Common Criteria Security Target for the Evaluation of the Product ORGA 900 of Worldline Healthcare GmbH according to the Common Criteria 3.1 Level EAL3+ Certification-ID: BSI-DSZ-CC-0596-V3-2022

Version: 3.34
Date: 13/12/23

Table of Contents

1 ST Introduction

1.1 ST Reference

Certification Id:	**BSI-DSZ-CC-0596-V3-2022**
CC-Version:	**3.1**
Evaluation Assurance Level:	**EAL3**, augmented **by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5**
Title:	Common Criteria Security Target for the Evaluation of the Product ORGA 900 of Worldline Healthcare GmbH according to the Common Criteria 3.1 Level EAL3+
Document version:	3.34
Publication date:	13/12/23
Authors:	Löher/Weiler/Osthoff/Petersen

1.2 TOE Reference

TOE: Mobile Card Terminal ORGA 900

Product variants relevant for this evaluation:

ORGA 930 M online, mobile card terminal, graphical display, 2 full size slots (eHC / KVK and HPC / SMC-B). This involves the delivery of new ORGA 930 M online devices.

TOE Version:	4.10.0:1.0.0

The TOE version includes the following versions:

Version Hardware:	1.0.0
Manufacturing code:	HC 00 04 00 00
Version Loader:	7.5.3
Version Application:	4.10.0
Version Configuration:	1.0.0/930MONLINE

ORGA 930 M: This product is identical to ORGA 930 M online except for ALC_DEL and the configurations (see Chapter 1.4) after updating the application and the loader to the same version of ORGA 930 M online.This is just the delivery of updates to existing ORGA 930 M eGK devices.

TOE Version:	4.10.0:1.0.0
Version Configuration:	1.0.0/930M

Manufacturer / Vendor: Worldline Healthcare GmbH, Flintbek

1.3 TOE Overview

The Mobile Card Terminal (MobCT) is a smartcard terminal (TOE type). It is intended to be 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. This data can viewed on a graphical display and printed out on an external printer by the medical supplier. The medical supplier is able to transfer the stored data to a Data Management System for a practice or hospital (DMS) for accounting. A DMS with Windows can be connected to this TOE, by using the USB connection cable. After a data record has been transferred successfully, the TOE deletes the record from the storage.

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 relayed to the authorised card. Once the authorised card is unlocked, the medical supplier can plug in a user card. The authorised card unlocks the user card via card-to-card (C2C) authentication. Afterwards the TOE is able to read data from the user card.

The TOE provides functionality to store data records in its own persistent storage after the data have 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 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 administrator is able to make firmware-updates. For firmware-updates the administrator needs to have special driver and update software of the TOE. This driver and software are supports only Windows variant operating system. If the administrator forgets the Admin-PIN, he can reset the TOE to factory settings, with the help of the developer. In this case, the administrator performs a Challenge & Response (C&R) operation.

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

The Body of the TOE is sealed. The sealing is compliant to the requirements of BSI – TR 03120 [TR03120].

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 1.4.3 for a description of user cards.
3 See chapter 1.4.2 for a description of authorised cards.

1.3.1 Required none-TOE hardware/software/firmware

Required external non-TOE hardware / software / firmware is listed in chapter 1.4.4 (last paragraph).

1.4 TOE Description

The TOE is a mobile smart card terminal based on the regulations for the German healthcare system. The TOE has 2 card slots:

- one is supporting eHC / KVK and
- one is supporting HPC / SMC-B).

In addition the TOE includes an USB connector as serial interface for printer connection and an USB interface for transferring stored data records from the TOE to a data management system for a practice or hospital (DMS) for accounting and for transferring a firmware file to update and downgrade the TOE firmware. The body of the TOE is equipped with seals by the manufacturer. The seals protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The sealing is compliant to the requirements of BSI – TR 03120 [TR03120]. The sealing gives the medical supplier the possibility to detect if the device has been tampered with. 1 shows the physical components of the TOE. Please refer to chapter 1.4.4 TOE type and Physical Scope for further information about physical scope of the TOE.

The TOE

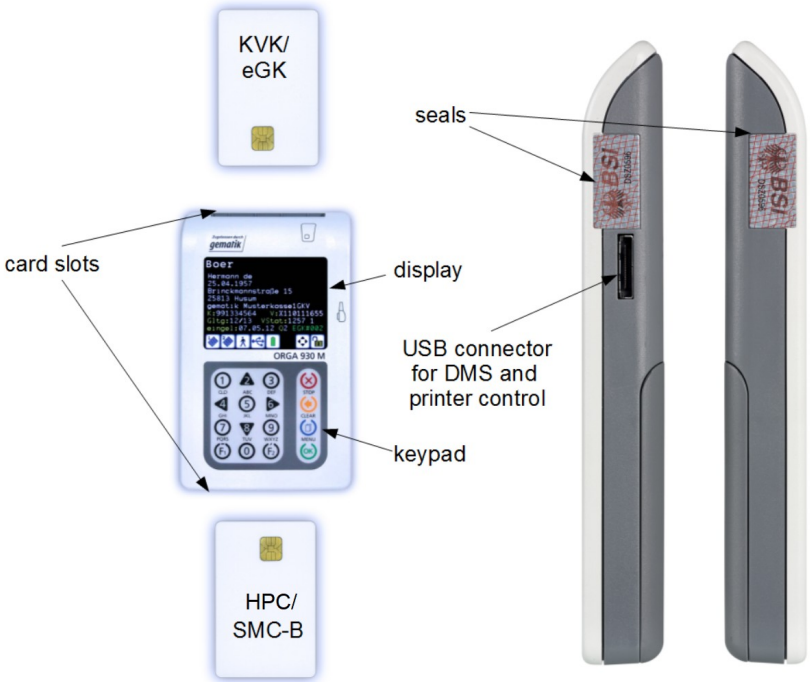

Figure 1: Physical scope of the Orga900

comprises two product variants, of which the initial variant is the "ORGA 930 M online". The hardware of the product variants is identical. The text ORGA 930 M is used in the product variants ORGA 930 M online and ORGA 930 M on the case. The application and loader are the same in both products. The differences between the product variants (listed in Chapter 1.2) are inside the configuration of the TOE. ORGA 930 M is an existing device that receive a

firmware update. ORGA 930 M online is a new device, which already contain the current TOE firmware on delivery. The TOE variants have different configurations, to distinguish the respective TOE variants from each other.

