Common-Criteria 3.1-Document

Security Target EAL3+ for G87-1505

Project Name:	G87-1505
Zertifizierung ID:	BSI-DSZ-CC-0513-V3
Document ID:	ASE _eHCB_1505
Version:	2.20
Status:	Final
Date:	19.06.2023
Prepared by:	Sebastian Schraml
Date/Signature:	19.06.2023
Checked by:	Sebastian Schraml
Date/Signature:	19.06.2023
Approved by:	Achim Pietig
Date/Signature :	19.06.2023

Cherry Digital Health GmbH
Cherrystraße 2
D-91275 Auerbach

History

15.12.2015	2.00	Revised regarding PP0032 V3.6	Jürgen Meier
22.04.2016	2.01	Secure PIN entry function added, Revised regarding OR v6, 2016-02-02	Jürgen Meier
13.12.2016	2.10	Adoption to PP0032, V3.7 and minor correction from OR v7	Jürgen Meier
21.02.2017	2.12	Revised regarding BSI comment (2017-01-20) and OR v8	Jürgen Meier
25.09.2017	2.13	Revised regarding BSI comments at ADV-Workshop (2017-07-17), TOE reference updated	Jürgen Meier
31.01.2018	2.14	TOE FW Version revised	Jürgen Meier
14.02.2018	2.15	Chapter 1.1 reworded, formatting errors in Chapter 6.1.1. corrected	Jürgen Meier
22.02.2018	2.16	Chapter 1.1, TOE description substantiated; Chapter 1.3, AGD information updated	Jürgen Meier
28.02.2018	2.17	AGD reference revised	Jürgen Meier
26.11.2022	2.18	add ECC support according to gemSpec_Krypt	Sebastian Schraml
22.02.2023	2.19	history shortened and add new Cipher Suites	Sebastian Schraml
19.06.2023	2.20	Update of firmware version	Sebastian Schraml

Distribution List

Name	Firma/Abteilung	Beschreibung
n.n.	TÜViT Essen	Evaluierung
n.n.	BSI	Zertifizierung
Sebastian Schraml	Cherry Digital Health GmbH	Engineering

Contents

1. ASE_INT.1 ST- Introduction

1.1 ST reference and TOE reference

Titel:	Security Target EAL3+ for G87-1505
Document Version:	2.20
Date:	19.06.2023
Document ID:	ASE _eHCB_1505
File name:	ASE_Security_Target_eHealth-Terminal_G87-1505-V219.docx
Author(s):	Sebastian Schraml
PP:	Protection Profile – Electronic Health Card Terminal (eHCT), Version 3.7 [18]
Zert. ID:	BSI-DSZ-CC-0513-V2

Target of Evaluation is the eHealth card keyboard of the series G87-1505 (TOE = Target of Evaluation) consisting of the software version 3.3.3 and the hardware with the version 1.1.1 of the manufacturer Cherry Digital Health GmbH.

The TOE version is 3.3.3:1.1.1. It consists of the firmware version and the hardware version in accordance with [19] and can be displayed by users request.
The TOE has different certified variants, e.g. due to different housing color.
The different variants can be identified by the part number of the TOE.
The following variants of the TOE are certified TOE versions

G87-1505LBZDE-2
G87-1505LBZDE-10

Every variant has the same TOE version 3.3.3:1.1.1.

AGD [5] describe in detail how the certified TOE version (3.3.3:1.1.1) can be identified by the user.

1.2 TOE Overview

The TOE described in this Security Target is the smart card keyboard *“G87-1505”* with integrated smart card readers. The TOE fulfills the requirements to be used with the German electronic Health Card (eHC) and the German Profession Card (HPC) based on the regulations of the German healthcare system. For further information about card compatibility, please see [14].
The TOE can be used as a secure PIN entry device for applications according to [22], which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.
The TOE signals whether the secure PIN entry mode is active or not by the display and by a red flashing LED beside the corresponding smartcard slots in case of a verification against an inserted smart card.
The TOE bases on the specification “Secure Interoperable ChipCard Terminal - SICCT” gematik - Spezifikation eHealth-Kartenterminal, Version 3.15.0, 16.05.2022
[15] extended and limited by the gematik- specification for the eHealth Terminal itself [14].

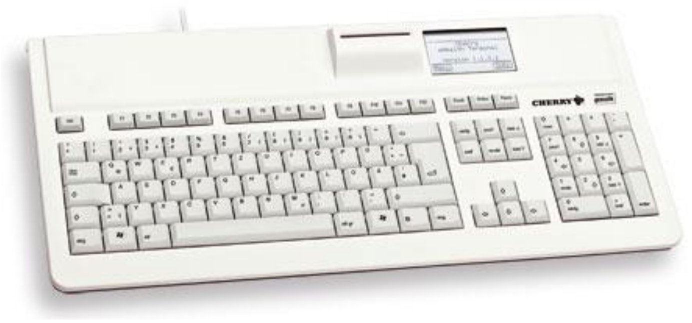


Figure 1: G87-1505

In its core functionality, the TOE is not different from any other smart card terminal which provides an interface to one or more smart cards including a mean to securely enter a PIN.
Additionally, the TOE provides an interface which allows routing the communication of a smart card to a remote IT product outside the TOE.
The G87-1505 does not provide a LAN- Interface for the communication with remote ITE. Separate software (Translating Proxy), which is not part of the TOE, secures the compatibility to communicate with other ITE over the LAN. The G87-1505 uses the LAN-Interface of the Host-PC for the communication. The Cherry Translating Proxy must be installed on the Host-PC for the communication with the so-called connector.
The TOE provides a PIN- Pad for secure PIN entry and a monochrome display (128x64 pixels) with backlight. Also, two ID-1 and two ID-000 contact units available for corresponding cards.
Both ID-1 card slots are equipped with two LED’s for the visualizing of the Secure PIN entry- Mode and the activation of a card. Both LED’s, a red one for Secure PIN entry and a green one to indicate card activity, of one ID-1 card slot directed to the surface of the TOE via one light conductor.

The TOE provides the following main functions:

- The access to one or more slots for smart cards
- Secure Network connectivity
- Secure PIN entry functionality
- Enforcement of the encryption of communication
- User authentification
- Management functionality including update and downgrade of Firmware, and
- Passive physical protection

The TOE use a SM-KT in form of a ID-000 card for cryptographic operation e.g. for authentication, integrity assurance and to ensure the confidentiality of data transmitted over the network interface. As physical characteristics of the SM-KT the TOE supports gSMC-KT cards.
IPv6 will be supported in addition to IPv4 by a firmware update.
The TOE uses the USB- Interface of the HOST-PC for power supply.

1.2.1 TOE major security features for operational use

One of the main security features of the TOE is the secure PIN entry functionality. It guarantees that an entered smartcard PIN which will be sent in plain text to the related smart card never leaves the TOE in plain text.
A further security function support this security function by ensuring that temporarily stored secrets, like a PIN, be deleted securely after its processing.
The TOE is also able to send/receive a PIN to/from a remote card terminal. This communication is routed via the connector. The connector never processes the PIN in clear text, as the authorized card (SM-KT) in the local and the remote card terminal are used to encrypt/decrypt the PIN. The TOE can be used as remote card terminal.
The TOE allows initiating batch signatures for the creation of more than one signature at a time without providing the PIN for each signature process. Batch signature is a functionality of the signing card.

The TOE uses the cryptographic functionality of a so-called SM-KT also to protect the communication between the TOE and other entities of a remote network e.g. the connector. A connector is a remote entity in the LAN which is necessary for the communication in the LAN of a medical supplier and for the communication with external Networks. Therefore, the TOE will use the cryptographic identity, in form of a X.509 certificate of the SM-KT and provide functionality for encryption/decryption as well as signature creation (see also [14]).
The SM-KT, in form of an ID-000 smart card, provides:

- Protection of the private key
- Cryptographic function based on RSA and ECC for encryption/decryption and signature creation
- A random number generator, and
- A function to read out the public key

More information about the SM-KT can be found in the corresponding Protection Profile and the corresponding gematik specification.
In addition to the cryptographic identity of the TOE, the TOE stores a shared secret which is generated by a connector and transferred to the TOE during the pairing process of the TOE and the connector. That shared secret is not stored on the SM-KT, but in a secure memory of the TOE. The whole identity of the TOE is therefore represented by the X.509 certificate and the shared secret.

The TOE provides functionality to update and downgrade its firmware. This includes both the change to a newer firmware as a downgrade to a firmware which is approved with the concept of firmware-group. The configuration data of the TOE, such as terminal type, IP address or pairing- information will be preserved and indicated by user request after a firmware update or a downgrade. (For details see [14]).
Firmware Update can only be triggered remotely over the SICCT- Interface by the connector or a specific software tool. Both options are implemented as push procedure as described in [14].

The TOE provides the possibility to manage different settings, including those above described update and downgrade of the firmware. An authorization mechanism ensures that only authorized user has the ability to use such security critical management functions.

An active tamper protection avoids physical manipulations of sensitive parts at operation conditions of the TOE. Also, different self-tests of the TOE ensure the integrity of different security functionalities.

