Common-Criteria-Dokument zur CC-Zertifizierung als Mobiles Kartenterminal nach EAL3+ *CARD STAR* /memo3 - Security Target (Sicherheitsvorgaben) Version 3.00, Stand 25.01.2018

Projekt	**Name:**	**CARD STAR /memo3**
Zertifizierung	**BSI-ID:**	BSI-DSZ-CC-0689-V2
Dokument	**Name:**	CSo3_ST
	Version:	3.00
	Status:	Final
	Datum:	25.01.2018
	Ersteller:	Tomas Müller

Änderungshistorie

Datum	Version	Beschreibung	Autor
11.12.2009	0.1	Ersterstellung	Dr. Klaus Leistner
14.12.2009	0.2	Überarbeitung aktive Gehäusesicherung, Versiegelung	Boris Leidner
15.01.2010	0.3	Überarbeitung, Konzeptionelle Änderungen:5 neue SFR, Security Functions, Übernahme der Originaltexte aus dem Protection Profile	Boris Leidner
07.04.2011	1.0	Umstellung auf Version Q1.02G und Firmware der Dockingstation	Dr. Klaus Leistner
18.05.2011	1.03	Umstellung auf Version Q1.03G	Dr. Klaus Leistner
27.08.2014	2.10	Überarbeitung nach Review-Protokoll V1.0 (BSI) und Adaption auf Basis Protection Profile Version 1.3	Dr. Klaus Leistner
06.01.2015	2.12	Kleine Änderungen bzgl. Protection Profile Version 1.4	Dr. Klaus Leistner
08.03.2016	2.16	Zusätzliche Hardwareversion B00 hinzu gefügt.	Tomas Müller
15.06.2016	2.19	Entfernung der Ausweitung des PP	Tomas Müller
11.08.2016	2.20	Dockingstation und Docking-Betrieb von den Zertifizierten Bestandteilen ausgeschlossen.	Tomas Müller
27.07.2017	2.22	Berücksichtigung Lieferkette in Kapitel 1.3	Tomas Müller
25.01.2018	3.00	Finalisierung und Anpassung der Versionsbezeichnung	Tomas Müller

Inhaltsverzeichnis

1 ST-Einführung „ASE_INT“

1.1 ST Identifikation

Titel der Sicherheitsvorgaben:	CARD STAR /memo3 - Security Target (Sicherheitsvorgaben)
Version:	3.00
Datum:	25.01.2018
Herausgeber:	CCV GmbH, Celectronic eHealth Division
In Übereinstimmung mit:	Common Criteria Protection Profile “MobileCard Terminal for the German Healthcare System (MobCT)” / BSI-CC-PP-0052, Version 1.4 vom 24. September 2014
Datei Name:	CSo3_ST
Autoren:	Dr. Klaus Leistner
CC Version	3.1, Release 4
Assurance Level:	**EAL 3** ergänzt durch **ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1** und **AVA_VAN.5**
Zertifizierungskennung:	BSI-DSZ-CC-0689-V2

1.2 EVG Identifikation

Name:	***CARD STAR* /memo3**
Hardwareversionen:	B00, B01
Firmwareversion:	4.0.6
Hersteller:	CCV Deutschland GmbH, Celectronic eHealth Division
Produkttyp:	Mobiles Kartenterminal für den Einsatz im Gesundheitswesen

1.3 EVG Übersicht

Gegenstand der Evaluation (EVG) ist das *CARD STAR* /memo3 des Herstellers CCV Deutschland GmbH, Celectronic eHealth Division.

Abbildung 1:*CARD STAR* /memo3

Der Evaluationsgegenstand (EVG) wird nur in einer Bauform hergestellt und geliefert.

Das CARD STAR /memo3 besitzt zwei Kartensteckplätze, Bedienelemente, externe Schnittstellen und eine eigene Stromversorgung, sowie ein Prozessorsystem zur Steuerung aller Komponenten und Verarbeitung der Daten. Die Funktionen des Prozessorsystems und der Peripherie werden über die Firmware 4.0.6 realisiert.

Die Verbindung zum steuernden Gerät (DMS) erfolgt direkt über eine der externen Schnittstellen (seriell oder USB).

Die Hardwareversion des CARD STAR /memo3 ist in Form der Artikelnummer im Batteriefach des EVG für den Verwender ersichtlich angegeben. Das Terminal wurde in den Versionen B00 und B01 ausgeliefert[1]. Die Firmwareversion kann über eine Info-Funktion auf der Anzeige angezeigt werden.

Im Lieferumfang des EVG sind enthalten: Terminal, Batterien, USB-Kabel und Bedienungsanleitung (enthält spezifische Anweisungen für Administratoren und Benutzer).

Der EVG wird ausschließlich vom Hersteller an einen Leistungserbringer oder die von Ihm benannte Person ausgeliefert, auch wenn die Bestellung über einen Zwischenhändler erfolgt.
Eine Lieferung durch Zwischenhändler ist nicht vorgesehen.

[1] Hardwareversionen nur unterschiedlich bezüglich der Dimensionierung einiger Bauelemente. Die Änderungen erfolgten aufgrund von ESD Problemen..

1.4 Überblick über die Sicherheitsbeschreibung des ST

1.4.0 Einführung

Diese Sicherheitsvorgaben definieren Sicherheitsziele und -anforderungen für das mobile Gesundheitskartenterminal, Produkt „CARD STAR /memo3“ basierend auf dem zugehörigen Schutzprofil und den Regelungen für das deutsche Gesundheitssystem.

Die Anforderungen sind auf die Sicherheitsdienste des EVG bezogen, besonders auf:

- den Zugriff auf die zwei Slots für Smartcards,
- die Verschlüsselung der persistent gespeicherten Daten,
- die Funktionalität der sicheren Eingabe der PINs,
- die Benutzerauthentifikation vor Verwendung gespeicherter Datensätze,
- die Verwaltung der gespeicherten Datensätze
- die sichere Verbindung zum Primärsystem (Data Management System),
- die Aktualisierung der Firmware,
- die Resistenz gegen physikalische Angriffe.

Hinweis zur Darstellung: Dieses Security Target enthält Textpassagen, die aus dem Protection Profile BSI-CC-PP-0052 [PP_MobCT] unverändert übernommen oder mit Anpassung zitiert worden sind. Diese Übernahmen und Zitate sind in englischer Sprache belassen und zur Kenntlichmachung in einer kleineren Schriftgröße dargestellt.

1.4.1 Beschreibung des EVG

Der EVG wird in seinen wesentlichen Funktionen im Abschnitt 1.2.1 des Protection Profile [PP_MobCT] beschrieben:

The Mobile Card Terminal (MobCT) is a smart card terminal for the German healthcare system. It is used by medical suppliers during visits to read out health insurance data and emergency data[2] from a *user card*[3] of a health insured person. The data may further be viewed on a display or printed by the medical supplier.
For accessing protected data on a user card the medical supplier needs an *authorised card*[4] and a corresponding PIN to unlock the authorised card (*card holder PIN*). The PIN is acquired by the TOE and then relayed to the authorised card. Once the authorised card is unlocked, the medical supplier can plug in a user card. The authorised card then unlocks the user card via card-to-card (C2C) authentication. Afterwards, the TOE is able to read data from the user card. Unprotected data on the user card can be read without the unlock process.
The TOE provides functionality to store the data records in its own persistent storage after the data has been read from a user card. All data records are encrypted using symmetric AES encryption while residing in the storage. The symmetric encryption key is generated by the TOE using the random number generator of the authorised card. The key is also encrypted while in the storage of the TOE. For the encryption and decryption of the symmetric key, the 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.

---

[2] 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.

[3] See chapter 1.4.4 for a description of user cards.

[4] See chapter 1.4.3 for a description of authorised cards.

The medical supplier is able to transfer the stored data to a Data Management System for a practice or hospital (DMS) for accounting. After a data record has been transferred, the TOE deletes the record from the storage. Data records can also be deleted manually by the medical supplier.
The body of the MobCT will be sealed. The sealing has to be compliant to the requirements of BSI – TR 03120.
The next figure (Abbildung 2) gives an overview of the TOE components.

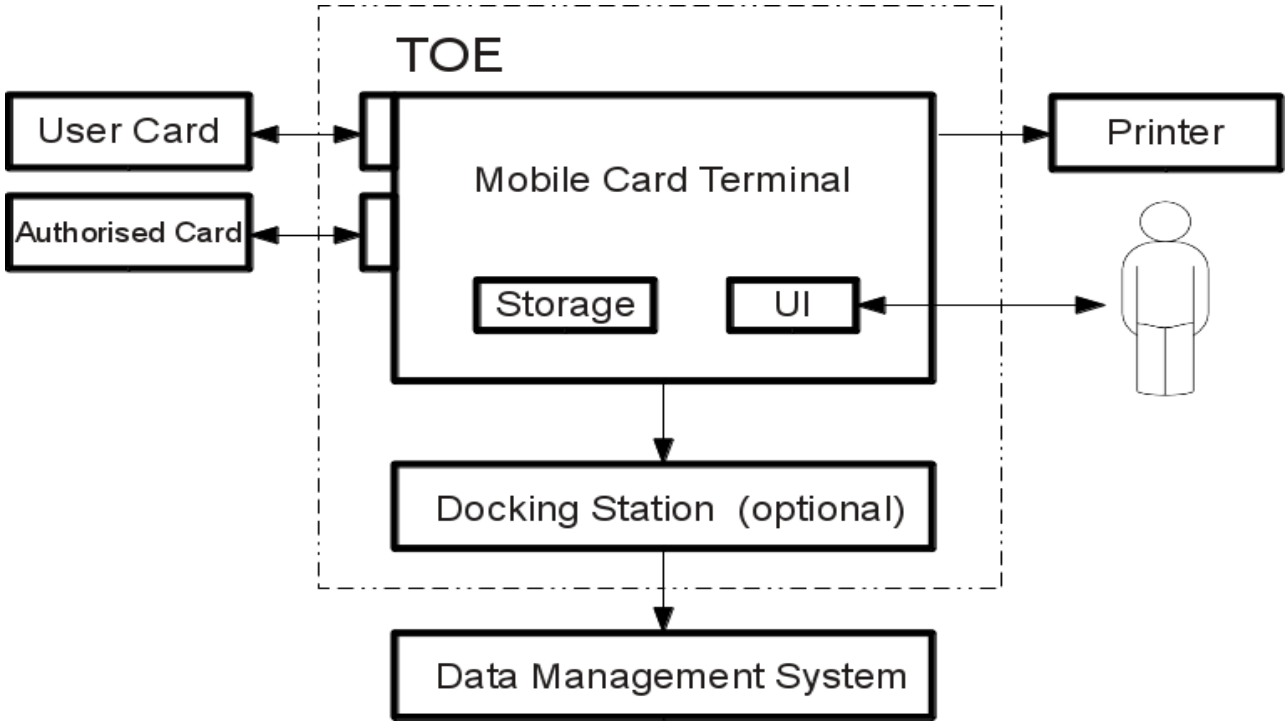

Abbildung 2: TOE demarcation[5]