The figure 2 shows the differences within the configurations:

- Unit version
- Licensing ID

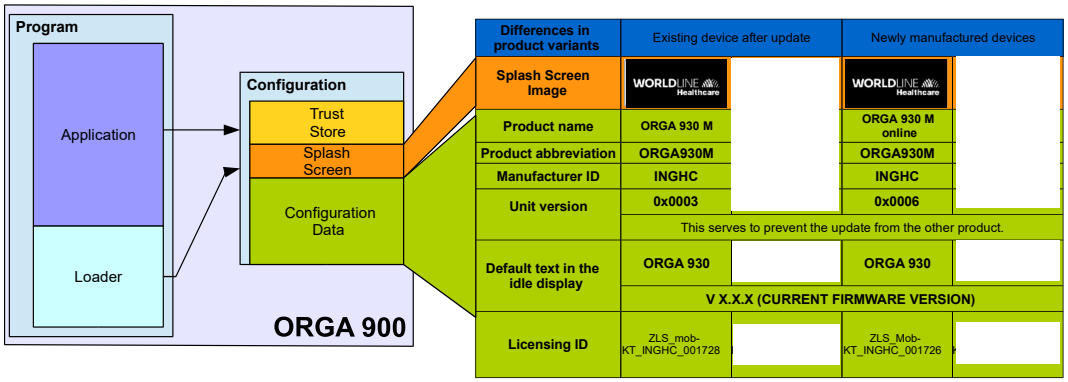

Figure 2: Differences between the product variants

The configurations can be read out in the management menu to identify the TOE. The manufacturing code can be found on the type label.

The TOE meets the security requirements of medical suppliers in order to read health insurance data and emergency data[1] from a user card[2] of a health insured person during a visit. This data can be viewed directly on the display of the TOE.

The TOE has an access control for health insurance data and emergency data. For accessing protected data the medical supplier needs an *authorised card*[3]. The TOE can support authorised cards from type German Health Professional Card (HPC) and SMC-B. Compatibility user cards are electronic Health Card (eHC) and Krankenversichertenkarte (KVK). The TOE described in this security target fulfils the requirements to be used for the user card and authorised card based on the regulations of the German healthcare system. Please refer to see Chapter 1.4.2 Authorised Cards and 1.4.3 User Cards for further information about card compatibility.

Furthermore the medical supplier needs a corresponding PIN to unlock the authorised card (card holder pin). The TOE implements information flow control for the card holder PIN. After the authorised card is unlocked the medical supplier is able to unlock other user cards via card-to-card (C2C) authentication. The unlocked authorised card is for viewing stored data records and live data record from the actual user card in the card slot on the display and printing out on an external printer. The stored data records can be transferred to the DMS.

The ORGA 900 provides functionality to store up to 275 data records in its own SFLASH (persistent storage). One of the security features of the TOE is cryptographic support for encryption of persistent storage. This implies that all data records from a user card are stored encrypted in the persitent storage. The TOE uses the functionality of the authorised card for random number generating. This random number and a public Key of DF.ESIGN and EF.ENC1 document are required for the generation of the symmetric encryption keys. The TOE stores up to 16 symmetric encryption keys indicated by serial

number (ICCSN) of the HPC. The TOE can be used by more than one medical supplier. However decryption of the data records is only possible with help of the authorised card which was used to encrypt the data. The TOE uses also the functionality of the authorised card and has to be in authenticated state for encryption and decryption of the data from user card. The encrypted insurance data are stored together with the HPC-Index and the Auth-Tag in the SFLASH of the TOE. The symmetric key and sensible information will be deleted from the volatile memory after authenticated state has been dropped down.

The medical supplier is able to delete data records manually from the TOE without transferring the data record to a DMS. After the data record has been transferred to the DMS successfully the data record will be deleted from the devices. The transmission of data with error detection by an EDC as specified in [gemSpec_MobKT]. This includes that after the data has been transferred successfully the DMS sends usually a command "read successful". Then the actual data records will be deleted and the next data record is able to be read. The connection between the TOE and the DMS will be established by using a USB cable.
Another kind of authenticated state is obtained after an administrator login (administrator authentication for an administrator session). When the TOE powers up for the first time the user is prompted to enter a new admin-pin. This pin must be 8 digits and will be stored as a generate HASH-value (SHA-512) into SFLASH of the TOE. If the administrator wants to log in later, a HASH value is also generated from the PIN input, which is compared with the stored HASH value. This includes firmware update, import of cross CVCs, management of time setting, reset to factory defaults and management of login credentials.

The delivery of the TOE includes a special update software for firmware-update and drivers.

The TOE offers the option to perform a TOE reset to factory defaults by performing a Challenge & Response (C&R) operation. On demand the TOE generates a challenge that has to be sent to the producer who in turn calculates the response data and informs the administrator about the response data. To allow the administrator to reset the TOE to factory defaults in case the TOE administrator doesn't know the PIN.

The TOE includes a self-function test which is realized by 'known-answer tests' and includes the HASH value calculation SHA-512 and AES-GCM Mode. The self-function test is performed at each start up of the TOE and can be accessed by the user via the menu operation at any time.
The TOE provides functionality to update and downgrade its firmware. This includes updating to a newer firmware and downgrading to a firmware that is included in the firmware group list. The configuration is preserved and indicated after a firmware update or a downgrade. Instructions are shown on the display of the TOE and in the PC program. The download file consists of header and data. In the first step the PC copies the download file into the TOE. In the second step examination of the contents. So it checks the downloaded signature, format, size and hardware compatibility and whether the software version is included in the firmware group list. In the next step after examination was successfully the TOE copies the data into the processor internal code flash and checks whether arrived without error. In the last step before the TOE is restarted the TOE calculates an HASH-value (SHA-512) over the entire area code and store it in SFLASH for subsequent integrity check.

The environment of the TOE 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.

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

Figure 3 gives an overview of the TOE demarcation.

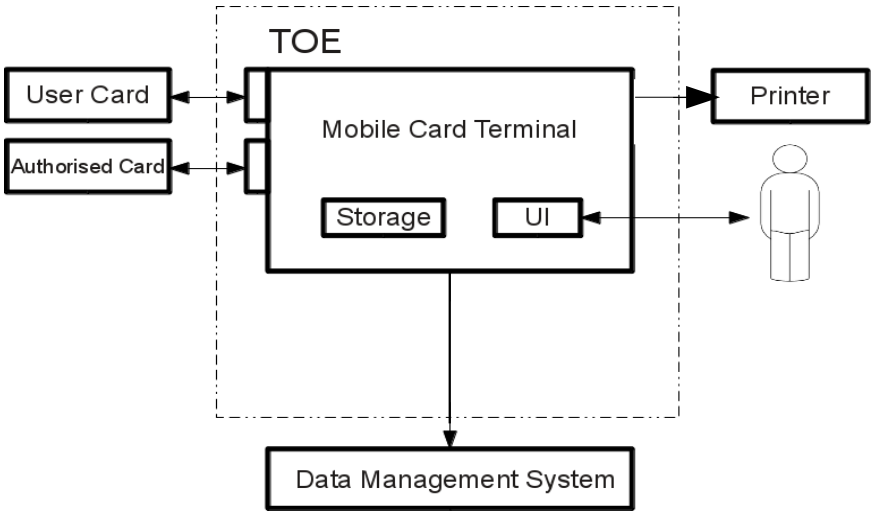

Figure 3: TOE Demarcation

1.4.1 Operational environment of the TOE

This Security Target 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).