1.2.2 TOE Type

The TOE is a keyboard with an integrated smart card terminal with secure PIN entry functionality which fulfils all necessary requirements for the use within the German telematics infrastructure.

1.2.3 Required non-TOE hardware/software/firmware

The below listed non-TOE software is required to communicate over the LAN- Interface of a Host-PC with the connector.

- eHealth USB-LAN Proxy V 4.0.0 or higher

The software is just a Translating Proxy which translates the USB communication protocol into the LAN communication protocol. The encryption/decryption of the communication will not be influenced by the software. It is still enforced by the TOE and will start and terminate in the TOE.
The software will be supported by the following operating systems:

- Microsoft Vista 32bit and 64bit or higher, including Windows Embedded 7
- Linux for x86 architecture 32bit and 64bit and for ARM architecture
  - Debian 5.0 or higher
  - Ubuntu 11.0 or higher
  - OpenSuSE 11.0 or higher
    supported kernel version 2.6.18 or higher
- Mac OS X 10.5 or higher

The following non-TOE software is required to use certain management functions of the TOE.

- eHealth Device Manager V 4.0.0 or higher

The software can be used amongst other things to administrate the TOE remotely or perform a software update of the TOE.
Furthermore, the following non-TOE hardware is required to operate the TOE:

- a SM-KT (Security Module - Kartenterminal) which represents the cryptographic identity of the TOE in form of a X.509 certificate. The TOE uses the random number generator of the SM-KT to generate cryptographic keys.
  Although this secure module is physically placed within the cage of the TOE it does not belong to the logical and physical scope of the TOE.
- a host system (Connector) which is necessary for a secure communication between the local network and the remote network of the telematics infrastructure.
- Local Area Network (LAN)
- A Host- PC with the above described Cherry Translating Proxy Software and with the following interfaces.
  - LAN Interface
  - USB Interface (Vers. 2.0 or higher)

The security function *SF.Secure_Communication* is only available after a SM-KT is installed because of the needed random number generator of the SM-KT.

1.3 TOE Description

The TOE consists of hardware and software with the major security feature to enter a PIN in a secure way and transfer this PIN securely to a card in one of the slots of the TOE.
In addition, the TOE provides the following security features to fulfill the requirements of the German health card system.

- secure communication,
- secure update function,
- management function,
- user authentication
- active tamper protection

The TOE comprises of the hardware with the version 1.1.1 which in form of a keyboard with smart card readers and the integrated software with the version 3.3.3.
The physical scope of the TOE comprises

- the hardware of the TOE within the sealed case with the following interfaces

  - USB- Interface (2.0), Type A / B
  - DC power supply interface
  - 2x ID-1 interfaces
  - 2x ID-000 interfaces
  - Display
  - Key matrix
- the integrated software, Version 3.3.3
- Quick Guide for Users (644-0649) [4]

The related Administrator Manual (644-0650) [5] is also into the scope of the TOE but it is not part of the physical delivered TOE. Both guidance, Quick Guide for Users and the Administrator Manual are available in electronic form; it can be downloaded at the Cherry web site www.cherry.de.
The integrity of the electronically delivered guidance documents is protected using SHA-256 checksum as stated at the Cherry website.

The physically delivered installation instruction contains information for users regarding the URL of the guidance documents for download.
Although, the SM-KT is physically within the cage of the TOE it does not belong into the scope of the TOE.
Seals are attached to the cage of the TOE allowing the user to detect whether the TOE has been tampered with. A description on how to check the sealing is part of the TOE guidance documentation.

The USB interface of the TOE is the physical and logical boundary of the TOE to the host system.
The logical scope of the TOE comprises the following security functions and is limited by the functionality for which the TOE relies on the services of the SM-KT, which is not part of the TOE.

Security function *SF.1_Secure_Communication*
The TOE provides a functionality to communicate with a so-called connector in a secure way. The communication path will be established after mutual authentication and is TLS 1.2 secured. The TOE supports the chipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
This security function uses the random number generator and the X.509 certificate of the SM-KT. So, this function is only available after the installation of the SM-KT and after successful pairing according to the gematik health card terminal specification [14].
This security function will be also used for secure communication for remote management of the TOE. In this case only unilateral authentication will be used.

Security function *SF.2 _Memory_Rework*
This security function guarantees that every information used by the TOE which is not necessary for the operation of the TOE like

- PINs
- cryptographic keys
- All information that is received by a card in a slot of the TOE or by the connector (except the shared secret)

will only be stored temporarily and secure deleted after the use.

Security function *SF.3_Secure_PIN_Entry*
The secure PIN entry mode can only be started by the TOE after receiving the corresponding SICCT command from the connector.
The state of secure PIN entry mode will be indicated to the user via the display and a flashing red LED beside the card slot (ID-1).
The TOE provides two different ways to enter the PIN between which the user can choose. The recommended option to enter the PIN is by the help of the arrow keys (left arrow, right arrow). Thereby,

numbers 0 to 9 are shown in the upper part of the display, with the active number marked. It is meant to use the arrow keys to select the appropriate number and confirm it with the enter key. The initial number marked is randomly chosen each time by the TOE.
Another option is to enter the PIN directly using the numeric key pad of the TOE.
The display will show for every entered number of the PIN a "*" at the display to inform the user that a number has been entered and how many numbers of the PIN have been actually entered. The PIN will never leave the TOE in plain text.

Security function *SF.4_Secure_Update*
The TOE provides a security function to update the integrated software of the TOE and to update the TSP-CA lists in a secure way.
The cryptographic functions SHA-256 and RSA with a key size of 2048bit will be used for hashing and signature verification.

Security function *SF.5_User _Authentication*
The TOE provides the following roles

- User
- Administrator
- TOE Reset Administrator

The access control mechanism requires a password for the user authentication. The following requirements will be preserved for the used password:

- Have a length of at least 8 characters,
- Be composed of at least the following characters: "0"-"9",
- Not contain the User ID/logon shall not be part of the password for the management interface,
- Not be displayed as clear text during entry

During the initial installation of the TOE, the administrator has to set an administrator password (PIN) and a PUK to perform a reset to factory defaults when the administrator login credentials are lost.

Security function *SF.6_TOE_Management*
This security function provides a mean to manage the TOE. The TOE provides a local management interface; a TLS secured remote management interface and a management over SICCT- Interface.
The following management functions can be executed by all roles

- *Display the product version number of the TOE*
- *Manage own login credentials*
- *View card terminal name of card terminal*
- *Display the MAC-address of the TOEs network interface*
- *Perform a TOE self-test*
- *View serial number of the TOE*

Only authorized administrator can use the following management functions

- *Manage the available network configuration*
- *Set card terminal name for card terminal*
- *Manage local and remote management login credentials*
- *Secure deletion of pairing information from all three possible pairing processes (initial pairing, review of pairing-information and maintenance-pairing)*
- *Manage the list of TSP CAs*
- *Perform a firmware update*
- *Enable/disable the remote management interface*
- *Reset the TOE to factory defaults*
- *Enable/disable reset to factory defaults without user authentication*
- *Perform the possible pairing process with the connector*
- *Enable/disable administrative SICCT commands (e.g. perform firmware update)*

The following management function is executable by authenticated TOE administrators using the SICCT Interface:

- Perform a firmware update

- Perform a TSP CA list update

The following management functions are executable only by authenticated TOE administrators using the local management interface:

- Enable/disable the remote management interface
- Perform the possible pairing processes with the connector
- Enable/disable reset to factory defaults without user authentication
- Enable/Disable administrative SICCT commands (e.g. perform firmware update)
- Reset to factory defaults

The following management functions are executable only by authenticated TOE administrators using the remote management interface (Web interface)

- Manage remote management login credentials (for the Web interface)
- Manage remote management login credentials (for the SICCT interface)

The security function ensures that only secure values allowed and by default security relevant settings are disabled after initial start-up.

The following management functions are by default disabled after initial start-up.

