN for the management interface shall meet the following:

- *Have a length of at least 8 characters,*
- *Be composed of at least the following characters: "0"-"9",*
- *Shall not contain the User ID / logon name as a substring,*
- *Shall not be saved on programmable function keys*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 29: If the TOE implements the user ID for the management interface, the rule within the selection is to be applied. Otherwise it shall be discarded.

Application Note 30: PIN for the management interface are the administrator PIN and, if applicable, the TOE Reset PIN. They are also named as "login credentials", "administrator credentials" and "administrator login credentials".

Application Note 31: Previous PP versions contained a bullet point “Shall not be displayed as clear text during entry”. It has been removed because of its redundancy to FIA_UAU.7.1 which describes that PINs have to displayed as asterisks during entry.

6.1.3.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*all TSF mediated actions but*

- *Firmware update*
- *Import of Cross CVCs*
- *Management of time settings,*
- *Reset to factory defaults,*
- *Management of login credentials*
- *[assignment: further TSF mediated actions or none]*

] 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.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

Application Note 32: The ST author shall add that a reset to factory defaults is allowed before identification and authentication if a “TOE reset without authentication” mechanism is implemented and activated.

6.1.3.4 FIA_UAU.5 Multiple authentication mechanism

FIA_UAU.5.1 The TSF shall provide [

- *a PIN based authentication mechanism for the management interface*
- *a PIN interface for the authentication of the medical supplier to the authorised card*

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following rules:** [

- *Administrators shall be authenticated to the management interface using the “PIN based authentication mechanism”.*
- *The TOE provides the interface for PIN entry for the authentication of the medical supplier to the authorised card and accepts the result of this authentication for the authentication of the medical supplier role to the TOE.*]

Hierarchical to: No other components.

Dependencies: No dependencies.

6.1.3.5 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [*asterisks as replacement for PIN digits during PIN entry*] to the user while the authentication is in progress.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

Application Note 33: This SFR provides protected authentication feedback for entry of the management PIN and the card holder PIN.

In case of the card holder PIN, identification is provided by the authorised card in the environment of the TOE. However, the card holder PIN is entered via the PIN pad of the MobCT (see FIA_UAU.5).

6.1.3.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [*all TSF mediated actions but*

- *Firmware update*
- *Import of Cross CVCs*
- *Management of time settings,*
- *Reset to factory defaults,*
- *Management of login credentials*
- *[assignment: further TSF mediated actions or none]*

] 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.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 34: For the PP FIA_UID.1 and FIA_UAU.1 are used for the identification and authentication of the administrator and for the medical supplier, but the list of TSF mediated actions does not contain any actions which

the medical supplier is permitted to perform (compare FMT_MTD1.1) even after authentication. If the ST author wishes to add functionality to the TOE, which is restricted to the medical supplier and only available after authentication, this functionality should also be listed here.

Furthermore, the ST author may add functionality for other users to the identification/authentication mechanism.

Application Note 35: The ST author shall add that a reset to factory defaults is allowed before identification and authentication if a "TOE reset without authentication" mechanism is implemented and activated.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*MobCT SFP*] to restrict the ability to **[[*set*]]** the security attribute [*validity of the administrator PIN*] **[[*to valid by setting the administrator PIN*]]**[20] to [*the administrator*].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Application Note 36: The modification of the validity of the administrator PIN is tied to the change of the administrator PIN. By setting the PIN, the administrator changes the validity of the PIN to valid.

6.1.4.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [*MobCT SFP*] to provide [restrictive] default values for **the security attribute validity of the administrator PIN that is** used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ~~**the**~~ [*no one*] to specify alternative initial values to override the default values when an object or information is created.

---

[20] Performed Operations:
The selection [selection: *change_default, query, modify delete, [assignment: other operations]*] has been fulfilled by selecting the assignment. This assignment was fulfilled by "set….to valid by setting the administrator PIN" which was separated via a refinement for better readability.

Hierarchical to: No other components.

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

Application Note 37: The validity of the administrator PIN indicates whether the current PIN is valid. The PIN is only invalid directly after delivery and after or during a reset to factory defaults. Under these circumstances the attribute ensures that the TOE forces the administrator to set a valid administrator PIN in order to prevent an attacker from gaining easy access to management functionality.

6.1.4.3 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [change_default, query, modify, delete, clear, *reset*] the [

- *installed firmware,*
- *cross CVCs,*
- *time settings,*
- *device configuration,*
- *administrator login credentials*
- [assignment*: **further device settings or none***]

] to [*the administrator and [selection: developer or none]*].

Hierarchical to: No other components.