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 of the TOE will be easily detectable by the medical supplier. In such case the device will not be used any more and needs to be replaced.

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

1.4.2 Authorised Cards

The following smart cards are authorised cards in the context of this ST:

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

Authorised Card	Description
	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

1.4.3 User Cards

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

User Card	Description
Krankenversicher-tenkarte (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

1.4.4 TOE type and Physical Scope

The TOE is a smart card terminal for mobile use and thus the physical scope of the TOE comprises:

- All hardware components, case and interfaces, which can be seen partly in the figure 1.
  - Two card slots for one authorised card and one user card.
  - A Keypad for entry of a PIN and to allow the user to start operations and navigate through menus (part UI)
  - A persistent storage (SFLASH) 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.
  - A USB connector to connect the DMS and for software updates.
  - A display for the interaction between user and TOE.

4 See also [gemSpec_MobKT]

- The update file with application and loader firmware and
- the related guidance documents
  (Note that, the TOE has different product relevant variants)
  - user guide
    - **ORGA 930 M online** has the user guide (Bedienungsanleitung mobiles smart card terminal ORGA 900 mit Firmware-Version 4.10.0. [AGD]
    - **ORGA 930 M** has the same user guide as ORGA 930 M online. This is valid for the device after successful update. After the update process with the update tool [see table 5] the download link is displayed on the user PC.
  - brief instruction
    - **ORGA 930 M online** has the brief instruction (Kurzanleitung ORGA 930 M online) [AGD_KAL]
    - **ORGA 930 M** has the same brief instruction as ORGA 930 M online. This is valid for the device after successful update. After the update process with the update sofware [see table 5] the download link is displayed on the user PC.
  - installation guide
    - **ORGA 930 M** has the installation guide for upgrade the firmware to same firmware as ORGA 930 M online with the update software (see table 5) (ORGA 930 M Firmware Upgrade) [AGD_IAN].
    - **ORGA 930 M online** has the same installation guide for update the firmware as ORGA 930 M with the update software (see table 5).
  - Upgrade files
    - **ORGA 930 M:** To upgrade the application and the loader to the same version of ORGA 930 M online with the update software (see table 5).
      - ORGA_930_M_online_FW_4.10.0.ppu

- Two seals are attached to the case of the terminal allowing the user of the TOE to detect whether the TOE has been tampered with. The description on how to check the sealing is part of the TOE guidance documentation.

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

- Smart cards (HPC, SMC-B, KVK, eHC)
- Printer
- Data Management System of a practice or hospital (DMS)
- Drivers for DMS (more details in table 5)
- Update Software and Update Driver (more details in table 5)

1.4.5 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
- Cryptographic support for encryption of persistent storage
- Integrity protection of emergency data[1]
- Residual information protection
- Self testing
- Logging access 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 are 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 ST)

1.4.6 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[1]).
- 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 Security Target the environment is assumed to completely counter the threat of physical manipulation of the TOE as such threats cannot be diminished by the TOE with reasonable efforts.

1.4.7 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).

1.4.7.1 User Data

The following user data shall be protected by the TOE and its operational environment:

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[1] 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 sends 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[1], it generates protocol data. All protocol data entries are later transmitted to the DMS alongside the data.

Table 3: User Data

1.4.7.2 TSF Data

Data	Description
Administrator credentials	The TOE stores references of the administrator credentials (e.g. a PIN) for the management interface

Data	Description
(also referred to as: PIN for the management interface, i.e. Administrator PIN, shared secret for the C&R TOE reset mechanism)	of the TOE and the shared secret for the C&R TOE reset mechanism. 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 immediately after delivery, after a succesful factory reset via the Challenge & Responce mechanism and after a succesful factory reset via Admin-PIN. 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 offers an additional TOE reset mechanisms (fallback) in case that administrator credentials are lost. The fallback authentication mechanism is described in this ST, see below. Its usage causes a reset to factory defaults. Subsequently the administrator must set a new administrator PIN. **The fallback mechanism is implemented by a challenge & response operation. On demand the TOE generates a challenge that has to be sent to the developer from the administrator. After successfully performing an organisational authentication procedure, the developer calculates the response data from the challenge and informs the administrator of the response data. This allows the administrator with the help of the developer to reset the TOE to factory defaults.**
~~**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	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.

Data	Description
(unencrypted)	
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 reset 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 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

1.4.8 External Entities

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.
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 setting • 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 provide additional management functionalities specifically for the developer: • **The challenge and response mechanism for the TOE reset to factory defaults.**
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**. DMS needs to have a Microsoft Windows Variant operating system.**
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.

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.

Entity	Description
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.
Drivers for DMS	Drivers usbser.sys from Microsoft and orgadfu.sys from the manufacturer is needed for the interaction between DMS and TOE. Driver is exclusively for the Microsoft Windows operating system.
Update Software and Driver	A special update software: • For ORGA 930 M and ORGA 930 M online ◦ ORGA_930_M_online_FW_4.10.0_Update-Tool.exe Version 2.0.0.3 and a special driver MCTDFUUpgrade.dll, CTORG32.dll, CTORG32.eni, libeay32.dll, ssleay32.dll and msvcr120.dll are needed for loading an update file into the TOE. Software and Driver is exclusively for the Microsoft Windows operating system.

Table 5: External Entities

The following subjects are active entities in the TOE:

Entity	Description
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 CC Conformance Claim

The CC version in use is Common Criteria, Version 3.1 R4 [CC_PART1], [CC_PART2] and [CC_PART3].

This Security Target 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

This Security Target claims strict conformance to the Protection Profile *Mobile Card Terminal (MobCT) for the Germany Healthcare System*, BSI-CC-PP-0052, Version 1.4 of 24 September 2014.

2.2.1 Discarded SFRs

The TOE does not implement the reset without authentication. Therefore and in conformity with application note 18 the SFRs

- FDP_IFC.1/MSI and
- FDP_IFF.1/MSI have been discarded.

2.3 Conformance Rationale

This Security Target is strictly conforming to the Protection Profile *Mobile Card Terminal (MobCT) for the Germany Healthcare System*, BSI-CC-PP-0052, Version 1.4 of 24 September 2014.