1.4.1.1 Umsetzung TOE Reset Mechanismus

Der EVG bietet dem TOE Administrator die Möglichkeit eine TOE Reset PIN zu setzen. Die TOE Reset PIN ist eine 8 – 16 stellige numerische PIN, die in dem EVG gespeichert wird und von dem Administrator aufzuschreiben und sicher zu verwahren ist. Die TOE Reset PIN wird verwendet, wenn der TOE Administrator die TOE Administrator PIN vergessen hat und der EVG auf factory defaults zurück gesetzt werden soll.

1.4.1.2 Umsetzungsstatus Notfalldaten

Die Applikation „Notfalldaten“ bzw. „emergency data“ ist nicht spezifiziert [MobKT] und nicht umgesetzt. Das entspricht dem Schutzprofil [PP_MobCT] in Abschnitt 1.2.1, Fußnote 1.
Ebenso wie in [PP_MobCT] sind die Anforderungen und weiteren Belange in diesem Dokument aufgeführt, jedoch aufgrund der fehlenden Umsetzung gegenstandslos.

[5] Das TOE bietet keine Printer-Unterstützung. Zusätzlich ist die optionale Dockingstation zwar vorhanden, jedoch nicht Bestandteil der Zertifizierung.

1.4.1.3 Physikalischer Schutz

Der EVG besitzt an mehreren Positionen Sensoren, die ein Eindringen in das Gehäuseinnere registrieren.
Sobald ein Sensor anspricht, wird dies in einer Hardwareschaltung dauerhaft gespeichert. Hierzu wird keine externe Stromversorgung benötigt. In diesem Fall nimmt nach dem Einschalten der EVG den Alarmzustand an, auch wenn die eigentliche Ursache nicht mehr besteht. In diesem Status ist das Gerät dauerhaft blockiert und der Alarmzustand wird auf dem Display angezeigt.
Eine erneute Inbetriebnahme kann nur durch den Hersteller erfolgen. Die erneute Inbetriebnahme darf erst nach eingehender Überprüfung aller Komponenten des Gerätes durch den Hersteller erfolgen.

Hinweis: Diese Funktionalität ist von keinem SFR gefordert und damit nicht Gegenstand der Evaluierung.

1.4.1.4 Anzeige der EVG-Identität

Für einen neu eingelegten HBA wird eine signifikante ID erzeugt und angezeigt, mit der der Benutzer später sein Gerät identifizieren kann. Diese Konfiguration ist erforderlich, bevor die Eingabe der Karten-PIN möglich ist. Ein heimliches Austauschen des Geräts gegen ein manipuliertes Exemplar ist somit nicht möglich.
Für den Administrator gibt es ein ähnliches Verfahren. Diese Identität wird bei Definition einer Administrator-PIN erzeugt und angezeigt. Beim Übergang zu einer Administratorsitzung wird diese Identität angezeigt.
Die Anzeige der Identität nutzt eine kryptographische Funktion.

Hinweis: Diese Funktionalität ist von keinem SFR gefordert und damit nicht Gegenstand der Evaluierung.

1.4.1.5 Nutzung der optionalen Dockingstation

Die Verbindung zum steuernden Gerät (DMS) erfolgt direkt über eine der externen Schnittstellen (seriell oder USB).
Alternativ wird eine Dockingfunktion angeboten:
Das stationäre Kartenlesegerät CARD STAR /medic2 kann als Dockingstation für den EVG dienen. Im angedockten Zustand geht es in die spezifische Dockingbetriebsart, dann können die Daten des EVG ausgelesen werden, um sie an das DMS zu senden.

Hinweis: Die optionale Dockingstation ist nicht Bestandteil der Zertifizierung. Die Nutzung der Dockingstation zu übertragen der Daten an das DMS erfolgt auf eigene Verantwortung des Benutzers. Ein entsprechender Hinweis ist auch in der Bedienungsanleitung enthalten.

1.4.2 Einsatzumgebung

Die Anforderungen an die Einsatzumgebung werden im Abschnitt 1.2.2 von [PP_MobCT] definiert:

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.

The TOE will be locked in a secure area whenever it is not used. The secure area is only accessible for the medical supplier and persons authorised by them. Intrusion to the secure area for the TOE will be easily detectable by the medical supplier. In such a case the device will not be used anymore and will have to be replaced.

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

1.4.3 Authorised card

The following smartcards 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 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.

Tabelle 1: Authorised Cards

1.4.4 User cards

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

User card	Description
Krankenversichertenkarte (KVK)	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[6] 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.

Tabelle 2: User Cards

1.4.5 Physische Ausprägung

Die im Abschnitt 1.2.5 des Schutzprofils [PP_MobCT] gelisteten Anforderungen an die Geräteausstattung ist wie folgt zu präzisieren:

The TOE comprises the following physical components (exclusive parts of the optional docking station):

- Two card slots for one authorised card (inside) and one user card (slot at the top side)
- A PIN pad for entry of a PIN (part of UI)
- One display for user interaction during the PIN entry, for showing emergency data[7], and for management of the TOE (part of UI)
- Keyboard to allow the user to start operations and navigate through menus (part of UI)
- A persistent storage to store data records
- A body which integrates all the other components and is physically protected by sealing, so that the medical supplier can detect if the device has been tampered with.
- Optionally[8]: a docking station for data transfer to the DMS.

[6] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

[7] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

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

- Smartcards (HPC, SMC-B, KVK, eHC)
- Printer[9]
- Data Management System of a practice or hospital (DMS)
- Update-Tool (Firmware-Updates and Cross CVCs)
- External display that is used to display emergency data (not included in the TOE – therefore not applicable with CARD STAR /memo3)

1.4.6 Logische Ausprägung

Im Abschnitt 1.2.6 des Schutzprofils [PP_MobCT] ist der EVG durch seine Sicherheitsfunktionalität logisch abgegrenzt:

The logical scope of the TOE can be defined by its security functionality[7]:

- Access control for stored health insurance data and emergency data
- 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
- Residual information protection
- Self testing
- Logging accesses to the eHC (not KVK)
- Protocol generation for stored data records
- Restricting transfer of data records to DMS
- Identification and authentication for administrators
- Management functionality including a secure firmware update

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

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

1.4.7 Physikalische Schutzmechanismen

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

- The TOE is stolen and manipulated or simply replaced by an attacker. This would allow an attacker to foist a “hostile” device upon the medical supplier which in turn could compromise all assets from this point on (e.g. card holder PIN, health insurance data, emergency data).
- The card holder PIN is transferred in clear text to the card slot of the HPC but the card slot is a point of the TOE which can not completely be 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 can not be diminished by the TOE with reasonable efforts.

---

[8] Die Dockingstation ist verfügbar, jedoch nicht Bestandteil des TOE und der Zertifizierung. Die Benutzung der Dockingstation ist optional und erfolgt auf eigene Verantwortung des Benutzers, da auch eine direkte Verbindung mit dem DMS möglich ist. Ein entsprechender Hinweis ist auch in der Bedienungsanleitung enthalten.

[9] Der TOE bietet keine Printer-Unterstützung.

1.4.8 Assets

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

1.4.8.1 User data

Data	Description
Card holder PIN	The TOE acquires a PIN from the medical supplier and passes it to the authorised card in one of the card slots. The card holder PIN shall be held confidential.
Data records	The term “data records” refers to health insurance data as well as emergency data[10] 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[11]	The TOE reads out protected emergency data from the eHC, encrypts and stores it, displays it, and transfers it to the DMS. Emergency data is equipped with a cryptographic signature and a public key of the authorised card that created the signature. Stored emergency data shall be held confidential and protected against modification.
Firmware updates	The administrator is able to perform firmware updates for the TOE. New firmware is considered to be user data (as long as the data has only been received but not yet used for an update) and its authenticity and integrity shall be ensured.
eHC access logs (also referred to as: access logging data)	Accesses to the eHC are logged. The log entry is written to the eHC by the TOE.
Protocol data	For every time the TOE reads out and stores health insurance and emergency data, it generates protocol data. All protocol data entries are later transmitted to the DMS alongside the data.