- Remote management interface
- Remote firmware update functionality
- Reset to default settings without authentication

The following management function is executable only by authenticated TOE Reset administrators using the local management interface:

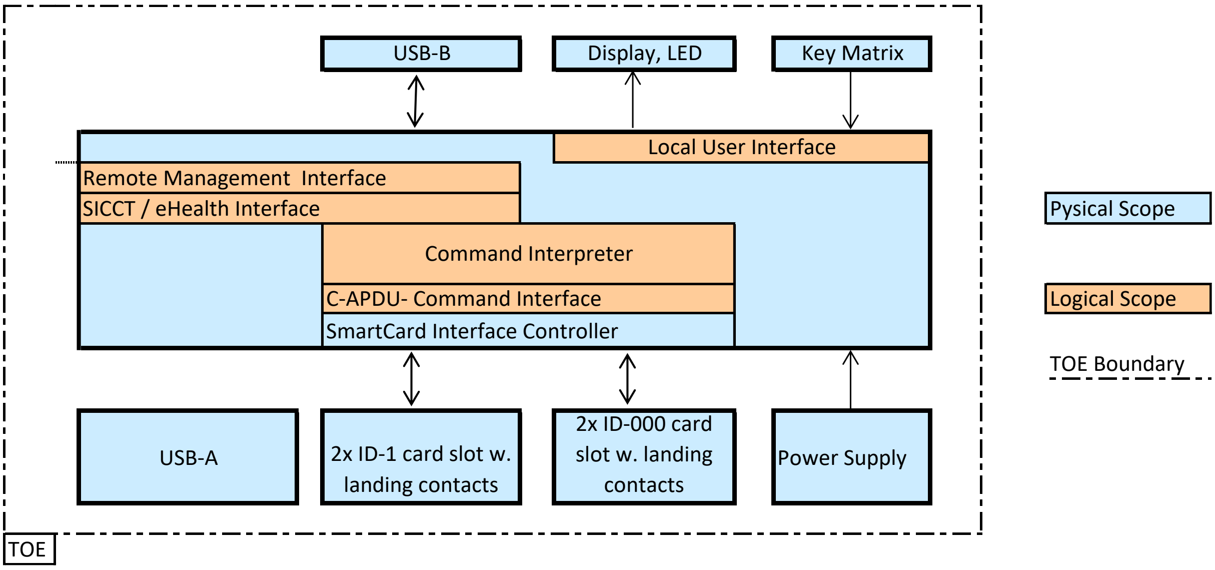
- Reset to factory defaults (fallback)

The management function "reset to factory defaults" can be executed by users without authentication but it is organizational reserved for authenticated administrator only. [5]

Security function *SF.7_Protection_against_Counterfeiting*

The security function SF.7_Protection_against_Counterfeiting provides a mean to detect the physical tampering of non-visible surfaces of the TOE. Physical tampering of those parts leads to a notification of the user and the TOE will be set into a secure state.
The TSF does also enforce a number of Self-test to ensure the integrity of security functions.

The drawing below shows the physical and logical scope of the TOE in a manner to illustrate the security functionality of the TOE in the context of the provided interfaces and the TOE boundary as described in this chapter.


USB-B
Display, LED
Key Matrix
Local User Interface
Remote Management Interface
SICCT / eHealth Interface
Command Interpreter
C-APDU- Command Interface
SmartCard Interface Controller
USB-A
2x ID-1 card slot w. landing contacts
2x ID-000 card slot w. landing contacts
Power Supply
Pysical Scope
Logical Scope
TOE Boundary
TOE

Picture 1: Physical and logical Scope of the TOE

2. ASE_CCL Conformance Claims

2.1 Common Criteria Conformance Claim

This Security Target and the TOE claim conformance to

- Common Criteria for Information technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, 2017 [1]

- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, 2017 [2]

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, 2017 [3]

Conformance is claimed for Part 2 conformant and Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, 2017

has to be taken into account.

2.2 PP Claim

This Security Target claims strict conformance to the Common Criteria Protection Profile “Electronic Health Card Terminal (eHCT)”, BSI-CC_PP_0032-V3-2016; Version 3.7, 21th September 2016.

2.3 Package Claim

The assurance level for the TOE is EAL 3 augmented by the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA.VAN.4.

§15 SigV, Abs. 4 definiert:
Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

Because of the TOE security measure SM.1 (sealing) manipulation will be visible for the user.
Additionally, the security function SF.7_Protection_against_Counterfeiting guarantees the detection of attacks at non-visible areas of the TOE and leads to locking of the TOE. Only the manufacturer can unlock the TOE.
Furthermore, this security function checks the integrity of the Firmware during every start-up of the TOE and informs the user about security relevant changes.

2.4 Conformance Claim with Technical Directives of the BSI

The Security Target based on the requirements of BSI TR-03120 [16] regarding sealing and physical protection of the TOE housing.

3. ASE_SPD – Security Problem Definition

This chapter describes:

- The **assets** which have to be protected by the TOE.
- The **subjects** which are interacting with the TOE.
- The **threats** which exist against the assets of the TOE
- The **organisational security policies** the TOE has to comply to.
- The **assumptions** which have to be made about the environment of the TOE.

3.1 Assets

The following assets need to be protected by the TOE and its environment:

Asset	Description
Card PIN (short PIN)	The TOE interacts with the user to acquire a PIN and sends this PIN to one of the cards in a slot of the TOE. The TOE has to ensure the confidentiality of the PIN. For remote-PIN verification the TOE sends/receives the PIN to/from another card terminal via the connector. This asset is user data.
Management credentials	The TOE stores credentials (e.g. passwords) to authenticate TOE administrators for management activities. The TOE has to ensure the confidentiality and integrity of these credentials. This asset is user data.
Shared secret	The TOE stores a shared secret which is generated by the connector during the initial pairing process. The shared secret and the SM-KT represent the identity of the card terminal. This identity is used for secure identification and authentication of the card terminal by the connector. The TOE has to ensure the confidentiality and integrity of the shared secret. This asset is TSF data.
Patient Data	This data comprises health information and billing data that is related to patients. The TOE gets patient data from the cards in its slots, encrypts this data and sends it to the connector. Further the TOE accepts patient data from the connector, decrypts it, and sends it to the corresponding eHC in its slot. The TOE has to ensure the confidentiality and authenticity of this data. This asset is user data.
Communication data	Confidential data that is transmitted between the TOE and the connector. This data comprises at least patient data and PINs for remote-PIN verification. The TOE has to ensure the confidentiality and authenticity of this data. This asset is user data.[1]
Configuration data	Data on which the TOE relies on for its secure operation. This data comprises - management credentials for local and remote management - the list of TSP CAs. The TOE has to ensure the integrity, confidentiality and authenticity of the management credentials. It has to ensure integrity and authenticity of the list of TSP CAs. This asset is user data.[2]
TSF Data	The TOE stores TSF data which is necessary for its own operation. TSF data comprises the following data:[3] - Shared secret - cryptographics keys - TOE software - TSP-CA list - firmware group list The TOE has to ensure the confidentiality and authenticity of this data. This asset is TSF data.

[1] No further Communication Data has been specified by the ST author

[2] No further Configuration data has been specified by the ST author

[3] This data has been specified as TSF Data by the ST author

Table 1: Assets

3.2 Subjects

The following subjects are interacting with the TOE:

Subject	Description
TOE Administrator	The TOE administrator is in charge of managing the security functions of the TOE.
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 application sensitive information. The attacker has a moderate level attack potential.
Authorized card	Authorized cards (HPC, SMC-B) are able to perform card-to-card authentication which is used for remote-PIN verification.
Card	The TOE is handling the communication for one or more smart cards in its card slots.
Connector	The connector is the only entity in the environment of the TOE (except for users of the management interface) which is foreseen to communicate with the TOE. It is the interface for the TOE to securely communicate with the telematic infrastructure of the German healthcare system.
Medical supplier	The medical supplier (e.g. a physician) uses the TOE together with his HPC (or SMC-B). With the HPC it is also possible for medical suppliers to generate qualified digital signatures. Other than the patient the medical supplier can be held responsible for the secure operation of the TOE.
Patient	The patient uses the TOE together with his eHC. The patient uses the TOE for other services of the eHC. A patient will never use the services of the TOE alone but will always be guided by the medical supplier.
Push Server	The Push Server is a trusted entity in the internal network of the medical supplier which updates firmware on card terminals that are connected to that network. The Push Server uses the SICCT interface or another network interface of the card terminal for remote update. See A.PUSH_SERVER for assumptions on the Push Server.
SM-KT	The SM-KT represents the cryptographic identity of the TOE. It is a secure module that carries a X509 certificate and provides: • Protection of the private key • Cryptographic functions for encryption / decryption and signature creation • A random number generator • A function to read out the public key
TOE Reset Administrator	The TOE Reset Administrator is the only user role that is able to perform a reset of the TOE settings when management credentials are lost. The type of authentication for this role depends on the particular implementation. The TOE Reset Administrator could be the developer himself.
User	A user is communicating with the TOE in order to use its primary services, i.e. to access a smart card which has been put into one of the slots of the TOE before. The TOE is used by different kinds of users including medical suppliers, patients and administrators.

Table 2: Subjects

3.3 Threats

This chapter describes the threats that have to be countered by the TOE.

The attack potential of the attacker behind those threats is in general characterized in terms of their motivation, expertise and the available resources.

As the TOE handles and stores information with a very high need for protection with respect to their authenticity, integrity and confidentiality it has to be assumed that an attacker will have a high motivation for their attacks.

On the other hand the possibilities for an attacker are limited by the characteristics of the controlled environment (specifically addressed by A.ENV).

Summarizing this means that an attacker with a moderate attack potential has to be assumed. The assets that are threatened and the path for each threat are defined in the following table:

Threat	Description
T.COM	An attacker may try to intercept the communication between the TOE and the connector in order to gain knowledge about communication data which is transmitted between the TOE and the connector or in order to manipulate this communication. As part of this threat an authorized user, who is communicating with the TOE (via a connector) could try to influence communications of other users with the TOE in order to manipulate this communication or to gain knowledge about the transmitted data.
T.PIN	An attacker may try to release the PIN which has been entered by a user from the TOE in clear text. As part of this attack the attacker may try to route a PIN, which has been entered by a user, to a wrong card slot.
T.DATA	An attacker may try to release or modify protected data from the TOE. This data may comprise: • Configuration data the TOE relies on for its secure operation • The shared secret of TOE and connector • Communication data that is received from a card and stored within the terminal before it is submitted to the connector An attack path for this threat cannot be limited to any specific scenario but includes any scenario that is possible in the assumed environment of the TOE. Specifically an attacker may • use any interface that is provided by the TOE • physically probe or manipulate the TOE
T.F-CONNECTOR	Unauthorized personnel may try to initiate a pairing process with a fake connector after an unauthorized reset to factory defaults, e.g. to initiate an unauthorized firmware update or to receive confidential (patient) data.