- Threats in the ST are identical to the threats in the PP.
- OSPs in the ST are identical to the OSPs in the PP except that for OSP.LOG_DATA additional information has been added to the protocol entries.
- Assumptions in the ST are identical to the Assumptions in the PP with the concretisation that the TOE is implemented without a TOE reset PIN and the connecting between TOE to the DMS is assumed by using an USB cable.
- Security Objectives in the ST are identical to the security objectives in the PP, except that O.I&A has the fallback mechanism implemented by a challenge response mechanism, no “TOE reset without authentication” is implemented, O.MANAGEMENT is completed by “Reset to factory defaults” for the administrator, which is assisted by developer. O.LOG_DATA additional information has been added to the protocol entries.
- Security Objectives for the Operational Environment in the ST are identical to the Security Objectives for the Operational Environment in the PP with the exceptions that OE.DMS the connection between the TOE and the DMS is established by using a USB cable.
- Security requirements in the ST are identical to the security requirements in the PP with the exceptions:
  - FCS_COP.1/C&R has been added to the ST
  - FDP_IFC.1/MSI and FDP_IFF.1/MSI are discarded in accordance with Application Note 18.
  - FIA_AFL.1/C&R Authentication failure handling has been added to the ST
  - FMT_MTD.1/Defaults Management of TSF data has been added to the

ST.

- FIA_SOS.1 additional mechanism to verify that secrets for the C&R-Operation has been added to the entries.
- FIA_UAU.5.1 the TSF provides additional an interface to authenticate the administrator / developer via the C & R-Operation.
- FIA_UAU.5.2 The TSF authenticate any user's claimed identity according to the additional rule for a Challenge & Response operation to perform.

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 ORGA 900 to allow the secure operation of the TOE and to protect the assets named in chapter *1.4.7*.

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

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
	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 checked 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 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). **The fallback mechanism is implemented by a challenge and 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 [gemSpec_MobKT]. The authorised card will provide the following functionality

Assumption	Description
	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 [gemSpec_Krypt]. • 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.
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 **USB cable** • 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.

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. No additional physical protection is provided by the TOE and therefore supplement [PP_MOBCT] is not 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.

Assumption	Description
	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.

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

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 Security Target.

Threat	Description
	insurance data and emergency data. The threatened assets are health insurance data and emergency data from 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 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.

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 [gemSpec_MobKT]: • the time-stamp, • 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 will 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 [gemSpec_MobKT]. • **List to check whether the card has been read and may have to be updated. The**

Policy	Description
	content of the list is AES encrypted. ◦ **Insurance ID,** ◦ **data of birth,** ◦ **first- and surname** • **List for faster sorting and searching of stored user data. The content of the list is AES encrypted.** ◦ **Card serial number,** ◦ **data of birth,** ◦ **the first letter of the first- and surname.** • **Number of stored data records for display of free memory data records slots.** • **List of current medical suppliers and their HPC (HPC-Database). This is used if the RTC time (system time) is lost and data records are available on the device, so the system time is set minimum to the last imported date records, to prevent misuse.** ◦ **HPC Card number** ◦ **Save date of the last data record**
OSP.TRANSFER	The TOE shall enable the medical supplier to transfer stored 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 [gemSpec_MobKT].
OSP.DMS_CONNECTION	The TOE will not permit to access the KVK or eHC while the TOE is connected to the DMS.
OSP.C2C	The TOE 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 could be performed by the TOE[12]. This OSP prevents that faked eHC can be used by the TOE.
OSP.TIME	The TOE is provided a reliable timestamp for the following purposes: • logging of eHC accesses,

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

Policy	Description
	• generation of protocol data, • the checking of the validity period of card certificates. The TOE will be not allowed 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 will be equipped with seals by the manufacturer. The seal protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The sealing will be compliant to BSI – TR 03120 ([TR03120]) and has been tested accordingly[13].
OSP.SELFTESTS	The TOE will be able to perform self tests to verify the correct operation of its security functionality and the integrity of the firmware. The self tests will run at least during initial start-up.
OSP.EMERGENCY_DATA[1]	The TOE will 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

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

13 The testing shall encompass an attestation that the seal fulfils the structural requirements of BSI – TR 03120 ([TR03120]) 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).

Objective	Description
	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 [gemSpec_Krypt]. 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 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

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

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
	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 provides an additional TOE reset mechanisms (fallback) called "TOE reset with authentication": • The fallback mechanism is implemented by using a challenge response mechanism: The TOE uses a challenge response mechanism for the TOE reset mechanism. It contains an unpredictable device-specific shared secret which is set by the developer before the delivery to the user. **This mechanism is used by the administrator to reset the TOE if the administrator PIN is lost.** The TOE shall lock an account after a specified number of unsuccessful authentication attempts for a specified period of time.
O.MANAGEMENT	The TOE shall provide the following management functionality to an authenticated administrator: • Firmware update • Import of Cross CVCs • Management of time

Objective	Description
	• Reset to factory defaults[16] • Management of login credentials. The TOE also provides the management functionality "Reset to factory defaults" for the administrator, which is assisted by 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 be 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.
O.LOG_CARDS	The TOE shall log accesses to eHCs on the cards itself. The following information shall be logged according to [gemSpec_MobKT]. • 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 registration number of the TOE as specified [gemSpec_MobKT].

16 When the device is reset to factory defaults, all data in the persistent storage except the firmware and the shared secret for the C&R TOE reset mechanism are securely deleted and the login credentials for the management interface are set back to initial values and require changing.

Objective	Description
	• **List to check whether the card has been read and may have to be updated. The content of the list is AES encrypted.** ◦ **Insurance ID,** ◦ **data of birth,** ◦ **first- and surname** • **List for faster sorting and searching of stored user data. The content of the list is AES encrypted.** ◦ **Card serial number,** ◦ **data of birth,** ◦ **the first letter of the first- and surname.** • **Number of stored data records for display of free memory data records slots.** • **List of current medical suppliers and their HPC (HPC-Database)** ◦ **HPC Card number** ◦ **Save date of the last data record**
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 [gemSpec_MobKT].
O.DMS_CONNECTION	The TOE shall not permit access to the KVK or eHC while the TOE is connected to the DMS.
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

Objective	Description
	the manufacturer. Body and seal protect security relevant parts of the TOE and prove the authenticity and physical integrity of the device. The body and the sealing shall be compliant to BSI – TR 03120 ([TR03120])[13].

Table 10: Security Objectives for the TOE

Application Note 1: -

Application Note 2: -

Application Note 3: -

Application Note 4: The TOE is included management interface for administrator but the TOE doesn't provide a management interface explicit for developers. For TOE reset to factory defaults by the developer the C&R mechanism is used by administrator.

Application Note 5: The TOE is implemented printer control for external printer, but it doesn't provide a management interface explicit for developers.

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. 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 wire-tapping; • they check that the sealing and the body of the TOE is undamaged every time the device is used by the medical supplier and • 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

Objective	Description
	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, • they set the new administrator PIN immediately upon performing the reset to factory defaults • the firmware is only updated to certified versions, • 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 • 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 additional TOE reset mechanisms (fallback). 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 [gemSpec_MobKT]. The authorised card shall provide the following functionality to the TOE: • Identification and authentication of medical

Objective	Description
	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 [gemSpec_Krypt]. • 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 **USB cable** • 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

Objective	Description
	visible sign of manipulation of the TOE.