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

6.1.4.4 FMT_MTD.3 Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [*time settings*].

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

Application Note 38: Secure values for the session time-out of the medical supplier session are times between 1 and 60 minutes[15], compare FTA_SSL.3.1.

6.1.4.5 FMT_SMF.1 Specification of Management Functions

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

- *Firmware update*
- *Import of Cross CVCs*
- *Management of time settings*
- *Reset to factory defaults*
- *Management of administrator login credentials*

[assignment: other relevant management functions or none]].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.1.4.6 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*administrator, medical supplier, and [assignment*: *other roles or none]*].

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

Application Note 39: FMT_SMR.1.1: "other roles" allows the ST author to add the role developer in case the TOE can be resetted to factory default by the developer as well as the administrator

6.1.5 TOE Access (FTA)

6.1.5.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after ~~a~~ [*15 minutes*] **of administrator inactivity, after [1 – 60 minutes] of medical supplier inactivity[15] and after power loss**.

Hierarchical to: No other components.

Dependencies: No dependencies

6.1.5.2 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 40: FTA_SSL.3 and FTA_SSL.4 apply to the sessions of medical supplier and administrator.

Session termination of the medical supplier refers to the dropping of the authenticated state of the TOE. When the authenticated state is dropped, the authenticated state of the authorised card shall be dropped, too and the medical supplier has to unlock the authorised card again in order to read data from the storage or an eHC or transfer it to a DMS.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable[21] time stamps.

Hierarchical to: No other components.

Dependencies: No dependencies

6.1.6.2 FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine **during operation of the TOE**[22] whether physical tampering with the TSF's devices or TSF's elements has occurred.

Hierarchical to: No other components.

[21] The clock precision shall be at least ±100ppm (which corresponds to an aberration of 52.3 minutes in a year).

[22] The phrase "during operation of the TOE" is meant to specify that the user can determine whether physical tampering has occurred without switching of the TOE.

Dependencies: No dependencies.

Application Note 41: The capability to detect physical tampering refers to the body of the TOE and its required sealing by the manufacturer.

The evaluator will examine that body and sealing are compliant to BSI – TR 03120 ([8])[13].

6.1.6.3 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up **and** at the conditions [assignment: **other** conditions under which self test should occur]] to demonstrate the correct operation of [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].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 42: As the focus of this requirement is to demonstrate the correct operation of the complete TSF, the ST author will have to describe test functionality for all important aspects of all security functions that the TOE provides.

6.2 Security Assurance Requirements

The following table lists the assurance components which are applicable to this PP.

Assurance Class	Assurance Components
ADV	ADV_ARC.1, **ADV_FSP.4, ADV_IMP.1**, **ADV_TDS.3**
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, **ALC_TAT.1**
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	**AVA_VAN.5**

Table 15: Chosen Evaluation Assurance Requirements

These assurance components represent assurance level **EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5**. The complete text for the requirements can be found in [3].

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	O.PIN	O.RESIDUAL	O.SELFTESTS	O.PROTECTION	O.AUTH_STATE	O.I&A	O.MANAGEMENT	O.LOG_CARDS	O.LOG_DATA	O.TRANSFER	O.DMS_CONNECTION	O.C2C	O.TIME	O.SEALING
FCS_CKM.1				X										
FCS_CKM.4				X										
FCS_COP.1/AES				X										
FCS_COP.1/FW							X							
FCS_COP.1/DATA				X										
FDP_ACC.1	X			X		X	X				X		X	
FDP_ACF.1	X			X		X	X				X		X	
FDP_IFC.1/Cards	X			X				X	X	X		X	X	
FDP_IFC.1/DMS										X	X			
FDP_IFC.1/MSI						X	X							
FDP_IFF.1/Cards	X			X				X	X	X		X	X	
FDP_IFF.1/DMS										X	X			
FDP_IFF.1/MSI						X	X							
FDP_ITC.1				X										
FDP_RIP.1/FW		X												
FDP_RIP.1/UserData		X												
FDP_SDI.2				X										
FDP_SVR.1				X										
FIA_AFL.1						X								
FIA_SOS.1						X								
FIA_UAU.1						X	X							
FIA_UAU.5	X					X								
FIA_UAU.7	X					X								
FIA_UID.1						X	X							
FMT_MSA.1						X								
FMT_MSA.3						X	X							
FMT_MTD.1							X							
FMT_MTD.3													X	
FMT_SMF.1							X							
FMT_SMR.1						X	X							
FTA_SSL.3					X									
FTA_SSL.4					X									
FPT_PHP.1														X
FPT_STM.1								X	X				X	
FPT_TST.1			X											