Table 3: Threats

3.4 Organisational Security Policies

The TOE shall be implemented according to the following specifications:

Policy	Description
OSP.PIN ENTRY	The TOE shall fulfill the requirements to be used as a secure PIN pad entry device for applications according to [21] . This specifically means that a PIN, which has been entered by a user at the TOE must never leave the TOE in clear text, except to smart cards in local card slots. For the case that a terminal implements an insecure mode (e.g. a mode, in which it cannot be guaranteed that the PIN will not leave the TOE or a mode in which not trustworthy entities are allowed to communicate with the TOE) the TOE has to be able to inform the medical supplier whether it is currently in a secure state or not.

Table 4: Organizational Security Policies

3.5 Assumptions

The following assumptions need to be made about the environment of the TOE to allow the secure operation of the TOE.

Assumption	Description
A.ENV	It is assumed that the TOE is used in a controlled environment. Specifically it is assumed: • The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible, • That the user handles his PIN with care; specifically that the user will keep their PIN secret, • That the user can enter the PIN in a way that nobody else can read it, • That the user only enters the card PIN when the TOE indicates a secure state, • That the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used, • That the network of the medical supplier is appropriately secured so that authorized entities are trustworthy, see also [13].
A.ADMIN	The administrator of the TOE and the medical supplier shall be non-hostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier shall be responsible for the secure operation of the TOE. Specifically it shall be ensured: • That they enforce the requirements on the environment (see A.ENV), • That the administrator ensures that the medical supplier received the necessary guidance documents (especially for firmware updates), • That the physical examination of the TOE is performed according to the process described by the manufacturer in the evaluation process (e.g. seal checking), • That the administrator checks the integrity of the terminal before the initial start-up procedure (every new pairing process) and the medical supplier checks the integrity of the terminal before every start-up procedure, • That they react to breaches of environmental requirements according to the process described by the manufacturer in the evaluation process (e.g. reshipment to the manufacturer).
A.CONNECTOR	The connector in the environment is assumed to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for

Assumption	Description
	a mutual authentication. It is assumed that the connector has undergone an evaluation and certification process in compliance with the corresponding Protection Profiles [13]. Further it is assumed that for the case the TOE uses a DF.KT of a gSMC-KT as SM-KT which are addressable via the connector, the TOE accesses this DF.KT via the base-channel 0. During the use of the SM-KT by the TOE the terminal card commands of the TOE have to be given precedence and the processing of possibly existing client SICCT commands has to be interrupted and continued only after completion of the internal command sequence. Therefore, the TOE queue the interrupts internally.[4] It is also assumed that the connector makes sure that a DF.KT of a gSMC-KT as SM-KT which is addressable via the connector can only be accessed by the TOE and cannot be used by any other system than the TOE. Further, it is assumed that the connector periodically monitors the pairing state with the TOE and provides warning mechanisms to indicate unexpected results like paired terminals which lack the shared secret.
A.SM	The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate. It is assumed that the cryptographic keys in this module are of sufficient quality and the process of key generation and certificate generation is appropriately secured to ensure the confidentiality, authenticity and integrity of the private key and the authenticity and integrity of the public key/certificate. The random number generator of the SM-KT is assumed to provide entropy of at least 100 bit for key generation. It is further assumed that the secure module is secured in a way that protects the communication between the TOE and the module from eavesdropping and manipulation and that the SM-KT is securely connected with the TOE (according to TR-03120 [16] and its appendix [17]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [12] and complies with the specification [20].
A.PUSH_SERVER	It is assumed that the internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [14]. The TOE administrator is assumed to be responsible for the operation of the Push Server and able to select the particular firmware version that the server is allowed to install on the card terminals. It is further assumed that every time an update process is performed for a card terminal the Push Server logs the following information: identifier of involved card terminal, version of firmware to install, result of the update process.
A.ID000_CARDS	It is assumed that all smartcards of form factor ID000 are properly sealed after they are brought into the TOE. Further, the developer is assumed to provide guidance documentation on how a TOE administrator could renew a sealing after an ID000 card is replaced by another one.

Table 5: Assumptions

[4] Sentence has been uniquely defined by the ST Author

4. ASE_OBJ - Security Objectives

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

4.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE

Objective	Description
O.ACCESS_CONTROL	To protect the configuration of the TOE against unauthorized modifications only an authorized user shall be able to read out information about the current configuration of the TOE and only the administrator shall be able to modify the settings of the TOE. Therefore the TOE shall provide an access control function based on the identity of the current user. Further the access control mechanism of the TOE has to ensure that the PIN cannot be read from the TOE. The TOE shall also ensure that the TOE administrator's credentials for local management are set before access to other TOE functionality is possible.
O.PIN_ENTRY	The TOE shall serve as a secure pin entry device for the user and the administrator. Thus the TOE has to provide the user and administrator with the functionality to enter a PIN and ensure that the PIN is never released from the TOE in clear text, except to smart cards in each addressed local card slot. For remote-PIN verification the PIN shall be encrypted, by local gSMC-KT, controlled by the Connector, so that it can only be decrypted by the receiving smart card (HPC or SMC-B).
O.I&A	For its access control policy and for parts of the management functionality the TOE has to be aware of the identity of the current user. Thus the TOE has to provide a mean to identify and authenticate the current user. The TOE shall maintain at least three distinct roles: administrators, the TOE Reset Administrator and users[5].

[5] It should be noted that the scope of the identification of the user is only to determine the role the current user belongs to.

Objective	Description
O.MANAGEMENT	In order to protect its configuration the TOE shall provide only an authenticated and authorized administrator with the necessary management functions. The TOE shall enforce an access control policy for management functions, as some functions shall only be accessible by administrators authenticated by the local management interface. Further, the following management functions can be used by unauthenticated users. • Display the product version number of the TOE • View card terminal name for card terminal The TOE shall provide a local management interface and management over SICCT interface. A firmware consists of two parts: (1) the so-called “firmware list” and (2) 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. A firmware update of the TOE shall only be possible after the integrity and authenticity of the firmware has been verified and the following holds: • The TOE provides functionality to update and downgrade its firmware. This includes both the change to a newer firmware as a downgrade to a firmware which is approved with the concept of firmware-group. • The configuration, such as terminal type, IP address or pairing-information shall be preserved and indicated after a firmware update or a downgrade (see [14] for further information). • The developer of the TOE shall ensure that in case of a downgrade of the firmware the TOE must warn the Administrator (e.g. within the Guidance) before the installation that the action to be performed is not an upgrade. The TOE must offer a chance to cancel the installation. The developer- specific update component shall warn the administrator about taking the responsibility in case of performing a downgrade. The administrator shall be able to manage the list of TSP CAs which is used to verify the authenticity of connectors. An update of the TSP CA list shall only be possible after the integrity and authenticity of the list has been verified. The TOE shall ensure that for all security attributes, which can be changed by an administrator or the user, only secure values are accepted. This includes the enforcement of a password policy for the management interfaces. In addition to the developer-specific update component the TOE supports update features of the SICCT specification, whereby a trigger component is able to update the TOE (e.g. the Configuration and Software Repository- Service (KSR) of the telematic infrastructure).
O.SECURE_CHANNEL	When establishing a connection between the TOE and the connector both parties shall be aware of the identity of their communication partner. Thus the TOE has to provide a mean to authenticate the connector and to authenticate itself against the connector in accordance with [14]. The TOE in each security context shall only have one connection to one connector at a time. For all communications which fall into the context of the electronic health card application the TOE shall only accept communication via this secure channel to ensure the integrity, authenticity and confidentiality of the transmitted data.

Objective	Description
	Only functions to identify the TOE in the network (service discovery) shall[6] be available without a secure channel.
O.STATE	The TOE does not realize additional functionality which doesn't fall into the scope of the certified TOE (e.g. value-added modules). However, the TOE ensures the indication of the secure PIN entry mode to the user if it is activated. Also when the TOE has established a secure connection to a connector the secure state of the connection will be indicated to the user.[7]
O.PROTECTION	The TOE shall be able to verify the correct operation of the TSF. To ensure the correct operation of the TSF the TOE shall verify the correct operation of all security functions at start-up and specifically verify the correct operation of the secure module (see A.SM). The TOE shall provide an adequate level of physical protection to protect the stored assets and the SM-KT[8]. It has to be ensured that any kind of physical tampering that might compromise the TOE Security Policy within 10 minutes can be afterwards detected by the medical supplier. To avoid interference the TOE has to ensure that each connection is held in its own security context where more than one connection of a TOE to a connector is established. Also if more than one smart card in the slots of the TOE is in use the TOE has to ensure that each connection is held in its own security context. The TOE shall delete • PINs, • Cryptographic keys, and • All information that is received by a card in a slot of the TOE or by the connector (except the shared secret) in a secure way when it is no longer used. In case a TOE comprises physically separated parts, the TOE shall prevent the disclosure and modification of data when it is transmitted between physically separated parts of the TOE.