Table 11: Security Objectives for the Operational Environment

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	
A.DEVELOPER																					X

Table 12: Security Objectives 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 [PP_MOBCT] 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 have 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 the PIN and credentials of the TOE reset mechanism by various means during PIN entry and processing and through its quality and OE.ADMIN describes that the administrator has to protect the 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 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.

The assumption **A.DEVELOPER** is covered by *OE.DEVELOPER* 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 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[17] 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

17 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.

[assignment: *data scheme*] and notify the user.

6 Security Requirements

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

Operations for assignment, selection, refinement and iteration have been performed.

All performed operations from the original text of [CC_PART2] are written in *italics* for assignments, underlined for selections and **bold** text for refinements. Furthermore the brackets ("[]") from [CC_PART2] are kept in the text.

Application Note 6: There are no different TOE configurations to consider with respect to SFRs. To specify which optional features (fallback reset mechanism) are used the ST author has refined the respective SFRs or introduced new SFRs (FCS_COP.1/C&R,FIA_AFL.1/C&R,FMT_MTD.1/Defaults).

Application Note 7: This ST is specified for all SFRs which contain cryptographic algorithms which algorithms / methods and which parameters (e.g. key sizes). For SFRs referring [gemSpec_Krypt] it is quoted the section of [gemSpec_Krypt] and is referred to for the selection of a cryptographic algorithm / method and its parameters.. These information are introduced by refinements and, in one case, in the form of a reference to another document, see FCS_COP.1.1/C&R and [C&RVer].

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
FCS_COP.1/C&R	**Cryptographic operation for challenge & response operation**
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/PIN	Authentication failure handling
FIA_AFL.1/C&R	**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.1/ Defaults	**Default 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 [*The generation of the symmetric key is performed using a random number generator which is provided by the authorised card. The quality of the random number is therefore at least PTG.2. The command of [gemSpec_COS] chapter 14.9.5.3 is used*] and specified cryptographic key sizes [***256 Bits***] that meet the following: [*symmetric encryption standards according* to [***[TR03116-1] chapter 3.4 PTG.2]***].
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 uses a hybrid encryption method according to [gemSpec_Krypt]. The cryptographic symmetric key, generated by FCS_CKM.1 is used for the symmetric encryption of 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 [*overwriting the key in the persistent storage (SFLASH) with 0xFF and overwriting the key in the volatile storage with 0x00*] that meets the following: [*cryptographic standards according to [gemSpec_Krypt]*].
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 [***AES-256 GCM, specified in [[gemSpec_Krypt], chapter 3.6 (GS-A_4389) and chapter 3.5.1 (GS-A_5016)]***] and cryptographic key sizes [***256 bit according to [NIST-SP-800-38D] with a tag-length of 256 Bit,***

	specified in [[gemSpec_Krypt], chapter 3.6 and 3.5.1]] that meet the following: [*cryptographic standards according to [[gemSpec_Krypt], chapter 3.6 and 3.5.1]]*
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 is used to encrypt the emergency data[1] 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 [*RSASSA-PKCS1-v1_5*] and cryptographic key sizes [*RSA-4096, SHA-512*] that meet the following: [*[[gemSpec_Krypt] chapter 3.7]* ***and [RFC8017]***].
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes] 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 are specified in the SFR above.

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 [gemSpec_Krypt]*] and cryptographic key sizes [*as specified in [gemSpec_Krypt]*] that meet the following: *[gemSpec_Krypt]*.
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 [gemSpec_Krypt] but to check the mathematical correctness of the signature.

6.1.1.6 FCS_COP.1/C&R Cryptographic operation for challenge & response operation

FCS_COP.1.1/C&R	The TSF shall perform [*generation of challenge data and response data input for a C&R operation*] in accordance with a specified cryptographic algorithm [*SHA-1,according to [C&RVer]*] and cryptographic key sizes [160 *Bits*, *according to [C&RVer]*] that meet the following: [C&RVer].
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 12:	A challenge response mechanism is used for a TOE reset mechanism. Therefore an iteration of FCS_COP.1 is added 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,* • *[challenge and response for C&R mechanism],* • *health insurance data,* • *emergency data*[1] • *firmware,* • *public key for firmware verification,* • *time settings,* • *symmetric keys (encrypted and decrypted),* • *card slot,* • *access logging data,* • *[printer control]* *Operations*: • *read,* • *modify,* • *delete,* • *[none]*]
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
Application Note 13:	The name of the kind of credential which is used for the TOE reset mechanism is "challenge and response".

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,* • *[challenge and response for C&R mechanism],* • *health insurance data,* • *emergency data*[1]*,* • *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,*
- *[printer control]*]

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* [PP_MOBCT]*. 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*
- [*none*]
- [*The TOE shall permit the authenticated administrator*

to access printer control]].

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.* • *[No subject shall read out the shared secret for a challenge response 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* • *[none]*].
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Application Note 14:	Credentials used for the TOE reset mechanism are the shared secret for a challenge and response mechanism.
Application Note 15:	The TOE doesn't provide a management interface for developers for printer control. One object (printer control) and one rule for printer control access have been additionally specified in FDP_ACF.1.2.
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 will 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* • [*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:	A "TOE reset without authentication" mechanism is not implemented so "MS information SFP" expressed in FDP_IFC.1/MSI and FDP_IFF.1/MSI are discarded. Therefore this SFR is trivially fulfilled.

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 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*[18] *including:* • *the* time of access, • *the accessed data, and* • *the identity of the authorised card which was used to access the eHC.*

18 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.

	If health insurance data or emergency data is 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,* • *[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 than the logging container.* • *Health insurance data and emergency data shall never be transferred to any card slot.* • *The TOE shall never write data to the KVK.* • *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: C2C authentication is initiated every time right before data is read from an eHC.
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. 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 will be informed by the guidance documents 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: additional information to the protocol data has been added to the protocol data.

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 [gemSpec_MobKT].* • *[no further rules]*].
FDP_IFF.1.3/DMS	The TSF shall enforce [*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:	The TOE does not use a docking station.

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**~~
Application Note:	According to Application Note 18, "TOE reset without authentication" mechanism is not implemented so "MS information SFP" expressed in FDP_IFC.1/MSI and FDP_IFF.1/MSI are discarded. Therefore the SFRs in FDP_IFF.1/MSI are trivially fulfilled.

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. Emergency data is not dealt with in OPB1 so this SFR is not regarded relevant.