Tabelle 3: User data

1.4.8.2 TSF data

At least the following TSF data is used by the TOE and has to be adequately protected:

Data	Description

[10] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

[11] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

Data	Description
Administrator credentials (also referred to as: Administrator PIN, PIN for the management interface, i.e. Administrator PIN and TOE Reset shared secret, TOE Reset PIN)	The TOE stores references of the administrator credentials (i.e. a PIN) for the management interface of the TOE. This data shall be held confidential and integrity protected. The administrator PIN shall have the attribute “administrator PIN validity”, which indicates whether the current PIN is valid. The PIN is only invalid directly after delivery and after or during a reset to factory defaults. Under these circumstances the attribute ensures that the TOE forces the administrator to set a valid management interface PIN in order to prevent an attacker from gaining easy access to management functionality. The modification of the validity of the management interface PIN is tied to the change of the management interface PIN. By setting the PIN, the administrator changes the validity of the PIN to valid. The TOE has to offer an additional TOE reset mechanism (fallback) in case that administrator credentials are lost. The authentication mechanism for this fallback has to be described in the ST. Its usage causes a reset to factory defaults. Subsequently the administrator must set a new administrator PIN. It is recommended to implement the fallback mechanism by a TOE Reset PIN which is an additional PIN that may be used by the administrator if he has forgotten the administrator PIN. The developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator’s authenticity.
User ID (for the management interface)	The TOE does not implement a user ID for the management interface, e.g. in order to support multiple administrators.
Symmetric encryption key for the encryption of the data records within the persistent storage (encrypted)	The encrypted symmetric keys for encryption of data records reside in the persistent storage. They are encrypted using the functionality of the authorised card of the respective medical supplier storing the data records.
Symmetric encryption key for the encryption of the data records within the persistent storage (unencrypted)	The decrypted symmetric key is stored in the volatile memory of the TOE, while the TOE is used by the medical supplier to encrypt or decrypt data records. The decrypted symmetric key shall be held confidential and its authenticity shall be ensured.
Public key for firmware signature check	In order to assure the integrity of new firmware, the TOE checks the signature of the firmware using a public key. The public key is part of the installed firmware. This data shall be protected against modification.
Cross CVC	Cross CVCs are used for the card-to-card authentication between cards of different roots.
Installed firmware	The TOE firmware shall be protected against modification. The firmware shall have the attribute firmware version, which allows the TOE to differentiate between different firmware releases (e.g. in order to prevent downgrades). The firmware can be resetted to factory defaults. This will cause all device settings (device configuration) and data stored by the TOE to be lost.
Time settings	Two kinds of “time settings” are used: A) The TOE has an internal clock, the setting of which is the responsibility of the administrator. The time settings 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.

Tabelle 4: TSF Data

1.4.9 External entities and subjects

The following external entities interact with the TOE:

Entity	Description
User	The medical supplier and the administrator are summarized under the term user.
Medical supplier[12]	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 may provide additional management functionalities specifically for the developer.
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify security relevant data.
Data Management System (DMS) for a practice or hospital	The DMS is the main system of the medical supplier (e.g. at an office or at a hospital). The medical supplier is able to transfer stored data records from the TOE to the DMS via a local interface.
Smart cards	The TOE communicates with smart cards like the HPC and the eHC placed in card slots. All of these smart cards hold an X.509 certificate which provide their card identity.
Authorised Card	An authorised card is a smart card, which is authorised to unlock the eHC. This smart card is used by the medical supplier and can either be an HPC or an SMC - B.
User Card	A user card is a smart card or a memory card which contains health insurance data. It is used by a health insured person and can either be an eHC or a KVK.

Tabelle 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.

Tabelle 6: Subjects

[12] 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.

2 Postulat der Übereinstimmung „ASE_CCL“

Diese Sicherheitsvorgaben (Security Target) sind generiert im Rahmen und unter Beachtung der Regeln der Common Criteria, Version 3.1, Release 4.

Das Security Target ist „CC Part 2 extended“ (wegen FDP_SVR.1) und „CC Part 3 conformant“.

Die Sicherheitsvorgaben erheben Anspruch auf strikte Übereinstimmung mit den Common Criterial Protection Profile für das „Mobile Card Terminal for German Healthcare System (MobCT)“, BSI-CC-PP-0052, Version 1.4 vom 24.09.2014 [PP_MobCT].
Dieses Protection Profile wurde vom Bundesamt für Sicherheit in der Informationstechnik herausgegeben. Es wurde am 19.01.2015 zertifiziert und ist als zertifiziertes Schutzprofil auf der Webseite des BSI veröffentlicht.

Vorgegeben ist die Vertrauenswürdigkeitsstufe EAL3, verstärkt durch die Anforderungen ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.5.

3 Definition der Sicherheitsprobleme „ASE_SPD“

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

3.1 Annahmen

The following assumptions need to be made about the environment of the TOE to allow the secure operation of the TOE and to protect the assets named in chapter 1.4.8.

Assumption	Description
A.MEDIC	The medical supplier is assumed to be non hostile, always act with care and read the existing guidance documentation of the TOE. The medical supplier ensures that the rules for the operational environment of the TOE are adhered to as required by the guidance. The medical supplier will be responsible for the secure operation of the TOE. This responsibility is equivalent to their responsibility for the safe operation of medica devices, the adherence with data protection, and the safe storage of drugs. 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.[13] Further, the medical supplier will ensure that • they never disclose the card holder PIN, • they are not observed while entering the card holder PIN, • they are not observed while reading insurance and emergency data from the display (with one exception: the medical supplier may show a patient his insurance and emergency data); • the authorised card is pulled from the card slot or the authenticated state of the TOE is dropped manually when the TOE is no longer in use; • they check the local interface 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.

[13] 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
A.ADMIN	The administrator is assumed to be non hostile, always act with care, read the existing guidance documentation of the TOE and adhere to the rules of the TOEs environment. The administrator will ensure that • the time of the TOE is set correctly, • the firmware is only updated to certified versions, • they set the new administrator PIN immediately upon performing the reset to factory defaults • they set the time-out value for the medical supplier inactivity during the initial start-up and afterwards, • they never disclose the PIN for the management interface and • they are not observed while entering the PIN for the management interface.
A.Developer	The developer is assumed to be non hostile, always act with care and knows the existing guidance documentation of the TOE. The developer provides an additional TOE reset mechanism (fallback) and describes it in the ST. If the fallback mechanism is implemented by a TOE Reset PIN, the developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator's authenticity. The request is documented by the developer. If the fallback mechanism is implemented by a challenge response mechanism the developer stores the device-specific shared secret in a safe way and tells the administrator the response to a challenge on his request after the successful verification of the administrator's authenticity. The request is documented by the developer.
A.CARDS	The authorised cards and the eHC are smart cards that comply with the specification of the gematik as referenced in [mobKT]. . The authorised card will provide the following functionality to the TOE: • Identification and authentication of medical suppliers using a PIN • Unlocking of eHCs via card-to-card authentication • Generation of random numbers with at least 100 bit of entropy for the generation of symmetric keys. • Asymmetric encryption/decryption of symmetric keys which are used to encrypt the persistent storage of the TOE. • Emergency data 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	The TOE is assumed to be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier. Furthermore, the connection between the TOE and the DMS is assumed to be: • established using a cable (USB, RS-232, etc.) • easy to survey for the medical supplier and • under the sole control of the medical supplier. Network interfaces (e.g. Ethernet) will not be used.

Assumption	Description
A.PHYSICAL	The secure TOE environment is assumed to protect the TOE against physical manipulation[14]. Specifically, the environment will assure that • the card holder PIN cannot be intercepted during transfer to the authorised card, and • data records can not be intercepted during transfer from the TOE to the DMS. The TOE is assumed to have no unnecessary electronic contacts and no obvious constructional defects.
A.ENVIRONMENT	While the TOE is in use by either the medical supplier or the administrator, they always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE is not in use, it is kept in a secure area. • The secure area is checked for physical manipulation before the TOE is taken from it and used. • A breach of this secure area by an attacker must be detectable. In this case the TOE has to be replaced, regardless of whether there is any visible sign of manipulation of the TOE.

Tabelle 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	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[15] records stored in the persistent storage of the TOE.
T.AUTH_STATE	An attacker could steal the TOE with a plugged authorised card while the TOE is in an authenticated state. Thereby, the attacker could access stored health insurance data and emergency data. The threatened assets are health insurance data and emergency data residing in the persistent storage. The attacker needs to have basic knowledge on the TOE.
T.ADMIN_PIN	An attacker may try to acquire the administrator PIN or credentials for the TOE reset mechanism (e.g. the TOE Reset PIN or the shared secret in case of a challenge response authentication mechanism) by guessing or predicting. An attacker may try to spy out the administrator PIN or credentials for the TOE reset mechanism via the display.

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

[15] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

Threat	Description
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.

Tabelle 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 [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.
OSP.LOG_DATA	The TOE shall generate a protocol entry containing the following information whenever health insurance data or emergency data is written to the persistent storage of the TOE: • the timestamp, • the approval number of the TOE as specified [MobKT]. Additional information may be added to this a protocol entry, as long as no patient information is revealed within or by the protocol entry (e.g. information for the internal administration of the data, for example an search index to accelerate search operations).
OSP.TRANSFER	The TOE shall enable the medical supplier to transfer data records to the DMS only. The TOE shall never transmit health insurance data or emergency data to card slots. Additionally the integrity of the data records is to be protected during transmission by an EDC as specified in [MobKT].
OSP.DMS_CONNECTION	The TOE shall not permit access to the KVK or eHC while the TOE is connected to the DMS. If the TOE uses a docking station, this docking station shall transmit health insurance data and emergency data to the DMS only. It shall never store either indefinitely.
OSP.C2C	The TOE shall initiate the card-to-card authentication between the authorised card and the eHC right before the TOE reads/writes data from/to the eHC. If the authentication did not succeed, no access shall be performed by the TOE[16]. This OSP prevents that faked eHC can be used by the TOE.
OSP.TIME	The TOE shall provide a reliable timestamp for the following purposes: • logging of eHC accesses, • generation of protocol data, • the checking of the validity period of card certificates. The TOE shall not allow the setting of the date while health insurance data is still in the persistent storage of the TOE.
OSP.SEALING	The body of the TOE shall be equipped with a seal by the manufacturer. The seal protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The sealing shall be compliant to BSI – TR 03120 ([TR03120]) and has been tested accordingly[17].