Table 6: Security Objectives for the TOE

4.2 Security Objectives for the Environment

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

Objective	Description
OE.ENV	It is assumed that the TOE is used in a controlled environment. Specifically it is assumed: • The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible, • That the user handles his PIN with care; specifically that the user will keep their PIN secret, • That the user can enter the PIN in a way that nobody else can read it,

[6] The ST author has replaced the wording "may" by the wording "shall"

[7] Objective "O.State" completely revised and uniquely defined by the ST author

[8] Please note that the SM-KT provides its own physical protection for the stored keys. However according to [14] it has to be ensured that the SM-KT is securely connected with the TOE. Thus the physical protection provided by the TOE has to cover the SM-KT.

Objective	Description
	• That the user only enters the card PIN when the TOE indicates a secure state, • That the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used, • The medical supplier sends the TOE back to the manufacturer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel, and • That the network of the medical supplier is appropriately secured so authorized entities are trustworthy, so also [13].
OE.ADMIN	The administrator of the TOE and the medical supplier shall be non-hostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier shall be responsible for the secure operation of the TOE. Specifically it shall be ensured: • That they enforce the requirements on the environment (see A.ENV), • That the administrator ensures that the medical supplier received the necessary guidance documents (especially for firmware updates), • That the physical examination of the TOE is performed according to the process described by the manufacturer in the evaluation process (e.g. seal checking), • That the administrator checks the integrity of the terminal before the initial start-up procedure (every new pairing process) and the medical supplier checks the integrity of the terminal before every start-up procedure, • That they react to breaches of environmental requirements according to the process described by the manufacturer (e.g. reshipment to the manufacturer) and • That the administrator checks the secure state of the TOE regularly[9].
OE.CONNECTOR	The connector in the environment has to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication. The connector has to undergo an evaluation and certification process in compliance with the corresponding Protection Profiles [13]. Further the connector has to periodically check the pairing state with the TOE and warn the administrator accordingly.
OE.SM	The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate. It is assumed that the cryptographic keys in this module are of sufficient quality and the process of key generation and certificate generation is appropriately secured to ensure the confidentiality, authenticity and integrity of the private key and the authenticity and integrity of the public key/certificate. The random number generator of the SM-KT shall provide entropy of at least 100 bit for key generation. It is further assumed that the secure module is secured in a way that protects the communication between the TOE and the module from eavesdropping and manipulation and that the SM-KT is securely connected with the TOE (according to TR-03120 [16] and its appendix [17]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [12] and complies with the specification [20].

[9] The secure state can be indicated by e.g. the pairing information with the connector, the firmware version or other security events which the developer has to define within the Guidance documentation.

Objective	Description
OE.PUSH_SERVER	The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [14]. The TOE administrator is responsible for the operation of the Push Server and able to select the particular firmware version that the server is allowed to install on the card terminals. Every time an update process is performed for a card terminal the push server logs the following information: identifier of involved card terminal, version of firmware to install, result of the update process.
OE.ID000_CARDS	All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE. Further, the developer shall provide guidance documentation on how a TOE administrator could renew a sealing after an ID000 card is replaced by another one.

Table 7: Security Objectives for the environment of the TOE

4.3 Security Objectives Rationale

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

	O.ACCESS_CONTROL	**O.PIN_ENTRY**	**O.I&A**	**O.MANAGEMENT**	**O.SECURE_CHANNEL**	**O.STATE**	**O.PROTECTION**	**OE.ENV**	**OE.ADMIN**	**OE.CONNECTOR**	**OE.SM**	**OE.PUSH_SERVER**	**OE.ID000_CARDS**
T.COM			**X**		**X**		**X**	**X**					
T.PIN	**X**	**X**					**X**	**X**					
T.DATA	**X**		**X**	**X**			**X**	**X**					
T.F-CONNECTOR								**X**	**X**	**X**			
OSP.PIN_ENTRY		**X**				**X**	**X**						
A.ENV								**X**					
A.ADMIN									**X**				
A.CONNECTOR										**X**			
A.SM											**X**		
A.PUSH_SERVER												**X**	
A.ID000_CARDS													**X**

4.3.1 Countering the Threats

The threat **T.COM** which describes that an attacker may try to intercept the communication between the TOE and the connector is countered by a combination of the objectives *O.I&A, O.SECURE_CHANNEL* and *O.PROTECTION. O.SECURE_CHANNEL* describes the secure channel, which is used to protect the communication between the TOE and the connector. This objective basically ensures that an attacker is not able to intercept the communication between the TOE and the connector and removes this threat since both parties have to be aware of the identity of their communication partner. *O.I&A* requires that the TOE has to be able to authenticate the connector. This authentication is part of the establishment of the secure communication between the TOE and the connector and contributes to removing the threat. *O.PROTECTION* ensures that each communication of the TOE with a connector or cards in its slots is held in a separate security context so that authorized users of the TOE can't influence the communication of other users. It further protects the TOE against physical tampering for 10 minutes. *OE.ENV* finally ensures that the network of the medical supplier is appropriately secured so that it cannot be accessed by unauthorized entities and that the TOE is protected against physical tampering if the TOE is unobserved for more than 10 minutes. Furthermore *OE.ENV* assures that the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used.

The threat **T.PIN**, which describes that an attacker may try to release the PIN from the TOE, is countered by a combination of the objectives *O.ACCESS_CONTROL, O.PIN_ENTRY* and *O.PROTECTION. O.ACCESS_CONTROL* defines that according to the access control policy of the TOE nobody must be allowed to read out the PIN. In this way it can be ensured that an attacker cannot read out the PIN via one of the logical interfaces of the TOE *O.PIN_ENTRY* defines that the TOE shall serve as a secure pin entry device for the user and the TOE administrator and contributes to countering T.PIN as it ensures that the PIN cannot be released from the TOE in clear text. This is the main objective that serves to remove the threat. *O.PROTECTION* contributes to countering T.PIN as it ensures that the TOE provides an adequate level of physical protection for the PIN for 10 minutes. It further protects the PIN when it is transmitted between physically separated parts, ensures that the PIN is securely deleted when it is no longer used and ensures that the PIN is sent to the correct card as the communication to every card slot is held in a separate context. *OE.ENV* finally ensures that that the network of the medical supplier is appropriately secured so that it cannot be accessed by unauthorized entities. The TOE is protected against physical tampering if it is unobserved for more than 10 minutes and that the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used. Furthermore *OE.ENV* contributes to countering T.PIN by ascertaining that the user enters the PIN in a way that nobody else can read it and that this can only be done when the TOE indicates a secure state.

The threat **T.DATA**, which describes that an attacker may try to release or change protected data of the TOE, is countered by a combination of *O.ACCESS_CONTROL, O.I&A, O.MANAGEMENT* and *O.PROTECTION. O.ACCESS_CONTROL* ensures that only authorized users are able to access the data stored in the TOE. *O.I&A* authenticates the user as the access control mechanism will need to know about the role of the user for every decision in the context of access control. *O.MANAGEMENT* ensures that only the TOE administrator is able to manage the TSF data and removes the aspect of the threat where an attacker could try to access sensitive data of the TOE via its management interface. *O.PROTECTION* provides the necessary physical protection for the data stored in the TOE for 10 minutes and defines additional mechanisms to ensure that secret data cannot be released from the TOE (delete secret data in a secure way keep communication channels separate and protect data when transmitted between physically separated parts of the TOE). *OE.ENV* finally ensures that the network of the medical supplier is appropriately secured so that it cannot be accessed by unauthorized entities and that the TOE is protected against physical tampering if the TOE is unobserved for more than 10 minutes. Furthermore *OE.ENV* assures that the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used and that the user only enters the card PIN when the TOE indicates a secure state.

The threat **T.F-CONNECTOR,** which describes that unauthorized personnel may try to initiate a pairing process with a fake connector after an unauthorized reset to factory defaults, is countered by a combination of *OE.ENV*, *OE.ADMIN* and *OE.CONNECTOR*. *OE.ENV* ensures that the medical supplier sends the TOE back to the developer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel. *OE.ADMIN* ensures that the administrator checks the secure state of the TOE regularly before it is used. *OE.CONNECTOR* ensures that the connector in the environment is trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication. It further ensures that the connector has to undergo an evaluation and certification process in compliance with the corresponding Protection Profiles. *OE.CONNECTOR* further ensures that the connector periodically checks the pairing state with the TOE and warns the administrator accordingly.

4.3.2 Covering the OSPs

The organizational security policy **OSP.PIN_ENTRY** requires that the TOE has to serve as a secure pin entry device (i.e. that the PIN can never be released from the TOE) and that the TOE has to be able to indicate whether it is working in a secure state or not.