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 [shared secret for the C&*R *TOE reset mechanism* and the public key for firmware signature verification*]*]
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note 24:	The data that is erased includes encrypted health insurance and emergency data[1] 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* • *[none]*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note 25:	The data that will 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: [*Auth-Tag*].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [*not use the data, inform the medical supplier, and [none]*].
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
Application Note 26:	User data attribute has been defined as "AES-GCM algorithm".
Application Note 27:	For OPB1 there is no emergency data[1] processing foreseen.
Application Note 28:	The notification of the medical supplier in case of an integrity error will 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]] is represented completely and unambiguously according to the [*scheme specified in* [gemSpec_MobKT].
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 [gemSpec_MobKT]*] 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/PIN Authentication failure handling

FIA_AFL.1.1/PIN	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/PIN	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	24 hours

Table 14: Lockout times

6.1.3.2 FIA_AFL.1/C&R Authentication failure handling

FIA_AFL.1.1/C&R	The TSF shall detect when [5] unsuccessful authentication attempts occur related to [*performing the Challenge&Response operation with the TOE with the same Challenge*].
FIA_AFL.1.2/C&R	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block any response data entry unless a new challenge has been generated by the TOE*].
Hierarchical to:	No other components.

Dependencies:	FIA_UAU.1 Timing of authentication

6.1.3.3 FIA_SOS.1 Verification of secret

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 digits* • *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* • ***The values of the challenge and the response data shall have a length of at least 8 digits and fulfil the requirements for the PIN for the management interface*]**.
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Application Note 29:	The TOE implements no user ID for the management interface, so the rule within the selection has been discarded.
Application Note 30:	PIN for the management interface is the administrator PIN. They are also named as "login credentials", "administrator credentials" and "administrator login credentials". Same rules apply for the response data for the challenge and response mechanism to be used by administrator with help of the developer for TOE reset to factory defaults.
Application Note 31:	Previous PP versions contained a bullet point "Shall not be displayed as clear text during entry". It has been removed in the PP and this security target because of its redundancy to FIA_UAU.7.1 which describes that PINs have to displayed as asterisks during entry.

6.1.3.4 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* • *[printer control]*] 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:	"TOE reset without authentication" mechanism is not implemented and it is therefore not added that a reset to factory defaults is allowed before identification and authentication.

6.1.3.5 FIA_UAU.5 Multiple authentication mechanisms

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* • ***an interface for authentication of the administrator / developer by performing a Challenge & Response operation with the TOE***] 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.* • ***The TOE provides for an interface to perform a Challenge & Response operation with the administrator / developer for authentication and accepts input of a matching response value to the TOE generated challenge value as the authentication to perform a factory reset.***]
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.3.6 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).

6.1.3.7 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* • *[printer control]*] 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:	No functionality is added to the TOE which is restricted to the medical supplier and only available after authentication. No functionality is added to the TOE for other users.
Application Note 35:	"TOE reset without authentication" mechanism is not implemented and therefore the ST author didn't add that a reset to factory defaults is allowed before identification and authentication.

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*]**]][19] 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

19 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.

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.
Hierarchical to:	No other components.
Dependencies:	MT_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* • *[printer control]*] to [*the administrator and [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.1 Defaults Default Management of TSF data

FMT_MTD.1.1/Defaults	The TSF shall restrict the ability to [*reset*] the [• TOE to factory defaults] to [*administrator and developer*].
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles

	FMT_SMF.1 Specification of Management Functions

6.1.4.5 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.

6.1.4.6 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 default* • *Management of administrator login credentials* • *[printer control]*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles [*administrator, medical supplier*, *and [developer]]*.
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:	The developer role is added because the developer calculates the response data and sends it back to the TOE administrator so that the TOE can be reset to the factory settings using 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 authorized card will 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[20] 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[21]** whether physical tampering with

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

21 The phrase "during operation of the TOE" is meant to specify that the user can determine

	the TSF's devices or TSF's elements has occurred.
Hierarchical to:	No other components.
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 ([TR03120])[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 [*restart, and start manually via management*]] 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 [*[public key for firmware signature check and the integrity of the shared secret for the C&R TOE reset mechanism]*, TSF data].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [*[stored TSF executable code]*, TSF].
Hierarchical to:	No other components
Dependencies:	No dependencies
Application Note 42:	Test functionality for all important aspects of all security functions that the TOE provides is described.

6.2 Security Assurance Requirements

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

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: Security 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**.

whether physical tampering has occurred without switching off the TOE.

The complete text for the requirements can be found in [CC_PART3].

6.3 Security Requirements Rationale time

6.3.1 Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage. Bold text indicates requirements which are not present in the [PP_EHCT].

	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										
FCS_COP.1/C&R						**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/PIN						X								
FIA_AFL.1/C&R						**X**								
FIA_SOS.1						X								
FIA_UAU.1						X	X							
FIA_UAU.5	X					X								
FIA_UAU.7	X					X								

	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
FIA_UID.1						X	X							
FMT_MSA.1						X								
FMT_MSA.3						X	X							
FMT_MTD.1							X							
FMT_MTD.1/ Defaults							**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: Security Functional Requirements Rationale

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 and 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 and FDP_IFF.1 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 SFRs FCS_COP.1/C&R, FDP_ACC.1, FDP_ACF.1, ~~**FDP_IFC.1/MSI, FDP_IFC.1/MSI,**~~ FIA_AFL.1/PIN, FIA_AFL.1/C&R, 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. FCS_COP.1/C&R define that the TOE implements an additional TOE reset mechanism. FDP_ACC.1 defines the access control policy for the TOE. FDP_ACF.1 defines the rules for the policy which prevents the PIN and the shared secret for the C&R TOE reset mechanism from being read. FIA_AFL.1/PIN defines the authentication failure handling for the management interface. FIA_AFL.1/C&R defines the authentication failure for the Challenge & Response operation. 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_MTD.1/Defaults, 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. FMT_MTD.1/Defaults defines that ability to reset to factory defaults is limited to the administrator and the developer. ~~**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, 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 require 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

Bold text indicates requirements which are not present in the [PP_MOBCT].

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	Fulfilled by the use of FCS_CKM.1, FCS_CKM.4

SFR	Dependencies	Support of the dependencies
	generation] FCS_CKM.4 Cryptographic key destruction	
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.
FCS_COP.1/C&R	**[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**
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
~~**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**~~	~~**Fulfilled by**~~

SFR	Dependencies	Support of the dependencies
	~~**flow control FMT_MSA.3 Static attribute initialisation**~~	~~**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/PIN	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_AFL.1/C&R	**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] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by the use of FDP_ACC.1, 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.1/ Defaults	**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	-

SFR	Dependencies	Support of the 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: Dependency Rationale

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 dependencies [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] of FCS_COP.1/C&R are not considered as no data is to be imported and no cryptographic key has to be generated. FCS_CKM.4 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 Security Target shall provide the same amount of trust as the Protection Profile for eHealth card terminals [PP_EHCT] 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.

7 TOE Summary Specification

The following sections describe the general technical mechanisms implemented by the TOE to meet all the requirement of the SFRs.

7.1 TOE Security Functionality

7.1.1 SF_1: Secure Identification & Authentication

The TOE provides several authentication mechanisms for the roles administrator, medical supplier and developer and associates users with roles. Each user has to be successfully identified and authenticated before being allowed to perform any TSF-mediated action.