Table 16: Coverage of Security Objective for the TOE by SFR

The security objective **O.PIN** is met by a combination of the SFR *FDP_ACC.1*, *FDP_ACF.1*, *FDP_IFC.1/Cards*, *FDP_IFF.1/Cards*, *FIA_UAU.5* and *FIA_UAU.7*. *FDP_ACC.1* defines the access control policy for the TOE. *FDP_ACF.1* defines the rules for the policy which supports the secure PIN entry by preventing access to the temporarily stored PIN. *FDP_IFC.1/Cards* defines the information flow control policy for card communication. *FDP_IFF.1/Cards* defines the rules for the policy. *FIA_UAU.5* defines the authentication mechanism for the terminal via the authentication of the medical supplier at the authorised card. Finally, *FIA_UAU.7* defines that the PIN can not be read from the display during entry.

The security objective **O.RESIDUAL** is met by the SFR *FDP_RIP.1/FW* and SFR *FDP_RIP.1/Data* as it defines the residual information protection.

The security objective **O.SELFTESTS** is met by the SFR *FPT_TST.1* as it defines the self tests of the TSF which have to be provided by the TOE.

The security objective **O.PROTECTION** is met by a combination of the SFR *FCS_CKM.1, FCS_CKM.4, FCS_COP.1/AES, FCS_COP.1/DATA, FDP_ACF.1, FDP_ACC.1*, *FDP_IFC.1/Cards, FDP_IFF.1/Cards, FDP_ITC.1*, *FDP_SDI.2* and *FDP_SVR.1*. FCS_CKM.1 and FCS_CKM.4 define the cryptographic key generation and destruction used for the AES storage encryption defined in *FCS_COP.1/AES*. *FCS_COP.1/DATA* defines the mathematical signature verification of stored data. *FDP_ACC.1* and *FDP_ACF.1* define the access control policy and rules for accessing stored data. *FDP_IFC.1/Cards* and *FDP_IFF.1/Cards* define that no data shall be written to the KVK and no data other than logging data shall be written to the eHC. *FDP_ITC.1* defines the import of the public key for signature verification of emergency data. *FDP_SDI.2* explicitly defines the integrity protection of stored data. Finally *FDP_SVR.1* defines the secure visualization of the emergency data.

The security objective **O.AUTH_STATE** is met by a combination of the SFR *FTA_SSL.3* and *FTA_SSL.4*. *FTA_SSL.3* defines how the authenticated state is dropped by the TSF and *FTA_SSL.4* defines how the medical supplier and the administrator can drop the authenticated state manually.

The security objective **O.I&A** is met by a combination of the SFR *FDP_ACC.1*, *FDP_ACF.1*, *FDP_IFC.1/MSI, FDP_IFC.1/MSI, FIA_AFL.1*, *FIA_SOS.1*, *FIA_UAU.1*, *FIA_UAU.5*, *FIA_UAU.7, FIA_UID.1*, *FMT_MSA.1*, *FMT_MSA.3*, and *FMT_SMR.1*. *FDP_ACC.1* defines the access control policy for the TOE. *FDP_ACF.1* defines the rules for the policy which prevents the PIN from being read. *FIA_AFL.1* defines the authentication failure handling for the management interface. *FIA_SOS.1* defines the quality metrics of credentials used for management. *FIA_UAU.7* defines that PINs are never sent in clear text to a display. *FIA_UAU.1* and *FIA_UID.1* describe that a user has to be identified and authenticated for some TSF mediated actions. *FIA_UAU.5* defines which roles need to be authenticated. *FMT_MSA.1* and *FMT_MSA.3* define that the TOE forces the administrator to initially set the administrator PIN. *FDP_IFC.1/MSI* and *FDP_IFC.1/MSI* defines the information of the medical supplier about TOE resets without authentication. Finally, *FMT_SMR.1* defines the roles that are enforced using the authentication mechanism.

The security objective **O.MANAGEMENT** is met by a combination of the SFR *FCS_COP.1/FW*, *FDP_ACC.1*, *FDP_ACF.1*, *FDP_IFC.1/MSI, FDP_IFC.1/MSI, FIA_UAU.1, FIA_UID.1*, *FMT_MSA.3*, *FMT_MTD.1*, *FMT_SMF.1* and *FMT_SMR.1*.

FCS_COP.1/FW defines the signature verification of the firmware. *FIA_UID.1* and *FIA_UAU.1* define the identification and authentication mechanism used to access the management interface. *FMT_SMF.1* defines the management functions. *FMT_SMR.1* defines the roles used for management. *FMT_MTD.1* defines that access to some TSF data is limited to administrators. *FDP_IFC.1/MSI* and *FDP_IFC.1/MSI* defines the information of the medical supplier about two security relevant events: New/unknown user and firmware update.