The secure pin entry device is specified in *O.PIN_ENTRY.* This objective defines that the TOE has to provide a function for secure PIN entry and (in case of a card PIN) that the TOE will inform the user to which card slot the PIN will be sent. *O.STATE* ensures that the TOE is able to indicate to the medical supplier, whether it is currently working in a secure state as required by OSP.PIN_ENTRY. Such a secure state includes (but is not limited to) that the secure PIN entry can be guaranteed. Finally *O.PROTECTION* ensures that the TOE is able to verify the correct operation of the TSF and that an adequate level of physical protection is provided.

4.3.3 Covering the Assumptions

The assumption **A.ENV** is covered by *OE.ENV* as directly follows.
The assumption **A.ADMIN** is covered by *OE.ADMIN* as directly follows.
The assumption **A.CONNECTOR** is covered by *OE.CONNECTOR* as directly follows.
The assumption **A.SM** is covered by *OE.SM* as directly follows.
The assumption **A.PUSH_SERVER** is covered by *OE.PUSH_SERVER* as directly follows.
The assumption **A.ID000_CARDS** is covered by *OE.ID000_CARDS* as directly follows.

5. ASE_ECD - Extended Components Definition

This Security Target uses no components which are not defined in CC part 2.

6. ASE_REQ - Security Requirements

This chapter defines the functional requirements and the security assurance requirements for the TOE and its environment.
Operations for assignment, selection, refinement and iteration have been made.
All operations which have been performed from the original text of [2] are written in *italics* for assignments, underlined for selections and **bold** text for refinements. Selectable assignments are written in *italics and underlined*. Furthermore the [brackets] from [2] are kept in the text.

6.1 Security Functional Requirements for the TOE

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

Cryptographic Support (FCS)	
FCS_CKM.1/Connector	Cryptographic key generation for connector communication
FCS_CKM.1/Management	Cryptographic key generation for remote management
FCS_CKM.4	Cryptographic key destruction for connector communication
FCS_COP.1/Con_Sym	Cryptographic operation for connector communication (symmetric algorithm)
FCS_COP.1/SIG	Cryptographic operation for signature generation/verification
FCS_COP.1/Management	Cryptographic operation for remote management
FCS_COP.1/SIG_FW	Cryptographic operation for firmware signature verification
FCS_COP.1/SIG_TSP	Cryptographic operation for signature verification of TSP CA lists
User data protection (FDP)	
FDP_ACC.1/Terminal	Subset access control for terminal functions
FDP_ACC.1/Management	Subset access control for management
FDP_ACF.1/Terminal	Security attribute based access control for terminal functions
FDP_ACF.1/Management	Security attribute based access control for management
FDP_IFC.1/PIN	Subset information flow control for PIN
FDP_IFF.1/PIN	Simple security attributes for PIN
FDP_IFC.1/NET	Subset information flow control for network connections
FDP_IFF.1/NET	Simple security attributes for network connections
FDP_RIP.1	Subset residual information protection
Identification and Authentication (FIA)	
FIA.AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1/Management	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification

Security Management(FMT)	
FMT_MSA.1/Terminal	Management of security attributes for terminal SFP
FMT_MSA.1/Management	Management of security attributes for management SFP
FMT_MSA.2	Secure security attributes
FMT_MSA.3/Terminal	Static attribute initialisation for terminal SFP
FMT_MSA.3/Management	Static attribute initialisation for management SFP
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Protection of the TSF(FPT)	
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.2[10]	Notification of physical attack
FPT_TST.1	TSF testing
TOE Access(FTA)	
FTA_TAB.1/SEC_STATE	Default TOE access banners for secure state
Trusted path/channels(FTP)	
FTP_ITC.1/Connector	Inter-TSF trusted channel for connector communication
FTP_TRP.1/Management	Trusted path for remote management

Table 8: Security Functional Requirements for the TOE

[10] SFR has been added by the ST author

6.1.1 Cryptographic Support (FCS)

6.1.1.1 FCS_CKM.1 Connector Cryptographic key generation for connector communication

FCS_CKM.1.1/ Connector

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*TLS 1.2, cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, HMAC-SHA1 and TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1*] and specified cryptographic key sizes *[AES: 128bit, 256bit, HMAC-SHA1: 160bit*] that meet the following: [*[14],***[23]**]

Hierarchical to: No other components.

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

Application Note 1: The cryptographic session keys, generated by FCS_CKM.1/Connector shall be used for the TLS encryption/decryption between the TOE and the connector (for further information see [14] also chapter 6.1.1.4). The generation (actually negotiation) of this key shall be done in accordance with the Diffie-Hellman protocol.
It should be noted that this negotiation includes a mutual authentication of the TOE and the connector based on certificate validation (see [14]) and validation of a shared secret. The TOE shall determine the role from the connector certificate presented during the buildup of the TLS connection. The TOE shall check that the determined role corresponds with the role "Signature Application Component (SAC)" (see [14]).
The TOE shall use the SM-KT for Random Number generation and Signature generation (see also A.SM) and its own functionality for Signature Verification required by FCS_COP.1/SIG.[11]
The connection to network based management interfaces shall always be secured with TLS Version 1.2.

[11] Sentence has been uniquely defined by the ST Author to clarify product specific implementations

6.1.1.2 FCS_CKM.1 Management Cryptographic key generation for remote Management

FCS_CKM.1.1/ Management

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [T*LS 1.2, cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, HMAC-SHA1 and TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1*] and specified cryptographic key sizes [*AES 128bit, 256bit, HMAC-SHA1: 160bit*] that meet the following:[*[14],***[23]**]

Hierarchical to: No other components

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

Application Note 2:
The cryptographic session keys, generated by FCS_CKM.1/Management shall be used for the TLS encryption/decryption for remote management (for further information see [14] (see also chapter 6.1.1.6). The generation (actually negotiation) of this key shall be done in accordance with the TLS handshake protocol (for further information see [9]), extended and limited by [14].
The TOE should use the functionality of the SM-KT for random number generation. Note, that the SM-KT is physically integrated into the TOE in the evaluated TOE configuration.
The connection to network based management interfaces shall always be secured with TLS Version 1.2.
This SFR can implicitly be fulfilled by the mechanisms for cryptographically secured communication with the connector.

6.1.1.3 FCS_CKM.4 Cryptographic key destruction for communication

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting the key value with zero values*] that meets the following:
[*none*]

Hierarchical to: No other component.

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

6.1.1.4 FCS_COP.1/Con_Sym Cryptographic operation for connector communication (symmetric algorithm)

FCS_COP.1.1/ Con_Sym The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-CBC with HMAC-SHA1*] and cryptographic key sizes [*AES-CBC: 128 bit, 256 bit; HMAC-SHA1: 160bit*] that meet the following: [*[14],* **[7], [9], [11]**].

Hierarchical to: No other components.

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

Application Note 3: The symmetric cryptographic algorithm in FCS_COP.1/Con_Sym shall be used to set up the trusted channel with a connector (see also chapter 6.1.7.1for the definition of the trusted channel itself).

6.1.1.5 FCS_COP.1/SIG Cryptographic operation for signature generation/verification

FCS_COP.1.1/SIG The TSF shall perform [*signature generation / verification*] in accordance with a specified cryptographic algorithm [*signature generation: usage of SM-KT, signature verification: SHA-256 with RSASSA-PKCS1-v1_5 or ECDSA using the curves brainpoolP256r1*] and cryptographic key sizes [*signature generation: RSA and ECDSA key size of SM-KT, signature verification: 2048bit for RSA and 256bit for ECDSA*] that meet the following: [*[14],* ***[23]***].

Hierarchical to: No other components.

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

Application Note 4: The algorithm for signature generation/verification in FCS_COP.1/SIG shall be used to establish the trusted channel with the connector (see also chapter 6.1.7.1 for the definition of the trusted channel itself).
Serving this purpose, the TOE shall use the support of the SM-KT for signature generation (see also A.SM). Further the TOE also shall verify that the connector certificate is trusted by the TSP CA using signature verification of FCS_COP.1/SIG

6.1.1.6 FCS_COP.1/Management Cryptographic operation for remote management

FCS_COP.1.1/ Management The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-CBC with HMAC-SHA1*] and cryptographic key sizes [*AES: 128 bit, 256bit; HMAC-SHA1: 160bit*] that meet the following: [*[14],* **[7], [9] [11]**].

Hierarchical to: No other components.

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

Application Note 5:	The cryptographic functionality in FCS_COP.1/Management and FCS_CKM.1/Management shall be used to establish the trusted path for remote management. See chapter 6.1.7.1 for the definition of the trusted path. The cryptographic functionality in FCS_CKM.1/Management shall comply with the requirements of the PKCS#1 standard described in [8][12]. This SFR can implicitly be fulfilled by the mechanisms for cryptographically secured communication with the connector.

[12] Sentence has been uniquely defined by the ST Author

6.1.1.7 FCS_COP.1/SIG_FW Cryptographic operation for firmware signature Verification

FCS_COP.1.1/ SIG_FW

The TSF shall perform [*signature verification for firmware updates*] in accordance with a specified cryptographic algorithm [*SHA-256 with RSASSA-PKCS1-v1_5*] and cryptographic key sizes [*2048 Bit for RSA*] that meet the following: [*[14],* **[10], [8]**].

Hierarchical to:

No other components.