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

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

Policy	Description
OSP.SELFTESTS	The TOE shall be able to perform self tests to verify the correct operation of its security functionality and the integrity of the firmware. The self tests shall run at least during initial start-up.
OSP.EMERGENCY_DATA[18]	The TOE shall verify the integrity of the emergency data after receipt and protect the integrity of the emergency data while it resides inside the TOE, in order to ensure correct visualisation of the data.

Tabelle 9: Organisational Security Policies

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).

[18] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

4 Sicherheitsziele „ASE_OBJ“

4.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE

Objective	Description
O.PIN	The TOE shall serve as a secure pin entry device for the user. Thus the TOE has to provide the user with the functionality to enter an authorised card PIN and ensure that the PIN is never released from the TOE and only relayed to the card slot where the authorised card is plugged in. The TOE shall accept the result of the authentication of the medical supplier to the authorised card for the authentication of the medical supplier role to the TOE.
O.RESIDUAL	The TOE shall delete all security relevant data from volatile memory in a secure manner when it is no longer used. This applies to: • the card holder PIN of the medical supplier, • the PIN for the management interface. • the health insurance data, • the emergency data, as well as • for unencrypted TSF data but the installed firmware.
O.SELFTESTS	The TOE shall be able to perform self tests to verify the correct operation of its security functionality and the integrity of the firmware. The self tests shall run at least during initial start-up.
O.PROTECTION	The TOE shall encrypt data records in the persistent storage[19] using the algorithms specified in [Crypto]. 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. • The medical supplier forces to drop the state manually. • Power loss. The TOE shall drop the authenticated state for a administrator session and thereby delete all unencrypted sensitive information from memory in the following situations: • 15 minutes of administrator inactivity after administrator authentication. • The administrator forces to drop the state manually (by logging off). • Power loss.

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

Objective	Description
O.I&A	The TOE shall provide an authentication mechanism (e.g. PIN based) for administrators. The TOE shall enforce the following quality metrics for secrets used for the management authentication mechanism: - at least 8 digits for a PIN, - the user ID shall not be a part of the PIN. The TOE shall not display the PIN during the authentication process. The TOE shall not allow the PIN to leave the TOE. The TOE shall force the administrator to set an administrator PIN during initialisation (first initialisation or after reset to factory defaults). The TOE shall lock an account after a specified number of unsuccessful authentication attempts for a specified period of time. The TOE shall provide an additional TOE reset mechanism (fallback) called “TOE reset with authentication”. If the fallback mechanism is implemented in the recommended way by a TOE Reset PIN: The TOE contains for the TOE reset mechanism an initial, unpredictable device specific TOE Reset PIN which is set by the developer before the delivery to the user. The TOE Reset PIN is changeable by the administrator in order to allow that in case of an administrator switch the former TOE Reset PIN is invalid. If the fallback mechanism is implemented by a challenge response mechanism: The TOE uses a challenge response mechanism for the TOE reset mechanism. It contains an unpredictable device-specific shared secret which is set by the developer before the delivery to the user. The TOE shall lock an account after a specified number of unsuccessful authentication attempts for a specified period of time. Optionally the TOE may offer another additional TOE reset mechanism called “TOE reset without authentication” which does not request for the administrator’s credentials before performing a TOE reset to factory defaults. If implemented, the functionality shall be turned off as factory default. Performing such a TOE reset shall not be accidentally possible. The TOE shall notify its medical suppliers before the first usage after a TOE reset without authentication. The message shall be acknowledged by the medical suppliers.
O.MANAGEMENT	The TOE shall provide the following management functionality to an authenticated administrator: • Firmware update • Import of Cross CVCs • Management of time • Management of login credentials • Reset to factory defaults[20]. In addition the TOE may also provide the management functionality “Reset to factory defaults” to the developer. A firmware consists of two parts: firstly the so-called “firmware list” and secondly the “firmware core” which includes the whole firmware except the firmware list. Firmware lists and cores have to versioned independently. The firmware list states all firmware core versions to which a change is allowed: An update of the firmware core is only allowed if the core version is included in the firmware list. In case of a downgrade of the firmware core the TOE must warn the administrator before the installation that he is doing a downgrade, not an upgrade. The TOE must offer him the chance to cancel the installation. An update of the firmware list is only allowed to newer versions. Both, updates of firmware core and list are only allowed if their integrity and authenticity is ensured. They can be updated independently.

[20] When the device is reset to factory defaults, all data in the persistent storage except the firmware and, if applicable, the TOE reset credentials are securely deleted and the login credentials for the management interface are set back to initial values and require changing.

Objective	Description
O.LOG_CARDS	The TOE shall log accesses to eHCs on the cards itself. The following information shall be logged according to [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 [MobKT]. Additional information may be added to this a protocol entry, as long as no patient information is revealed within or by the protocol entry.
O.TRANSFER	The TOE shall enable the medical supplier to transfer data records to the DMS only. The TOE shall never transmit health insurance data or emergency data to card slots. The integrity of the data records is to be protected during transmission by an EDC as specified in [MobKT].
O.DMS_CONNECTION	The TOE shall not permit access to the KVK or eHC while the TOE is connected to the DMS. If the TOE uses a docking station, this docking station shall transmit health insurance data and emergency data to the DMS only. It shall never store either indefinitely. .
O.C2C	The TOE shall initiate the card-to-card authentication between the authorised card and the eHC right before the TOE reads/writes data from/to the eHC. If the authentication did not succeed, no access shall be performed by the TOE.
O.TIME	The TOE shall provide a reliable timestamp for the following purposes: • logging of eHC accesses, • generation of protocol data, • the checking of the validity period of card certificates. The TOE shall not allow the setting of the date while health insurance data is still in the persistent storage of the TOE.
O.SEALING	The body of the TOE shall be equipped with a seal by the manufacturer. The seal protects security relevant parts of the TOE and proves the authenticity and physical integrity of the device. The sealing shall be compliant to BSI – TR 03120 ([TR03120]) and has been tested accordingly.

Tabelle 10: Security Objectives for the TOE

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. 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 wiretapping; • they check that the sealing and the body of the TOE is undamaged every time the device is used by the medical supplier • they request the administrator to set the time-out value for medical supplier inactivity as low as possible and • they do only use the TOE after consulting with the administrator if “TOE reset without authentication”, “First TOE usage” or “Firmware Update” messages are indicated.
OE.ADMIN	The administrator shall be non hostile, always act with care, 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, • 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.

Objective	Description
OE.Developer	The developer is assumed to be non hostile, always act with care and knows the existing guidance documentation of the TOE. The developer provides an additional TOE reset mechanism (fallback). If the fallback is implemented in the recommended way by a TOE Reset PIN: The developer sets an initial, unpredictable device-specific TOE Reset PIN for the TOE reset mechanism before delivery to the user. The developer may store the TOE Reset PIN for the administrator in a safe way and tells it to him on request after the successful verification of the administrator's authenticity. The request is documented by the developer. If the fallback mechanism is implemented by a challenge response mechanism: The developer sets an unpredictable device-specific shared secret for a challenge response mechanism which is used for the TOE reset mechanism before delivery to the user. The developer stores the shared secret in a safe way and tells the administrator the response to a challenge on his request after the successful verification of the administrator's authenticity. The request is documented by the developer.
OE.CARDS	The authorised cards and the eHC are smart cards that comply with the specification of the gematik as referenced in [mobKT]. The authorised card shall provide the following functionality to the TOE: • Identification and authentication of medical suppliers using a PIN • Unlocking of eHCs via card-to-card authentication • Generation of random numbers for the generation of symmetric keys as specified in [Crypto]. • Asymmetric encryption/decryption of symmetric keys which are used to encrypt the persistent storage of the TOE. • Emergency data on the eHC shall be signed with the use of the authorised card that created the data records on the eHC to allow the TOE to verify integrity.
OE.DMS	The TOE shall only be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier. Furthermore, the connection between the TOE and the DMS shall be: • established using a cable (USB, RS-232, etc.) • be under the sole control of the medical supplier • easy to survey for the medical supplier. Network interfaces (e.g. Ethernet) shall not be used.
OE.PHYSICAL	The secure TOE environment shall protect the TOE against physical manipulation. Specifically, the environment shall assure that • the card holder PIN can not be intercepted during transfer to the authorised card, and • data records can not be intercepted during transfer from the TOE to the DMS. The TOE shall have no unnecessary electronic contacts and no obvious constructional defects.
OE.ENVIRONMENT	While the TOE is in use by either the medical supplier or the administrator, they always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE is not in use, it is kept in a secure area. • The secure area is checked for physical manipulation before the TOE is taken from it and used. • A breach of this secure area by an attacker must be detectable. In this case the TOE has to be replaced, regardless of whether there is any visible sign of manipulation of the TOE.

Tabelle 11: Security Objectives for the environment of the TOE

4.3 Erklärung der Sicherheitsziele

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

Tabelle 12: Security Objectives for the environment of the TOE

Hinweis: In die Tabelle 12 der Abhängigkeiten ist die Zeile A.Developer eingearbeitet worden.