The security objective **O.LOG_CARDS** is met by a combination of the SFR *FDP_IFC.1/Cards*, *FDP_IFF.1/Cards* and *FPT_STM.1*. *FDP_IFC.1/Cards* and *FDP_IFF.1/Cards* define the logging of eHC accesses and restrict the write access to the eHC to logging and deny the write access to the KVK in general. *FPT_STM.1* defines the reliable time stamp which is necessary for the logging mechanism.

The security objective **O.LOG_DATA** is met by a combination of the SFR *FDP_IFC.1/Cards*, *FDP_IFF.1/Cards* and *FPT_STM.1*. *FDP_IFC.1/Cards* and *FDP_IFF.1/Cards* define the rules for the generation of the protocol data and restrict the protocol data, which is unencrypted, to non-sensitive data. *FPT_STM.1* defines the reliable time stamp which is necessary for the generation of the protocol data.

The security objective **O.TRANSFER** is met by a combination of the SFR *FDP_IFC.1/DMS*, *FDP_IFF.1/DMS, FDP_IFC.1/Card* and *FDP_IFF.1/Card*. *FDP_IFC.1/DMS* defines the DMS communication SFP and *FDP_IFF.1/DMS* defines the rules for the DMS communication SFP. *FDP_IFC.1/Card* and *FDP_IFF.1/Card* describe that data records shall never be transferred to card slots.

The security objective **O.DMS_CONNECTION** is met by a combination of the SFR *FDP_ACC.1*, *FDP_ACF.1*, *FDP_IFC.1/DMS* and *FDP_IFF.1/DMS. FDP_ACC.1* defines the access control policy for the TOE. *FDP_ACF.1* defines the rules for the policy which prevents access to eHC and KVK cards while the TOE is connected to the DMS. *FDP_IFC.1/DMS* and *FDP_IFF.1/DMS* define the rules for the data transfer to the DMS.

The security objective **O.C2C** is met by a combination of the SFR *FDP_IFC.1/Cards* and *FDP_IFF.1/Cards*. The two SFR describe an information flow policy that requires the TOE to initiate card-to-card authentication prior to read data from an eHC.

The security objective **O.TIME** is met by a combination of the SFR *FDP_ACC.1*, *FDP_ACF.1*, *FDP_IFC.1/Cards*, *FDP_IFF.1/Cards, FMT_MTD.3* and *FPT_STM.1*. *FDP_ACC.1* defines the access control policy for the TOE. *FDP_ACF.1* defines the rules for the policy which prevents the authenticated administrator from changing the date of the time settings while data records are stored in the persistent storage. *FDP_IFC.1/Cards* and *FDP_IFF.1/Cards* define the rules for the protocol data and logging data and the checking of the validity period of the X.509 certificate, for all of which accurate time settings are used. *FMT_MTD.3* defines that only secure values for time settings shall be used. *FPT_STM.1* defines the reliable time stamp which is necessary for the authentication failure handling.

The security objective **O.SEALING** is met by the SFR FPT_PHP.1, which defines that the TOE is to be protected by seals.

6.3.2 Dependency Rationale

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the use of FCS_COP.1/AES, and FCS_CKM.4
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]	Fulfilled by the use of FCS_CKM.1
FCS_COP.1/AES	[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	Fulfilled by the use of FCS_CKM.1, FCS_CKM.4
FCS_COP.1/FW	[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	See chapter 6.3.2.1 for FDP_ITC.1 and FCS_CKM.4
FCS_COP.1/DATA	[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	Fulfilled by the use of FTP_ITC.1 See chapter 6.3.2.1 for FCS_CKM.4.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by the use of FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Fulfilled by the use of FDP_ACC.1 and FMT_MSA.3.
FDP_IFC.1/Cards	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/Cards
FDP_IFC.1/DMS	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/DMS

SFR	Dependencies	Support of the Dependencies
FDP_IFC.1/MSI	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/MSI
FDP_IFF.1/Cards	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/Cards See chapter 6.3.2.1 for FMT_MSA.3
FDP_IFF.1/DMS	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/DMS See chapter 6.3.2.1 for FMT_MSA.3
FDP_IFF.1/MSI	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/MSI See chapter 6.3.2.1 for FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/Cards See chapter 6.3.2.1 for FMT_MSA.3
FDP_RIP.1/FW	No dependencies	-
FDP_RIP.1/UserData	No dependencies	-
FDP_SDI.2	No dependencies	-
FDP_SVR.1	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.5	No dependencies.	-
FIA_UAU.7	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UID.1	No dependencies	-
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by the use of FDP_ACC.1,