Dependencies:

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

Application Note 6:

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.
The cryptographic functionality shall comply with the requirements of the PKCS#1 standard described in [8].[13]

6.1.1.8 FCS_COP.1/SIG_TSP Cryptographic operation for verification of TSP CA lists

FCS_COP.1.1/ SIG_TSP

The TSF shall perform [*signature verification*] in accordance with a specified cryptographic algorithm [*SHA-256 with RSASSA-PKCS1-v1_5*] and cryptographic key sizes [*2048 Bit for RSA*] that meet the following: [*[14]* **[10]**, **[8]**].

Hierarchical to:

No other components.

Dependencies:

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

Application Note 7:

The functionality is used to verify the integrity and authenticity of a potential update of the TSP CA list. Such functionality relies on hashing and encryption using a public key (signature verification).
The cryptographic functionality shall comply with the requirements of the PKCS#1 standard described in [8] (if applicable).
Please also note that if the vendor chose to provide TSP CA list updates via the firmware update mechanism, this SFR is to be considered to be fulfilled accordingly.[14]

[13] Application Note has been uniquely defined by the ST Author

[14] Application Note has been uniquely defined by the ST Author

6.1.2 User data protection (FDP)

6.1.2.1 FDP_ACC.1 Terminal Subset access control for terminal functions

FDP_ACC.1.1/ Terminal

The TSF shall enforce the [*Terminal SFP*] on

[

Subjects:

- *all subjects*

Objects:

- *PIN,*
- *TSP CA list*
- *shared secret*
- *management credentials*
- *firmware,*
- *cryptographic keys*,
- *Communication data*

[

- *failure counter for management interfaces*
- *notification of physical attacks*

]

Operations:

- *Read,*
- *Modify*

[

- *Delete*
- *Reset*

]

]

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.2 FDP_ACC.1 Management Subset access control for management

FDP_ACC.1.1/ Management

The TSF shall enforce the [*Management SFP*] on

[

Subjects:

- *users,*
- *[none]*

Objects:

- *Manageable objects, i.e. management functions*

Operations:

- *execute*

].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.3 FDP_ACF.1 Terminal Security attribute based access control for terminal functions

FDP_ACF.1.1 /Terminal

The TSF shall enforce the [*Terminal SFP*] to objects based on the following:

[
Subjects:
- *all subjects,*

attribute:
- *user role*[15]

Objects:
- *PIN,*
- *shared secret*
- *management credentials*
- *firmware,*
- *cryptographic keys*,

attribute:
- *firmware version*,
- *Enable/Disable the functionality of an unauthorized reset to factory defaults*[16]

[
Other objects:
- *TSP CA list*

attribute :
- *TSP CA list version*

]
].

FDP_ACF.1.2 /Terminal

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

If a firmware update is initiated, a modification of the firmware of the TOE shall only be allowed after the integrity and authenticity of the firmware has been verified according to FCS_COP.1/SIG_FW and:

- *The card terminal shall recognize non- authentic transmissions. The security anchor required for this action shall be placed in a writing-protected area of the external interfaces of the TOE.*
- *Furthermore, the security anchor shall be located in a read-only area of the device and shall only be able to be replaced with an administrative action.*
- *The transmission mechanism shall be in a position to detect transmission errors independently.*
- *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 according this Security Target*[17]*. For the use in*

[15] The role of the user (e.g. medical supplier, TOE administrator)

[16] i.e. its configuration status

[17] Reference changed from Protection Profile to Security Target

the German Healthcare System the named versions must also be approved by the gematik.

  - *In case of downgrades of the firmware 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.*
  - *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.*
  - *Installation 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/SIG_FW.*

If a TSP CA list update is initiated, a modification of the list shall only be allowed after the integrity and authenticity of the new TSP CA list has been verified according to FCS_COP.1/SIG_TSP.
The developer of the TOE shall ensure that in case of a downgrade of the firmware the TOE must warn the Administrator (e.g. within the Guidance) before the installation that the action to be performed is not an upgrade. The TOE must offer a chance to cancel the installation. A downgrade of the TOE shall only be possible after warning the administrator about the risks of this action. This warning shall be performed by the developer-specific update component.

The following management functions shall be executable by authenticated TOE administrators (excluding SICCT interface):
[<u>Enable/Disable the functionality of unauthorized reset to factory defaults</u>]

[

- *A firmware update should not lead to the deletion of the shared secret.*
- *Only the following explicit SICCT commands enter the TOE into the secure PIN entry mode which is indicated by a red flashing LED.*
  - *SICCT PERFORM VERIFICATION*
  - *SICCT MODIFY VERIFICATION DATA*

  The Secure PIN entry LED can be controlled only by the TOE.
- *The PIN can only be entered over the numeric PIN pad of the TOE.*

]

FDP_ACF.1.3 /Terminal

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- *Only an authorized user should be able to perform a firmware update.*
- *Only an authorized user should be able to perform a TSP CA list update.*
- *Only an authorized user should be able to change its own management credentials*
- *Only an authorized user should be able to delete the Shared Secret.*

].

FDP_ACF.1.4 /Terminal

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

[

- *No subject shall access any object but the TOE administrator's local management credentials before the TOE administrator's credentials are initially set.*
- *No subject shall read out the PIN, shared secret, management credentials or secret cryptographic keys while they are temporarily stored in the TOE*
- *No subject shall modify the public key for the signature verification of firmware updates unless a new public key is part of a firmware update.*
- *No subject and no action, especially a firmware update, should modify the value of the failure counter of the management interfaces.*
- *No subject and no action, especially a reset to factory defaults, should reset a notification of physical attacks.*

]

Hierarchical to: No other components.

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

Application Note 8: Specific implementations of a TOE compliant to the PP/ST require more objects that are subject to Access Control and more granular rules for Access Control. Therefore, the open assignment in FDP_ACF.1.2 has been used to specify the Access Control Policy for the TOE in more detail. Note that "firmware version" in FDP_ACF.1.2/Terminal could also be interpreted as a firmware group version. This allows the use of the firmware group concept described in [14] making downgrades possible.

An additional unauthorized reset to factory defaults mechanism is specified for the TOE in consideration of the following notes:

- The TOE administrators shall be able to enable/disable this mechanism.
- This mechanism shall be disabled by the default setting of the TOE.
- The TOE shall offer two reset options, i.e. authorized and unauthorized reset to factory default settings for the TOE administrator, if the later is enabled.
- The unauthorized reset to factory default settings may be technically performed by every user. Therefore, Guidance documentation shall advise the users that a reset shall only be performed by the TOE administrator.
- An unauthorized reset to factory defaults by unauthorized personnel results in an organizationally insecure state.

- The TOE administrator shall check the TOE and its environment regularly.
- The potentially insecure state shall be identified by the TOE.
- Information about the question of how the TOE and its environment indicate the insecure state after an unauthorized reset to factory defaults by unauthorized personnel shall be provided in the Guidance documentation.
- The information given in the Guidance documentation has to deal with the identification of the potentially insecure state and the further necessary steps of the user/administrator.
- The handling of potentially insecure TOE's on manufacturer's side shall be subject to ALC work units.[18]

6.1.2.4 FDP_ACF.1/Management Security attribute based access control for Management

FDP_ACF.1.1/ Management

The TSF shall enforce the [*Management SFP*] to objects based on the following:

[

Subjects:

- *users,*
- *[none]*

Subject attributes:

- *role(s),*
- *management interface,*[19]
- *[none]*

Objects:

- *management functions,*

Object attributes:

- *None*

]

[18] Application note has been uniquely defined by the ST Author

[19] The subject attribute management interface specifies the interface from which the user is connecting (i.e. local, remote, SICCT).

FDP_ACF.1.2 /Management

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
The following management functions shall be executable by all roles:

- *Display the product version number of the TOE*
- *Manage own login credentials*
- *View card terminal name for card terminal*
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [*Reset the TOE settings to factory defaults (unauthorized reset to factory defaults)*[20]]

[

- *Perform a TOE self-test*
- *View serial number of the TOE*

]

The following management functions shall be executable by authenticated administrators (excluding SICCT interface):

- [*Manage the available network configuration*]
- [*Set card terminal name for card terminal*]
- [*Enable/Disable remote update functionality for firmware update*]
- *Manage local and remote management login credentials*
- *Secure deletion of pairing information from all three possible pairing processes (initial pairing, review of pairing-information and maintenance-pairing)*
- *Manage the list of TSP CAs*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*
- [*Enable/Disable the functionality of unauthorized reset to factory defaults*]
- *[Enable/Disable administrative SICCT commands (e.g. perform firmware update)*
- *Enable/Disable the remote management interface]*

The following management functions shall be executable by administrators that were authenticated using the SICCT interface:

- [*Set card terminal name for card terminal*]
- *Perform a firmware update*

The following management functions shall be only executable by administrators that were authenticated using the local management interface:

- *Enable/disable the remote management interface (if applicable)*
- *Perform the pairing process with the connector*
- *[Enable/Disable reset to factory defaults without user authentication*
- *Enable/Disable administrative SICCT commands]*

The TOE Reset Administrator shall only be able to execute the following management function:

- *Reset the TOE settings to factory defaults(fallback)*
- *[Change the PUK]*

].