4.3.1 Abwehr der Bedrohungen durch den EVG

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 the supplement of the Protection Profile [PP_suppl] 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 bya combination of *O.AUTH_STATE, OE.MEDIC, OE.ADMIN* and *OE.ENVIRONMENT. O.AUTH_STATE* describes the occasions on which the device shall drop the authenticated state. *OE.MEDIC* and OE.ADMIN describe that the medical supplier and the administrator shall be responsible for the secure usage of the device and *OE.ENVIRONMENT* describes the general handling of the TOE in terms of the control the medical supplier and the administrator has to exert over the environment of the TOE.
The threat **T.FIRMWARE**, which describes that an attacker could try to alter firmware of the TOE, is countered by a combination of *O.I&A, O.MANAGEMENT* and *O.RESIDUAL*. *O.I&A* describes that the TOE shall authenticate administrators. *O.MANAGEMENT* describes the management functionality for updating the firmware including a verification of the firmware's authenticity. *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 mechanism for the administrator PIN and credentials for the TOE reset mechanism protects the PIN and credentials 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 a TOE Reset Pin resp. the answer for challenge response mechanism is only told to the administrator on request after the successful verification of the administrator's authenticity.

4.3.2 Abdeckung der organisatorischen Regeln

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 Abdeckung der Annahmen

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 Definition der erweiterten Komponenten „ASE_ECD“

5.1 Definition of the family FDP_SVR Secure Visualisation[21]

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: Secure Visualisation	1

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 identified in case FAU_GEN is part of the PP/ST.

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[22] is incomplete.
FDP_SVR.1.3	The TSF shall reject any visual representation of data which comprises parts which cannot be interpreted or represented unambiguously by the TSF according to the [assignment: data scheme] and notify the user.

[21] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2, daher ist dieser Abschnitt irrelevant

[22] The term “data” in FDP_SVR.1.2 and FDP_SVR.1.3 refers to the data (“data to be interpreted”) as assigned in FDP_SVR.1.1.

6 Sicherheitsanforderungen „ASE_REQ“

6.1 Funktionelle Sicherheitsanforderungen

Im Securitry Target wurden für die SFRs Operationen durchgeführt. Alle Assignments wurden *kursiv* und in Klammern gesetzt. Alle Selections wurden unterstrichen und in Klammern gesetzt. Refinements wurden **fett** gesetzt. Iterationen wurden durch ein “/” gefolgt von einem einen Bezeichner im Namen des SFRs kenntlich gemacht.

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 [*random number generator featured by authorised card*] and specified cryptographic key sizes [*as specified in **[Crypto]***] that meet the following: [*symmetric encryption standards according to **[Crypto]***].

Application Note 1: The TOE shall use a hybrid encryption method according to [Crypto]. The cryptographic symmetric key, generated by FCS_CKM.1 shall be used for the symmetric encryption of the emergency data and the health insurance data within the persistent storage of the TOE. The symmetric encryption key is then encrypted via the authorised card.
The generation of the symmetric key is performed using a random number generator which is provided by the authorised card.

6.1.1.2 FCS_CKM.4- Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with aspecified cryptographic key destruction method [*overwriting*] that meets the following:[*cryptographic standards according to **[Crypto]***].

6.1.1.3 FCS_COP.1/AES- Cryptographic operation for storage encryption

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

Application Note 2: The cryptographic functionality in FCS_COP.1/AES and FCS_CKM.1 shall be used to encrypt the emergency data[23] 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 [*SHA + RSA*] and cryptographic key sizes [*256Bit (SHA) + 2048Bit (RSA*)] that meet the following: [***[Crypto]***].

Application Note 3: 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.

6.1.1.5 FCS_COP.1/DATA- Cryptographic operation for emergency data[23]

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

Application Note 4: 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, but to check the mathematical correctness of the signature.

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,*
- *TOE reset PIN (i.e. PUK),*
- *health insurance data,*
- *emergency data,*
- *firmware,*
- *public key for firmware verification,*
- *time settings,*
- *symmetric keys (encrypted and decrypted),*
- *card slot,*
- *access logging data*
- *[none]*

Operations:
- *Read,*
- *modify,*

[23] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2, daher ist dieser Abschnitt irrelevant

- *delete*
- *[none]*].

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,*
- *TOE reset PIN (i.e. PUK),*
- *health insurance data,*
- *emergency data,*
- *firmware,*
- *public key for firmware verification,*
- *Cross CVCs,*
- *time settings,*
- *symmetric keys (encrypted and decrypted),*
- *card slot,*
- *access logging data*

Object attributes:

- *firmware version,*
- *administrator PIN validity,*
- *[none]*].

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

- *Access to health insurance data or emergency data from the storage shall be allowed if the data was decrypted with the help of the same authorised card which was used to encrypt the data.*
- *An update of the firmware of the TOE shall only be allowed by an authenticated administrator:*
  - *A firmware consists of two parts: firstly the so-called "firmware list" and secondly the "firmware core" which includes the whole firmware except the firmware list. The firmware list states all firmware core versions to which a change is allowed. Firmware lists and cores have to be versioned independently.*
  - *An update of the firmware core is only allowed if the core version is included in the firmware list. Firmware lists must only contain version numbers of firmware cores which are certified accordingly the Protection Profile [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.*

[No other rules]].

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 TOE Reset PIN], [No subject except the administrator shall set the TOE Reset PIN]*
- *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]*

].

Application Note 5: In FDP_ACF.1.2 “With the help of” refers to the fact that the data is en-/decrypted with the symmetric key which is stored on the TOE and is itself encrypted by the authorised card.
The TOE uses functionality of the authorised card to determine if the stored data was stored with the help of (and therefore may be accessed with the help of) the authorised card. This means for FDP_ACF.1.2 that the TOE is able to determine if the decrypted data is real data and not data that was decrypted with a false key. In the latter case, access to the data shall be denied by the TOE.

Application Note 6: 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*[24]].

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*].

6.1.2.5 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 by the medical supplier via the PIN pad shall only be sent to the card slot where the authorised card is plugged in. No PIN must be sent to the card slot where the eHC is plugged in.*
- *The TOE shall only read data from the eHC when the card-to-card authentication between the authorised card and the eHC succeeded recently.*

].

FDP_IFF.1.3/Cards The TSF shall enforce the [*following rule:*
If protected health insurance data or emergency data is read from the eHC, the TOE shall write an access log entry to the logging container of the eHC[25] *including:*
- *the time of access,*

[24] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

[25] The eHC possesses a logging container. Every read-access to the eHC which accesses emergency data (not implemented, see 1.4.1.2) or protected health insurance data has to be logged within this container.

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

If protected health insurance data or emergency data is read from the eHC, 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 registration number,*
- *[assignment: no further data]*

].

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

].

Application Note 7: FDP_IFF.1.2/Cards: here Here “recently” means that the C2C authentication shall be initiated every time right before data is read from an eHC. This limits the risk that the eHC can be replaced with a faked eHC to read faked data records.

Application Note 8: FDP_IFF.1.3/Cards: the The identity of the authorised card which was used to access the eHC clearly identifies the medical supplier that initiated the operation. However, in case the authorised card is not a personal card but a card of an institution/organisation used by more than one medical supplier, the institution/organisation needs to account which person possessed the card at a specific time.

6.1.2.6 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 [**MobKT**].*
- *[no further rules]*

].

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

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

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

6.1.2.7 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*].

Application Note 9: User data in FDP_ITC.1 is the public key of the associated private key that was used to sign the emergency data[26] on the eHC. The public key is also transferred from the eHC (as part of the data) to the TOE in order to check the signature for mathematical correctness.

6.1.2.8 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 [calibration data, TOE reset credentials]*].

Application Note 10: The data to be erased includes encrypted health insurance and emergency data[2627] in the persistent storage, as well as temporary user data e.g. an unencrypted symmetric encryption key and user settings.

6.1.2.9 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 state, 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*[27]*,*
- *card holder PIN of the medical supplier,*
- *PIN for the management interface and*
- *[no other objects]*].

Application Note 21: The data to be erased does not include the encrypted data storage of the TOE or user settings.

6.1.2.10 FDP_SDI.2–Stored data integrity monitoring and action

[26] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

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: [*checksum of every data set*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*not use the data, inform the medical supplier, and [No other actions]*].

Application Note 11: The notification of the medical supplier in case of an integrity error shall be visual.

6.1.2.11 FDP_SVR.1–Secure visualisation of data content

FDP_SVR.1.1 The TSF shall ensure that the [*emergency data*[27] *and [no further data to be interpreted]*] is represented completely and unambiguously according to the [*scheme specified in [**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 [**MobKT**]*] and notify the user.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1–Authentication failure handling

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

FIA_AFL.1.2 Whenthedefined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the authentication mechanism for a period of time according to* **Tabelle 13** *depending on the number of consecutive unsuccessful authentication attempts*].

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

Tabelle 13: Lockout times

6.1.3.2 FIA_SOS.1 –Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following**: [
A PIN for the management interface shall meet the following
- *Have a length of at least 8 characters,*
- *Be composed of at least the following characters: "0"-"9",*
- *Shall not be saved on programmable function keys].*

[27] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

Application Note 12: PIN for the management interface are the administrator PIN and, the TOE Reset PIN. They are also named as “login credentials”, “administrator credentials” and “administrator login credentials”.

6.1.3.3 FIA_UAU.1 –Timing of authentication

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

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

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

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

6.1.3.4 FIA_UAU.5 –Multiple authentication mechanism

FIA_UAU.5.1 The TSF shall provide [

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

] to support user authentication.

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

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

6.1.3.5 FIA_UAU.7 –Protected authentication feedback

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

Application Note 13: This SFR provides protected authentication feedback for entry of the management PIN and the card holder PIN.
In case of the card holder PIN, identification is provided by the authorised card in the environment of the TOE. However, the card holder PIN is entered via the PIN pad of the MobCT (see FIA_UAU.5).

6.1.3.6 FIA_UID.1 –Timing of identification

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

- *Firmware update*
- *Import of Cross CVCs*
- *Management of time settings,*

- *Reset to factory defaults,*
- *Management of login credentials*
- *[assignment: none]*

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

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

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 management interface PIN*] [**[*to valid by setting the administrator PIN*]**][28] to [*the administrator*].