- For authentication to the management interface the TOE uses a PIN-based authentication mechanism.
- For authentication of the administrator, the administrator can execute the Challenge & Response mechanism in case the Admin-PIN is lost.
- For authentication of the medical supplier to the authorised card the TOE uses a PIN-based authentication mechanism and the result of this authentication is accepted for the authentication of the medical supplier to the TOE.

The TOE will 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.

On consecutively unsuccessful authentication attempts the TOE will lock the authentication mechanism for a period of time, specified in chapter 6.1.3.1 Table 14.

On delivery and after reset to factory defaults the validity of the administrator PIN (management interface PIN) is set to "*not valid*". When the validity of the administrator PIN is set to *not valid* the administrator is forced by the TOE to set the administrator PIN before any other action can be performed by the TOE. After setting the administrator PIN the validity is set to *valid*. To perform any of the functions listed above the TOE must first be unlocked by entering a PIN that:

- is 8 digit long
- composed of at least the following characters: "0"-"9"
- cannot be saved on programmable function keys
- cannot be displayed as clear text during entry (secure PIN-Entry-Mode)

The PIN is entered in a secure PIN-Entry-Mode via the TOE-keypad and finished by pressing the TOE's <OK>–Button. The secure PIN-entry mode is only able to be activated by the TOE and is indicated by a padlock symbol for every PIN digit that has to be given. For every entered PIN digit the padlock symbol will be replaced by an asterisk symbol. PINs and PIN digits will never be displayed in clear text and no subject can read out the administrator PIN. PINs will not leave the TOE, except towards an inserted HPC/SMC-B for verification purposes.
The TOE provides an additional TOE reset mechanisms (fallback).The ability to reset to factory defaults is limited to the administrator and the developer. This mechanism is used only by the administrator, which is assisted by the developer to reset the TOE when the Admin-PIN is lost. The fallback mechanisms is implemented by using challenge and response mechanism. It contains unpredictable device-specific shared secret which is set by the developer before the delivery to the user. The values of the challenge and the response data have a length of 8 digits. After 5 unsuccessful response entries for a challenge the TOE will block further response data entries unless a new

challenge has been generated.

7.1.2 SF_2 Secure Residual

The TOE terminates an authenticated session and thereby delete all unencrypted sensitive information from the memory after:

- inactivity
  - 15 minutes of administrator,
  - [1 – 60 minutes] of medical supplier
- power loss,
- the administrator or medical supplier forces to drop the state manually (by logging of)
- the authorised card has been pulled from its card slot or otherwise loses its authentication state .

On dropping of the authenticated state, power loss and deallocation of the resource from 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.

The TOE will ensure that any previous information content of a resource is made unavailable. The deallocated memory areas will then be overwritten with 0xFF and made available again for normal use.

7.1.3 SF_3 Secure Self-Tests

The TOE performs self-tests at initial start-up and are able to be started manually via management. The self-tests check the TOE's functionality by evaluating the integrity of the stored data. This includes the integrity of the firmware in processor flash (loader and application) and integrity of TSF SFLASH-Page with configuration data (serial number, admin PIN, public key for TSF-firmware signature check, shared secret for the C&R TOE reset mechanism and other general configurations). These two integrities have a separate target HASH-value (SHA-512). The self-tests are realized by known-answer tests. These tests generate a HASH-value (SHA-512) that will be created over the storage data and check this with known integrity HASH-VALUE (answer) of the storage data. Authorised user can verify the integrity of the TSF firmware and TSF SFLASH-Page.

The TOE monitors the integrity of user data stored in the persistent storage of the TOE based on the AES-GCM algorithm. The self-tests includes an "AES-GCM test". In case an integrity error has been detected the TOE shows a message on its display and does not use the data.

7.1.4 SF_4 Secure Data Protection

The TOE encrypts health insurance data stored in the persistent storage of the TOE with the cryptographic algorithm AES-GCM and cryptographic key size of

256 bits and with a symmetric cryptographic key.

The generation of the symmetric cryptographic key is initiated and performed by the authorised card of the user.

The symmetric cryptographic key for encryption / decryption of health insurance data is asymmetrically encrypted using the functionality of the authorised card of the user and stored in the TOE.

Access to health insurance data from the storage is allowed if the data were decrypted with the help of the same authorised card which was used to encrypt the data.

The TOE will verify the integrity and the correct visualisation of the emergency data by verifying the digital signature of the emergency data and that provides secure storage and secure visualisation of the emergency data. In case an integrity error has been detected the TOE shows a message on its display and does not use the data.

The user data is additionally checked via:

- the first read byte contains a value, which is specified in SPEC (Chapter 7.5).
- includes all mandatory fields
- validity of the user card ends

7.1.5 SF_5 Secure Management

The TOE grants access to the management functions i.e.

- installing firmware,
- import of cross CVCs
- management of time settings,
- resetting to factory defaults and
- management of the administrator login credentials
- printer control

to the administrator who has to authenticate himself by PIN-entry or for the latter perform a successful Challenge & Response operation with the TOE.

In addition the TOE provides the management functionality "Reset to factory defaults" and "reset to factory default by using C&R TOE reset mechanism".

- On **reset to factory defaults** the TOE deallocates all information in the memory (except the installed firmware, the shared secret for the C&R TOE reset mechanism and the public key for firmware signature verification) and erase encrypted health insurance in the persistent storage, as well as temporary user data e.g. an unencrypted symmetric encryption key and user settings from the persistent storage. The deallocated memory areas will then overwritten with reset values and made available again for normal use. In the persistent storage (SFLASH) the reset value is 0xFF and volatile storage (RAM) the reset value is 0x00.
- On **reset to factory defaults by using a Challenge & Response TOE reset mechanism** the TOE will thereby losing all TSF data except the installed firmware the shared secret for the C&R TOE reset mechanism and the public key for firmware signature verification. On

demand the TOE generates and displays a challenge using a secret shared with the manufacturer using SHA-1 to generate a 160 bits hash value. This challenge has to be sent to the developer who in turn calculates the response data and informs the administrator about the response data. The TOE accepts input of a matching response value to the TOE generated challenge value as the authentication to perform a factory reset. The TOE offers no interface to read out or display the shared secret of the TOE. This mechanism is used only by the administrator, which is assisted by the developer to reset the TOE when the Admin-PIN is lost.

- The TOE shall permit the authenticated administrator to modify the date only if no data records are stored in the persistent storage of the TOE. The TOE accepts values that are formatted:

Name	Format	Description
Time	HH:MM:SS	Hour:Minute:Second
Date	dd.mm.jjjj	Day:Month:Year

If the RTC clock loses the date and time and data records are saved, the date is taken from the last saved data record of the current medical supplier list (See SF_6). The TOE continues to be usable with the data and prevents misuse.

Session time-out values for the medical supplier session accepted by the TOE are times between 1 minute and 60 minutes. The TOE will provide management for **import of cross CVCs**, which are used for the card to card authentication between cards of difference roots, **login credentials** and **printer control.**

The configurations of chapter 1.2 and 1.4 can be read out in the management menu to identify the TOE.