SFR	Dependencies	Support of the Dependencies
	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by the use of FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.1 and FMT_SMF.1
FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FTA_SSL.3	No dependencies	-
FTA_SSL.4	No dependencies	-
FPT_PHP.1	No dependencies	-
FPT_STM.1	No dependencies	-
FPT_TST.1	No dependencies	-

Table 17: Dependencies of the SFR for the TOE

6.3.2.1 Justification for missing dependencies

The dependencies [FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] of FCS_COP.1/FW are not considered as the public key for signature verification is supposed to be brought into the TOE by the manufacturer. The dependency FCS_CKM.4 of FCS_COP.1/FW is not considered as there is no key that needs to be destructed.

The dependency FCS_CKM.4 of FCS_COP.1/DATA is not considered as there is no key that needs to be destructed.

The dependency FMT_MSA.3 for FDP_IFF.1/Cards was not considered as there are no attributes considered to be managed by the TSF in FDP_IFF.1/Cards.

The dependency FMT_MSA.3 for FDP_IFF.1/DMS was not considered as there are no attributes considered to be managed by the TSF in FDP_IFF.1/ DMS.

The dependency FMT_MSA.3 for FDP_IFF.1/MSI was not considered as there are no attributes considered to be managed by the TSF in FDP_IFF.1/MSI.

The dependency FMT_MSA.3 for FDP_ITC.1 was not considered as there are no attributes considered to be managed by the TSF in FDP_ ITC.1.

6.3.3 Security Assurance Requirements Rationale

The Evaluation Assurance Level for this Protection Profile is **EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5**.

The reason for choosing assurance level EAL 3 is that this Protection Profile shall provide the same amount of trust as the Protection Profile for eHealth card terminals [10] used in the German healthcare system.

The augmentation of AVA_VAN.5 is necessary because of the high confidentiality needs of the card holder PIN for the HPC as specified by the gematik. All other augmented assurance components are dependencies of AVA_VAN.5.

A Glossary and Acronyms

Term	Definition
AES	Advanced Encryption Standard
ASCII-ISO646DE	Character set standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI - TL 03400	Technische Leitlinie: Produkte für die materielle Sicherheit (BSI 7500)
BSI - TL 03415	Technische Leitlinie: Anforderungen und Prüfbedingungen für Sicherheitsetiketten (BSI 7586)
C2C	Card-to-card (authentication)
CC	Common Criteria
DMS	Data Management System for a practice or hospital
EDC	Error Detection Code
eHC	electronic Health Card
HPC	Health Professional Card
KVK	Krankenversichertenkarte
LAN	Local Area Network
MobCT	Mobile Card Terminal for the German Healthcare System
MS	Medical Supplier
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC	Secure Module Card
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

B Literature

Common Criteria

[1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*; Version 3.1 Revision 4, September 2012; CCMB-2012-09-001

[2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*; Version 3.1 Revision 4, September 2012; CCMB-2012-09-002

[3] *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*; Version 3.1 Revision 4, September 2012; CCMB-2012-09-003

Cryptography

[4] *gematik: Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur*, as referenced by [5]

Specifications

[5] *gematik: Spezifikation Mobiles Kartenterminal (inkl. Mini-AK und Mini-PS)*, Version 2.6.0, 17 June 2014

[6] *TeleTrusT SICCT-Spezifikation* as referenced by [5]

[7] *gematik: Einführung der Gesundheitskarte - Zulassungsverfahren Mobile Kartenterminals*, as referenced by [5]

[8] *BSI – TR 03120 Sichere Kartenterminalidentität (Betriebskonzept)*, in its current version[23]

[9] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

Protection Profiles

[10] *Common Criteria Protection Profile Electronic Health Card Terminal (eHCT)*, BSI-CC-PP-0032, in its current version

[11] *Mobile Card Terminal for the German Healthcare System: Additional security functionality for physical protection;* supplement to BSI-CC-PP-0052, in its current version

[23] Transitional arrangement: It is sufficient to fulfil version 1.0 of TR-03120 and version 1.0.2 of its amendment

a) in case of an initial certification: if an application for the issuance of a certificate based on a lower version than 1.1 of this PP was requested from BSI before 30 May 2013 and an application for the issuance of a certificate based on version 1.1 of this PP was requested from BSI before 01 April 2014 and changes of the TOE in between the two applications concern only software modifications,

b) in case of a re-certification: if an application for the issuance of a certificate based on this PP is requested from BSI before 01 April 2019 and the TOE has been certified according this PP before and changes compared to certified TOE versions concern only software modifications.