Application Note 14: 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 attributes initialisation

FMT_MSA.3.1 The TSF shall enforce the [*MobCT SFP*] to provide [restrictive] default values for **the security attribute validity of the management interface 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.

Application Note 15: *The validity of the administrator PIN indicates whether the current PIN is valid. The PIN is only* invalid directly after delivery and after or during a reset to factory defaults. Under these circumstances the attribute ensures that the TOE forces the administrator to set a valid administrator PIN in order to prevent an attacker from gaining easy access to management functionality.

6.1.4.3 FMT_MTD.1 – Management of TSF data

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

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

] to [*the administrator and [none]*].

[28] 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.

6.1.4.4 FMT_MTD.3 – Secure TSF data

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

Application Note 16: Secure values for the session time-out of the medical supplier session are times between 1 and 60 minutes[29], compare FTA_SSL.3.1.

6.1.4.5 FMT_SMF.1 – Specification of Management Functions

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

- *Firmware update*
- *Import of Cross CVCs*
- *Management of time settings*
- *Reset to factory defaults*
- *Management of administrator login credentials*
- *[assignment: none]*

6.1.4.6 FMT_SMR.1 – Security roles

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

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

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 [*15 minutes*] **of administrator inactivity, after [1 – 60 minutes] of medical supplier inactivity and after power loss.**

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.

Application Note 17*:* FTA_SSL.3 and FTA_SSL.4 apply to the sessions of medical supplier and administrator. Session termination of the medical supplier refers to the dropping of the authenticated state of the TOE. When the authenticated state is dropped, the authenticated state of the authorised card shall be dropped, too and the medical supplier has to unlock the authorised card again in order to read data from the storage or an eHC or transfer it to a DMS.

[29] 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.

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[30] time stamps.

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[31]** whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application Note 18*:* The capability to detect physical tampering refers to the body of the TOE and its required sealing by the manufacturer.

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 [*[periodically during normal operation]*] 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 [TSF data].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [TSF].

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

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

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

Assurance Class	Assurance Components
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

Tabelle 14: Chosen Evaluation Assurance Requirements

These assurance components represent assurance level EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.5.

6.3 Beziehungen der Sicherheitsanforderungen

6.3.1 Abdeckung der Sicherheitsziele durch die Anforderungen

Die folgende Tabelle gibt einen Überblick über die Abdeckung der Sicherheitsziele durch die definierten Sicherheitsanforderungen.

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

	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
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											

Tabelle 15: Abdeckung der Sicherheitsziele

The security objective **O.PIN** is met by a combination of the SFR FDP_ACC.1, FDP_ACF.1, FDP_IFC.1/Cards, FDP_IFF.1/Cards, FIA_UAU.5 and FIA_UAU.7. FDP_ACC.1 defines the access control policy for the TOE. FDP_ACF.1 defines the rules for the policy which supports the secure PIN entry by preventing access to the temporarily stored PIN. FDP_IFC.1/Cards defines the information flow control policy for card communication. FDP_IFF.1/Cards defines the rules for the policy. FIA_UAU.5 defines the authentication mechanism for the terminal via the authentication of the medical supplier at the authorised card. Finally, FIA_UAU.7 defines that the PIN can not be read from the display during entry.
The security objective **O.RESIDUAL** is met by the SFR FDP_RIP.1/FW and SFR FDP_RIP.1/Data as it defines the residual information protection.
The security objective **O.SELFTESTS** is met by the SFR FPT_TST.1 as it defines the self tests of the TSF which have to be provided by the TOE.
The security objective **O.PROTECTION** is met by a combination of the SFR FCS_CKM.1, FCS_CKM.4, FCS_COP.1/AES, FCS_COP.1/DATA, FDP_ACF.1, FDP_ACC.1, FDP_IFC.1/Cards, FDP_IFF.1/Cards, FDP_ITC.1, FDP_SDI.2 and FDP_SVR.1. FCS_CKM.1 and FCS_CKM.4 define the cryptographic key generation and destruction used for the AES storage encryption defined in FCS_COP.1/AES. FCS_COP.1/DATA defines the mathematical signature verification of stored data. FDP_ACC.1 and FDP_ACF.1 define the access control policy and rules for accessing stored data. FDP_IFC.1/Cards and FDP_IFF.1/Cards define that no data shall be written to the KVK and no data other than logging data shall be written to the eHC. FDP_ITC.1 defines the import of the public key for Signature verification of emergency data[32]. FDP_SDI.2 explicitly defines the integrity protection of stored data. Finally FDP_SVR.1 defines the secure visualization of the emergency data[32].
The security objective **O.AUTH_STATE** is met by a combination of the SFR FTA_SSL.3 and FTA_SSL.4. FTA_SSL.3 defines how the authenticated state is dropped by the TSF and FTA_SSL.4 defines how the medical supplier and the administrator can drop the authenticated state manually.
The security objective **O.I&A** is met by a combination of the SFR FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FMT_MSA.1, FMT_MSA.3, and FMT_SMR.1. FDP_ACC.1 defines the access control policy for the TOE. FDP_ACF.1 defines the rules for the policy which prevents the PIN from being read. FIA_AFL.1 defines the authentication failure handling for the management interface. FIA_SOS.1 defines the quality metrics of credentials used for management. FIA_UAU.7 defines that PINs are never sent in clear text to a display. FIA_UAU.1 and FIA_UID.1 describe that a user has to be identified and authenticated for some TSF mediated actions. FIA_UAU.5 defines which roles need to be authenticated. FMT_MSA.1 and FMT_MSA.3 define that the TOE forces the administrator to initially set the administrator PIN. Finally, FMT_SMR.1 defines the roles that are enforced using the authentication mechanism.

[32] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2

The security objective **O.MANAGEMENT** is met by a combination of the SFR FCS_COP.1/FW, FDP_ACC.1, FDP_ACF.1, FIA_UAU.1, FIA_UID.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. FCS_COP.1/FW defines the signature verification of the firmware. FIA_UID.1 and FIA_UAU.1 define the identification and authentication mechanism used to access the management interface. FMT_SMF.1 defines the management functions. FMT_SMR.1 defines the roles used for management. FMT_MTD.1 defines that access to some TSF data is limited to administrators.
The security objective **O.LOG_CARDS** is met by a combination of the SFR FDP_IFC.1/Cards, FDP_IFF.1/Cards and FPT_STM.1. FDP_IFC.1/Cards and FDP_IFF.1/Cards define the logging of eHC accesses and restrict the write access to the eHC to logging and deny the write access to the KVK in general. FPT_STM.1 defines the reliable time stamp which is necessary for the logging mechanism.
The security objective **O.LOG_DATA** is met by a combination of the SFR FDP_IFC.1/Cards, FDP_IFF.1/Cards and FPT_STM.1. FDP_IFC.1/Cards and FDP_IFF.1/Cards define the rules for the generation of the protocol data and restrict the protocol data, which is unencrypted, to non-sensitive data. FPT_STM.1 defines the reliable time stamp which is necessary for the generation of the protocol data.
The security objective **O.TRANSFER** is met by a combination of the SFR FDP_IFC.1/DMS, FDP_IFF.1/DMS, FDP_IFC.1/Card and FDP_IFF.1/Card. FDP_IFC.1/DMS defines the DMS communication SFP and FDP_IFF.1/DMS defines the rules for the DMS communication SFP. FDP_IFC.1/Card and FDP_IFF.1/Card describe that data records shall never be transferred to card slots.
The security objective **O.DMS_CONNECTION** is met by a combination of the SFR FDP_ACC.1, FDP_ACF.1, FDP_IFC.1/DMS and FDP_IFF.1/DMS. FDP_ACC.1 defines the access control policy for the TOE. FDP_ACF.1 defines the rules for the policy which prevents access to eHC and KVK cards while the TOE is connected to the DMS. FDP_IFC.1/DMS and FDP_IFF.1/DMS define the rules for the data transfer to the DMS. The security objective **O.C2C** is met by a combination of the SFR FDP_IFC.1/Cards and FDP_IFF.1/Cards. The two SFR describe an information flow policy that requires the TOE to initiate card-to-card authentication prior to read data from an eHC.

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

6.3.2 Dependency Rationale

SFR	Dependencies	Support of the dependencies
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the use of FCS_COP.1/AES, and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by the use of FCS_CKM.1

SFR	Dependencies	Support of the dependencies
FCS_COP.1/AES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the use of FCS_CKM.1, FCS_CKM.4
FCS_COP.1/FW	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	See chapter 6.3.2.1 for FDP_ITC.1 and FCS_CKM.4
FCS_COP.1/DATA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the use of FTP_ITC.1 See chapter 6.3.2.1 for FCS_CKM.4.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by the use of FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Fulfilled by the use of FDP_ACC.1 and FMT_MSA.3.
FDP_IFC.1/Cards	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/Cards
FDP_IFC.1/DMS	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/DMS
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_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/Cards See chapter 6.3.2.1 for FMT_MSA.3
FDP_RIP.1/FW	No dependencies	-
FDP_RIP.1/UserData	No dependencies	-
FDP_SDI.2	No dependencies	-
FDP_SVR.1	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled byFIA_UID.1
FIA_UAU.5	No dependencies.	-

SFR	Dependencies	Support of the dependencies
FIA_UAU.7	FIA_UID.1 Timing of identification	Fulfilled byFIA_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.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FTA_SSL.3	No dependencies	-
FTA_SSL.4	No dependencies	-
FPT_PHP.1	No dependencies	-
FPT_STM.1	No dependencies	-
FPT_TST.1	No dependencies	-

Tabelle 16: Abhängigkeiten der Sicherheitsanforderungen

6.3.2.1 Justification for missing dependencies

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

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

needs to be destructed.