7.1.6 SF_6 Secure Card_Communication

When an authorised card is put into one of the TOE's slots, the TOE will read out the card's X.509 certificate and check

- whether the card claims to be an authorised card,
- whether the X.509 certificate of this authorised card is mathematically correct and
- whether the current date is given by the TOE falls within the validity period of the certificate before permitting any other interaction with a card.

The Card holder PIN entered via the PIN pad is only sent to the card slot where the authorised card is plugged in. No PIN is sent to the card slot where the eHC is plugged in.

When protected health insurance data is read from the eHC the TOE writes an access log entry to the logging container of the eHC including:

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

When health insurance data read from the eHC is stored by the TOE the TOE

generates a protocol data entry and attach it to the health insurance data. The protocol data includes:

- the time of access,
- terminal approval number.

The TOE ensures that

- it never writes data to containers of the eHC other than the logging container
- it never writes data to the KVK;
- health insurance data never is transferred to any card slot;
- it never includes patient specific data within or by its protocol data.

The TOE will never let anybody read out or modify the card holder PIN or symmetric keys while they are temporarily stored in the volatile memory of the TOE.

The time is used for a reliable timestamp for the following purposes:

- logging of eHC accesses,
- generation of protocol data,
- checking of the validity period of card certificates.

The TOE provides reliable time stamp with a clock precision better than ±100ppm (which corresponds to an aberration of 52.3 minutes in a year).

Additionally two AES encrypted lists are implemented in the TOE. One list checks whether the card has been read and may have to be updated. The list is AES encrypted and has the following attributes:

- Insurance ID,
- data of birth,
- first- and surname

The other list is for faster sorting and searching of stored user data. The list is AES encrypted and has the following information:

- Card serial number,
- data of birth,
- the first letter of the first- and surname.

The TOE shows on the display the number of stored data records and the free space for data records in the TOE.

List of current medical suppliers and their HPC (HPC-Database). The entry is created when a medical supplier has saved a data record on the TOE.

- HPC Card number
- Save date of the last data record

7.1.7 SF_7 Secure DMS_Communication

The TOE enables the medical supplier to transfer data records from the persistent storage to the DMS only. The transmission takes place via error detection code (EDC), which is specified in [gemSpec_MobKT]. After the data record has been transferred to the DMS successfully it is been deleted from the devices. Therefore the DMS sends usually a command "read successful" to the TOE. The next data record is only been able to be read after this command.

The connection between the TOE and the DMS is established by using a USB-cable.

While the TOE is connected to the DMS no subject is allowed to access a card slot containing an eHC or KVK.

7.1.8 SF_8 Secure Firmware-Update

On **firmware update** the TOE can be securely updated with new firmware. The secure update guarantees that only authentic firmware electronically signed by the manufacturer will be accepted by the TOE and installed on the TOE.

For signature verification purposes the TOE firmware contains the public cryptographic key and the TOE performs a signature verification for firmware updates with cryptographic algorithms SHA and RSA and cryptographic key sizes of: SHA-512 and RSA-4096 that meet [gemSpec_Krypt].

The public key is part of the firmware and the TOE allows no subject to modify the public key for the signature verification for firmware updates. The TOE offers no functionality to modify the public key for the signature verification for firmware updates.

A firmware update file 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 are versioned independently.

An update of the firmware core is only enabled if the core version is included in the firmware list. Firmware list only contain version numbers of firmware cores which are certified accordingly [PP_MOBCT].

In case of downgrades of the firmware core the TOE warns the administrator before the installation that a downgrade is about to be performed, not an upgrade. The TOE offers the chance to cancel the installation.

Firmware list and core can be updated independently. In case of a common update the TOE installs 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 is only allowed after the integrity and authenticity of the firmware has been verified using the mechanism as described in FCS_COP.1/FW.

Installing of firmware cores and lists is only allowed after the integrity and authenticity of the firmware has been verified using the mechanism as described in FCS_COP.1/FW.

The TOE permits 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.

7.2 Security Measures

7.2.1 SM_1 Security Seals

The TOE's integrity is protected against unauthorised and unnoticed attempts to tamper with the TOE by security seals.

- The seals used are forgery proof and tamper proof and are compliant to BSI - TL 03400 and BSI - TL 03415.
- The seals are applied over the gap of the two halves of the casing and over a mounting screw.

8 Glossary and Acronyms

AES
: Advanced Encryption Standard

Auth-Tag
: Output of the GCM Encryption and Decryption

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)

CA
: Certification Authority

CC
: Common Criteria

CT
: Card Terminal

DF
: Dedicated File

DMS
: Data Management System for a practice or hospital

EAL
: Evaluation Assurance Level

EDC
: Error Detection Code

eGK
: elektronische Gesundheitskarte

eHC
: electronic Health Card

HPC
: Health Professional Card

ID
: Identity

KVK
: Krankenversichertenkarte

LAN
: Local Area Network

LED
: Light Emitting Diode

MobCT
: Mobile Card Terminal for the German Healthcare System

MS
: Medical Supplier

PIN
: Personal Identification Number

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 Functionality
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus

9 Literature

[CC_PART1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model;, Version 3.1 Revision 5, April 2017
[CC_PART2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017
[CC_PART3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017
[PP_EHCT]	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032, in its current version
[PP_MOBCT]	Mobile Card Terminal for the German Healthcare System: Additional security functionality for physical protection; supplement to BSI-CC-PP-0052, in its current version,.
[TR03116-1]	Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung, Version 3.19, Dezember 03.2015
[TR03120]	BSI – TR 03120 Sichere Kartenterminalidentität (Betriebskonzept), Version 1.1
[gemSpec_MobKT]	gematik: Spezifikation Mobiles Kartenterminal (inkl. Mini-AK und Mini-PS), 2.15.0, 24.02.2022
[gemZul_Prod_mobKT]	Zulassung Produkte der Telematikinfrastruktur hier: Mobiles Kartenterminal (mobKT) (Ausbaustufe 2), Version 2.4.0, 09.04.2020
[gemSpec_COS]	Spezifikation des Card Operating System (COS)Elektrische Schnittstelle, Version 3.13.1
[gemSpec_Krypt]	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.21.0
[RFC8017]	RSA Cryptography Standard, Version 2.2,October 27.2012
[C&RVer]	Verfahren zum Ruecksetzen des Admin PINs im ORGA900 und ORGA 6000, Version 0.5.
[AGD]	Bedienungsanleitung mobiles smart card terminal ORGA 900 mit Firmware-Version 4.10.0, Version 23.12.1
[AGD_KAL]	Kurzanleitung ORGA 930 M online, Version 23.12.1
[AGD_IAN]	Installationsanleitung: Firmware-Update des mobilen Gesundheitskartenterminals ORGA 930 M online, Version 22.11.1