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

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

The dependency FMT_MSA.3 for FDP_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 Security Target is **EAL 3 augmented byADV_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 (based on Protection Profile [PP_MobCT]) 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 EVG-Übersichtsspezifikation „ASE_TSS.1“

Dieses Kapitel beschreibt im Unterkapitel 7.1 die EVG-Sicherheitsfunktionen und in 7.2 die Sicherheitsmaßnahme. Die vom Entwickler ergriffenen Maßnahmen zur Vertrauenswürdigkeit werden im Unterkapitel 7.3aufgeführt.

Begriffsklärungen

Begriff **Kommunikation**

Hiermit ist – sofern nicht ausdrücklich abweichend beschrieben – immer der Informationsaustausch zwischen dem EVG und dem Host zu verstehen.

Begriff **Host**

Host ist die steuernde Einheit, die Befehle an den EVG sendet und Antworten empfängt.
Der Host ist der Computer (PC) mit einem Primärsystem (Data Management System), der über eine direkte Kabelverbindung mit dem EVG in Verbindung steht.

Begriff **Patientenkarte**

Die Patientenkarte ist die KVK (KrankenVersichertenKarte) oder eGK (elektronische GesundheitsKarte), nicht jedoch HBA (HeilBerufsAusweis) oder SMC (Institutskarte).
Hinweis: Von den Patientenkarten besitzt nur die eGK geschützte Daten und somit eine Zugriffskontrolle.

7.1 EVG-*Sicherheitsfunktionen*

Der EVG bietet dem Nutzer verschiedene Sicherheitsfunktionen zur Abdeckung der Sicherheitsanforderungen. Die Realisierung der einzelnen Sicherheitsfunktionen wird im Folgenden beschrieben.

In der folgenden Tabelle sind alle EVG-Sicherheitsfunktionen aufgelistet.

Sicherheitsfunktion	Bezeichnung
SF.DATEN	Schutz der Daten
SF.ANZEIGE	Sichere Anzeige von Notfalldaten
SF.I&A	Identifizierung & Authentifizierung
SF.KARTEN	Kartenkommunikation
SF.MANAGE	Management
SF.DMS	Kommunikation mit dem Hostsystem
SF.TESTS	Selbsttests

Tabelle 17: Sicherheitsfunktionen

7.1.1 Schutz der Daten (SF.DATEN)

Der EVG setzt eine Zugriffskontrolle um, die den Zugriff auf Daten regelt, die vom EVG temporär im Arbeitsspeicher oder im persistenten Speicher hinterlegt werden (**FDP_ACC.1, FDP_ACF.1**).

Es wird sichergestellt, dass auf gespeicherte Nutzerdaten (Versicherungsdaten und Notfalldaten) nur dann zugegriffen werden kann, wenn dazu die entsprechende berechtigte Karte verwendet wird. Dies wird zudem dadurch sichergestellt, dass die Nutzerdaten mit AES verschlüsselt werden, bevor sie abgelegt werden (**FCS_COP.1/AES)**. Der notwendige symmetrische Schlüssel wird vom EVG mit Hilfe der berechtigten Karte generiert (**FCS_CKM.1**). Die zugehörigen Zufallszahlen liefert die berechtigte Karte. Der symmetrische Schlüssel wird wiederummit dem öffentlichen Schlüssel der berechtigten Karte asymmetrisch verschlüsselt und kann somit auch nur mit derselben Karte wieder entschlüsselt werden.

Sobald kryptographische Schlüssel nicht mehr benötigt werden, werden Sie entsprechend im Speicher überschrieben (**FCS_CKM.4**).

Die Zugriffskontrolle garantiert zudem (**FDP_ACF.1.4**), dass

- Niemand die Kartenhalter-PIN oder symmetrische Schlüssel verändern oder auslesen kann, während sie im Arbeitsspeicher des EVG vorgehalten werden
- Niemand auf Konfigurationsdaten zugreifen kann, solange die Administrator-PIN invalide (also nicht gesetzt) ist
- Niemand die Administrator-PIN auslesen kann
- Niemand den öffentlichen Schlüssel für die Überprüfung der Firmware-Signatur verändern kann
- Niemand auf die Kartenslots der eGK bzw. KVK zugreifen kann, solange der EVG mit dem DMS verbunden ist.

Der EVG überwacht die Integrität der Daten, die im persistenten Speicher untergebracht sind, in dem er zusätzlich Prüfsummen über die Daten berechnet und sichert. Stellt der EVG fest, dass die Daten verändert worden sind, verweigert er die Verwendung der Daten und informiert den Heilberufler (**FDP_SDI.2**).

Weiterhin überschreibt der EVG sämtliche Daten in seinen Speichern (temporär und persistent, mit Ausnahme der installierten Firmware), sobald sie nicht mehr benötigt werden (**FDP_RIP.1/FW**). Wird der authentifizierte Zustand des EVG zurückgesetzt oder das Gerät ausgeschaltet, so werden die folgenden Daten aus dem Speichern des EVG gelöscht, sofern vorhanden (**FDP_RIP.1/UserData**):

- unverschlüsselte AES-Schlüssel für den persistenten Speicher
- unverschlüsselte Nutzerdaten (Versicherungsdaten und Notfalldaten)
- Kartenhalter-PIN des Heilberuflers
- Administrator-PIN für Management

7.1.2 Sichere Anzeige von Notfalldaten (SF.ANZEIGE)[33]

Der EVG zeigt Notfalldaten, die von einer eGK ausgelesen worden sind, auf seinem Display an (**FDP_SVR.1**). Hierbei wird sichergestellt, dass die Daten komplett und unmissverständlich vom Display abgelesen werden können (unter Berücksichtigung der Anforderung aus [MobKT]). Der bedienende Nutzer wird informiert, sofern das Display nicht die kompletten Daten anzeigen kann und ermöglicht die Anzeige der restlichen Daten.

Der EVG zeigt keine Notfalldaten an, sofern diese auch in mehreren Schritten nicht komplett und vollständig (unter Berücksichtigung der Anforderung aus [MobKT]) angezeigt werden können. Dies kann beispielsweise durch Fehler im Datensatz auftreten. Um mögliche Fehler im Datensatz zu erkennen, wird die Signatur der Notfalldaten auf mathematische Korrektheit überprüft (**FCS_COP.1/DATA**). Dazu wird der öffentliche Schlüssel importiert, der den Notfalldaten auf der eGK beiliegt (**FDP_ITC.1**).

[33] Notfalldaten nicht umgesetzt, siehe Abschnitt 1.4.1.2, daher ist dieser Abschnitt irrelevant

7.1.3 Identifizierung & Authentifizierung (SF.I&A)

Der EVG stellt zwei PIN-basierte Authentifizierungsmechanismen für zwei verschiedene Rollen bereit (**FIA_UAU.5, FMT_SMR.1**). Der erste Mechanismus wird für die Authentifizierung von Administratoren verwendet, die infolgedessen Managementfunktionen ausführen können (**FIA_UID.1**, **FIA_UAU.1**). Zudem überprüft der EVG die Anzahl der fehlgeschlagenen Authentifizierungsversuche. Nach einer bestimmten Anzahl Versuche (siehe Tabelle 13) wird der Zugang für eine entsprechende Zeit gesperrt (**FIA_AFL.1**).

Weiterhin bietet der EVG einem Heilberufler die Möglichkeit sich gegenüber seinem Heilberufsausweis zu authentifizieren, indem er die eingegebene PIN an die Karte weiterleitet (**FIA_UAU.5**). Hierdurch erlangt der EVG den authentifizierten Zustand. In diesem Zustand ist das Auslesen von Nutzerdaten möglich (siehe SF.KARTEN). Wird der EVG über einen einstellbaren Zeitraum (1 bis 60 Minuten) nicht verwendet, so verliert er automatisch den authentifizierten Status. Dies geschieht auch, wenn der EVG automatisch oder manuell abgeschaltet wird (**FTA_SSL.3**) oder der Nutzer die berechtigte Karte aus dem Schacht zieht (**FTA_SSL.4**). Verliert der EVG seinen authentifizierten Status, so ist auch die Karte-zu-Karte-Authentifizierung mit der berechtigten Karte zurückgesetzt.

Außerdem wird generell sichergestellt, dass die Ziffern einer PIN bei der Eingabe bei beiden Authentifizierungsmechanismen durch Platzhalter ersetzt werden (**FIA_UAU.7**).

Der EVG bietet dem TOE Administrator die Möglichkeit die TOE Reset PIN zu setzten. Die TOE Reset PIN ist eine 8 – 16 stellige numerische PIN, die in dem EVG gespeichert wird.

7.1.4 Kartenkommunikation (SF.KARTEN)

Der EVG kommuniziert mit berechtigten Karten (HBA, SMC) und Patientenkarten (eGK und KVK). Bevor Daten von einer Patientenkarte ausgelesen werden können, liest der EVG das X.509-Zertifikat der eingesteckten berechtigten Karte aus und überprüft, ob:

- die Karte sich als berechtigte Karte ausgibt,
- das X-509-Zertifikat mathematisch korrekt ist und ob
- das aktuell im EVG eingestellte Datum im Gültigkeitszeitraum des Zertifikats liegt.

Wenn eine Kartenhalter-PIN eingegeben wird, stellt der EVG sicher, dass diese nur an den Kartenschacht versendet wird, der die berechtigte Karte enthält.

Der EVG liest nur dann Daten von einer eGK aus, wenn zuvor eine Karte-zu-Karte-Authentifizierung zwischen der berechtigten Karte und der eGK erfolgreich stattgefunden hat und dieser Status noch besteht.

Werden Nutzerdaten aus geschützten Bereichen der eGK ausgelesen, vermerkt der EVG diesen Zugriff in dem Logging-Container der eGK. Hierbei werden die folgenden Daten mit aufgenommen:

- Zeitpunkt des Zugriffs,
- Bezeichnung der Daten, auf die zugegriffen wurde
- Die Identität der berechtigten Karte, mittels der auf die eGK zugegriffen wurde.

Weiterhin notiert sich der EVG die folgenden Protokolldaten

- den Zeitpunkt des Zugriffs und
- die Registrierungsnummer des EVGs, sofern diese konstante Information nicht erst bei der Übertragung hinzugefügt wird

und legt sie zusammen mit den ausgelesenen Nutzerdaten in seinem Speicher ab.

Der EVG nutzt die Systemzeit, um verlässliche Zeitstempel (+-100ppm) für den Logging-Container und die Protokolldaten zu generieren (**FPT_STM.1**). Basis dafür ist eine Echtzeituhr (RTC). Diese ist realisiert als integrierter Schaltkreis, also als eigenes Bauteil der Elektronik.

Die Echtzeituhr wird permanent stromversorgt, also auch wenn sich der EVG im ausgeschalteten Zustand befindet.

Bei der Kommunikation mit den Karten stellt der EVG sicher, dass

- bis auf den Logging-Container keine Daten auf die eGK geschrieben werden,
- niemals Daten auf eine KVK geschrieben werden,
- Nutzerdaten (Versicherungsdaten und Notfalldaten) niemals an Kartenschächte transferiert werden und

- niemals patientenspezifische Daten in den Protokolldaten abgelegt werden.

(**FDP_IFC.1/Cards, FDP_IFF.1/Cards**)

7.1.5 Management (SF.MANAGE)

Der EVG stellt die folgenden Managementfunktionen für authentifizierte Administratoren bereit (**FMT_SMF.1, FMT_MTD.1**):

- Firmware Update
- Setzen der Systemzeit mit sicheren Werten (**FMT_MTD.3**)
- Zurücksetzen in den Auslieferungszustand
- Ändern und Setzen der Zugangs-PIN für den Administrator

Bei der Änderung der Administrator-PIN erzwingt der EVG, dass die PIN mindestens aus 8 Ziffern besteht. Andernfalls wird die PIN nicht geändert oder gesetzt (**FIA_SOS.1**). Nach Auslieferung fordert der EVG den Administrator dazu auf, die PIN initial zu setzen. Vorher sind keine anderen Funktionen möglich (**FMT_MSA.1, FMT_MSA.3**).

Ein Firmware-Update wird nur dann vorgenommen, wenn (**FDP_ACF.1.2**)

- die Version der zu installierenden Firmware in der aktuellen Firmware-Gruppen-Liste eingetragen ist und
- nachdem die Integrität und Authentizität der Firmware durch eine Signaturüberprüfung sichergestellt worden ist (**FCS_COP.1/FW**). Die kryptographische Funktionalität verwendet dazu einen öffentlichen Schlüssel, der in der jeweils installierten Firmware vorgehalten wird.

Für die Signaturprüfung der Firmware werden SHA-256 und RSA mit 2048Bit-Schlüssel verwendet.

Wird der EVG in den Auslieferungszustand zurückgesetzt, so werden alle Daten mit Ausnahme der Firmware im EVG gelöscht (**FDP_RIP.1/FW**).

Die Systemzeit kann vom Administrator nur dann verändert werden, wenn keine ausgelesenen Nutzerdaten im persistenten Speicher des EVG vorhandensind (**FDP_ACF.1.2**).

7.1.6 Kommunikation mit dem Hostsystem (SF.DMS)

Der EVG ist in der Lage, die gespeicherten Nutzerdaten in seinem persistenten Speicher an ein Hostsystem (DMS) zu übertragen.

Die Kommunikation des EVG mit dem Host erfolgt direkt (**FDP_IFC.1/DMS** und **FDP_IFF.1/DMS**).

Als direkter Weg steht ausschließlich die USB-Schnittstelle des EVG zur Verfügung. Diese kann für USB-Kommunikation oder für seriellen Datenverkehr (COM) verwendet werden.

Zur Sicherung der Übertragungsstrecke muss eine regelmäßige Sichtkontrolle des Verbindungskabels zwischen EVG und Host durch den Benutzer erfolgen. Auf diese organisatorische Sicherheitsmaßnahme wird in der Bedienungsanleitung hingewiesen.

7.1.7 Selbsttests (SF.TESTS)

Bei Start des EVG und periodisch im Betrieb werden Selbsttestroutinen ausgeführt, um anschließend einen sicheren Betrieb zu gewährleisten (**FPT_TST.1**).

Erkannte Fehler aus dem Selbsttest führen generell zum Blockieren des Gerätes, da in diesem Fall ein fehlerfreier und sicherer Betrieb des EVG nicht zugesichert werden kann.

Wird das Gerät aus- und wieder eingeschaltet, so erfolgen die gleichen Tests erneut, die Auswertung wird ebenfalls in gleicher Weise durchgeführt.

7.2 EVG-Sicherheitsmaßnahmen

7.2.1 Versiegelung (SM.SIEGEL)

Anhand authentischer und fälschungssicherer Sicherheitssiegeln, welche über die Trennkante der Gehäuseteile geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden (**FPT_PHP.1**). Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Das eingesetzte Siegel ist fälschungssicher, weist Authentizitätsmerkmale auf und erfüllt die Anforderungen entsprechend [TR03120].

Der Benutzer wird in der Bedienungsanleitung darauf hingewiesen, dass die Siegel vor Benutzung des EVG auf Siegelbruch zu prüfen sind.

7.3 Erklärung der EVG-Übersichtsspezifikation

7.3.1 Sicherheitsanforderungen und Sicherheitsfunktionen

Die in der folgenden Tabelle zusammengefassten Sicherheitsfunktionen entsprechen und ergänzen die Sicherheitsanforderungen des EVG.
Alle Sicherheitsanforderungen werden durch die vorhandenen Sicherheitsfunktionen, die sich gegenseitig zu einem sicheren Gesamtsystem ergänzen, abgedeckt.

	SF.DATEN	SF.ANZEIGE	SF.I&A	SF.KARTEN	SF.MANAGE	SF.DMS	SF.TESTS	SM.SIEGEL
FCS_CKM.1	X							
FCS_CKM.4	X							
FCS_COP.1/AES	X							
FCS_COP.1/FW					X			
FCS_COP.1/DATA		X						
FDP_ACC.1	X							
FDP_ACF.1	X				X			
FDP_IFC.1/Cards				X				
FDP_IFC.1/DMS						X		
FDP_IFF.1/Cards				X				
FDP_IFF.1/DMS						X		
FDP_ITC.1		X						
FDP_RIP.1/FW	X				X			
FDP_RIP.1/UserData	X							
FDP_SDI.2	X							
FDP_SVR.1		X						
FIA_AFL.1			X					
FIA_SOS.1					X			
FIA_UAU.1			X					
FIA_UAU.5			X					

	SF.DATEN	SF.ANZEIGE	SF.I&A	SF.KARTEN	SF.MANAGE	SF.DMS	SF.TESTS	SM.SIEGEL
FIA_UAU.7			X					
FIA_UID.1			X					
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_MTD.1					X			
FMT_MTD.3					X			
FMT_SMF.1					X			
FMT_SMR.1			X					
FTA_SSL.3			X					
FTA_SSL.4			X					
FPT_STM.1				X				
FPT_PHP.1								X
FPT_TST.1							X	

Tabelle 18: Abdeckung der Sicherheitsanforderungen durch die Sicherheitsfunktionen

8 Anhang

8.0 Abkürzungen

AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria, siehe [CC]
C2C	Card-toCard-Authentifizierung
CT	Card Terminal
DMS	Data Management System (Primärsystem)
EAL	Evaluation Assurance Level
eGK	Elektronische Gesundheitskarte
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
EVG	Evaluierungsgegenstand
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
HBA	Heilberufsausweis
HPC	Health Professional Card (identisch HBA)
I & A	Identification and Authentication
KVK	KrankenVersichertenKarte
MobCT	Mobile Health Card Terminal
PIN	Persönliche Identifikationsnummer
PP	Protection Profile

RTC	Real Time Clock (Echtzeituhr)
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC	Secure Module Card (Institutskarte)
ST	Security Target
TOE	Target of Evaluation (siehe EVG)
TSF	TOE security functions / Sicherheitsfunktionen des Evaluationsgegenstandes
USB	Universal Serial Bus: Universelle Schnittstelle für Datenübertragung

8.1 Literaturverzeichnis

[CC_P1]	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012 Part 1: Introduction and general model
[CC_P2]	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012 Part 2: Security functional components
[CC_P3]	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012 Part 3: Security assurance components
[MobKT]	Gematik Dokument „Spezifikation Mobiles Kartenterminal“, Version 2.6 vom 17.06.2014
[PP_MobCT]	Common Criteria Protection Profile “Mobile Card Terminal for the German Healthcare System (MobCT)” / BSI-CC-PP-0052 Version 1.4 vom 24. September 2014, zertifiziert am 19.01.2015
[PP_suppl]	Supplement to BSI-CC-PP-0052, “Mobile Card Terminal for the German Healthcare System (MobCT): / Additional security functionality for physical protection” / BSI, Version 1.0.1 vom 25. September 2012
[PP_eHCT]	Common Criteria Protection Profile “Electronic Health Card Terminal (eHCT)” / BSI-CC-PP-0032 Version 3.5.1 vom 24. Juni 2015
[TR03120]	BSI – TR 03120 Sichere Kartenterminalidentität (Betriebskonzept), Version 1.0 vom 23.10.2007
[Crypto]	Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.2.0, 21.02.2014, gematik.
[manu]	Mobiles Kartenterminal für eGK und KVK, Bedienungsanleitung Version vom 27.07.2017, CCV Deutschland