[20] Note that an unauthorized reset to factory defaults can technically be performed by every user but shall only be performed by the TOE administrator. Therefore, an unauthorized reset to factory defaults, executed by unauthorized personnel, results in an insecure state which will make it necessary for the administrator to replace the TOE. This potentially insecure state will be indicated by the TOE. The Guidance documentation describes how a user can indicate this insecure state and advice the administrator which steps has to be taken for reprocessing of the TOE.

FDP_ACF.1.3 /Management

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- *Authenticated administrators using the remote management interface (web interface) should be able to manage remote management credentials (for the Web interface)*
- *Authenticated administrators using the remote management interface (web interface) should be able to manage remote management credentials (for the SICCT interface)*

*[**that do not contradict the intention of the policy**]*

].

FDP_ACF.1.4 /Management

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

[

- *No subject should be able by default setting after initial start-up to perform any management function by using the remote management interface.*
- *No subject should be able by default setting after initial start-up to perform a remote update of the firmware.*
- *No subject should be able by default setting after initial start-up to perform a reset to factory defaults.*

*[**that do not contradict the intention of the policy**]*

]

Hierarchical to: No other components.

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

Application Note 9: FDP_ACF.1/Management was used to define the access control for management functionality of the TOE. It applies to all interfaces, which are capable of management functionality[21]

[21] Application note has been uniquely defined by the ST author

6.1.2.5 FDP_IFC.1/PIN Subset information flow control for PIN

FDP_IFC.1.1/PIN The TSF shall enforce the [*PIN SFP*] on
[
Subjects:

- *user,*
- *card,*
- *connector*
- *remote card terminal*[22]

Information:

- *PIN*

Operation:

- *Entering the PIN*

].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

6.1.2.6 FDP_IFF.1/PIN Simple security attributes for PIN

FDP_IFF.1.1/PIN The TSF shall enforce the [*PIN SFP*] based on the following types of subject and information security attributes:
Subject attribute:
[

- *Slot identifier*[23]*,*
- *[none]*

]

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

PINs shall never be stored in the non-volatile memory of the TOE.

The PIN entered by the user shall only be sent via the secure channel targeting the card in the card slot of the TOE or a remote card terminal for remote-PIN verification.

In the latter case the TOE shall assure that the connection to the connector is TLS secured.

].

FDP_IFF.1.3/PIN The TSF shall enforce the [*PIN digits shall never be displayed on the display during entry of the PIN. The TOE shall rather present asterisks as replacement for digits.*].

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

FDP_IFF.1.5/PIN The TSF shall explicitly deny an information flow based on the

[22] A remote card terminal either sends or receives a PIN for remote-PIN verification.

[23] This is the slot the user plugged his smart card in

following rules:
[

- *The PIN shall never leave the TOE in clear text for remote-PIN verification.*

].

Hierarchical to: No other components.

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

Application Note 10: *Please note that the term "display" in this and other SFR refers to a generic display device and does not require any specific realization. Specifically, this term does not require any display based on text or graphics but could e.g. also be realized as a simple LED as long as the requirements are fulfilled. However, [14] may specify more detailed requirements about the display device.*

For more information about the specific realization of the display for the TOE see Chapter 1.2 "TOE Overview".[24]
For remote-PIN verification the TOE may send the PIN to another card terminal via the connector. The PIN is then encrypted and transferred using card-to-card authentication of the smart cards in both card terminals.

Remote-PIN verification is initiated by the connector. Therefore, it is responsible to select the participating card terminals and to initiate card-to-card authentication between both.

Communication between TOE and connector is additionally secured using FCS_COP.1/Con_ Sym.
For more information about the specific realization of the remote PIN implementation see Chapter 7.1 "SF.3_Secure_PIN_Entry[25]

6.1.2.7 FDP_IFC.1/NET Subset information flow control for network connections

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

Subjects:

- *Connector,*
- *the TOE,*

Information:

- *all information arriving at the network interface*

Operation:

- *accept the communication]*

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

[24] Reference added by the ST author to state the application note more precisely.

[25] Reference added by the ST author to state the application note more precisely.

6.1.2.8 FDP_IFF.1/NET Simple security attributes for network connections

FDP_IFF.1.1/NET The TSF shall enforce the [*NET SFP*] based on the following types of subject and information security attributes:
[
Subject:
- *Connector*

Information:
- *Passwords,*
- *Patient data,*
- *Shared secret*
- *any other information,*

Information attribute:
- *sent via trusted channel*

[none]
].

FDP_IFF.1.2/NET The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[
Any information arriving at the network interface from the connector must only be accepted if the communication path is encrypted and the connector has been successfully authenticated[26]*.*
The TOE shall have only one connection to one connector at a time.
]

FDP_IFF.1.3/NET The TSF shall enforce the *[no further information flow control SFP rule]*

[26] See the trusted channel in section 6.1.7.1 and verification in section 6.1.1.5.

FDP_IFF.1.4/NET The TSF shall explicitly authorise an information flow based on the following rules:
[
The TOE shall accept the following SICCT commands arriving at the network interface even if no pairing process is established and no valid connector certificate is presented:

- *SICCT CT INIT CT SESSION*
- *SICCT CT CLOSE CT SESSION*
- *SICCT GET STATUS*
- *SICCT SET STATUS*
- *SICCT CT DOWNLOAD INIT*
- *SICCT CT DOWNLOAD DATA*
- *SICCT CT DOWNLOAD FINISH*

The TOE shall additionally accept the following EHEALTH commands (please refer to [14] *) arriving at the network interface if no pairing process is established but a valid connector certificate*[27] *is presented:*

- *EHEALTH TERMINAL AUTHENTICATE*

Commands to identify the TOE in the network (service discovery) may be accepted and processed even without an encrypted or authenticated connection.
].

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

- *Passwords for management interfaces shall never leave the TOE*
- *The shared secret shall never leave the TOE in clear text (even over trusted channel)*
- *Patient data shall not be transferred via the management interfaces*

].

Hierarchical to: No other components.

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

Application Note 11: Please note that the information flow policy defined in FDP_IFC.1/NET and FDP_IFF.1/NET is focused on the communications, which fall into the scope of the application for the electronic health card and which happen between the connector and the TOE.
Connections for administration of the TOE may not be initiated by a connector. Therefore such a connection may not be covered by this policy.
Further, according to [14] the terminal is free to accept unencrypted communications for other applications, which may be additionally realized by the terminal (or during the migration phase). In these cases the terminal would have to indicate to the user that it is working in an insecure state.

[27] For the steps in verifying signatures of the certificate application component see [14], Table 2.

For detailed information about the specific realization of secure communication see Chapter 7.1 “SF.1_Secure_Communication”. The TOE shall not accept unencrypted communication other than specified in [14].[28]

Please note that as a limitation to gematik - Spezifikation eHealth-Kartenterminal, Version 3.15.0, 16.05.2022

[15] the control byte for the bits b2..b1 of the Command-To-Perform Data Object CMD DO shall not contain other values than {b 2 = 1, b1 = 0} or {b 2 = 1, b1 = 1}.

6.1.2.9 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects:

[

- *PIN,*
- *cryptographic keys,*
- *all information that is received by a card in a slot of the TOE or by the connector (except the shared secret),*
- *[none]*

].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 12 The functionality, defined in FPD_RIP.1 defines that the TOE is not allowed to save any information that was received by the connector or a card in a slot of the TOE permanently. This is necessary as the TOE relies on a controlled environment (A.ENV) to provide an adequate level of protection for the assets. If a TOE was e.g. stolen an attacker must not be able to read any of the information that was received from the connector or a card in a slot of the TOE. Only information that is absolutely indispensable for the operation of the TOE (e.g. a secret that may be used for an initial review or the review of pairing information as part of the authentication with the connector) shall be stored permanently within the TOE.

To provide Batch Signature functionality, the TOE uses the functionality of the authorized card. In particular, this means that the PIN shall not be stored temporarily to trigger single signature processes using the stored PIN. The PIN shall be sent to the card once only and be made unavailable immediately after the batch signing process is initiated.[29]

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 [*[at least 3]*] unsuccessful authentication attempts occur related to [*management authentication excluding authentication for the TOE Reset Administrator*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has

[28] In order to describe the application note more precisely, the underlined parts has been refined by the ST author.

[29] In order to describe the application note more precisely, the underlined parts has been refined by the ST author.

been [met, surpassed], the TSF shall [*lock the particular management interface for that account for a time period according to* ***Table 9: Lockout times*** *depending on the number of consecutive unsuccessful authentication attempts*]

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

Application Note 13: The assignment in FIA_AFL.1.2 implies that each management interface shall have its own counters for unsuccessful authentication attempts.

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

Table 9: Lockout times

6.1.3.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Role*[30], [*none*]]

Hierarchical to: No other components

Dependencies: No dependencies.

Application Note 14: For the case that no further user attributes are needed for any policy of a TOE "none" should be considered as a valid assignment in FIA_ATD.1.1

[30] The role (attribute) of the user (e.g. medical supplier, TOE administrator)

6.1.3.3 FIA_SOS.1 Verification of secrets

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

[

Passwords for management shall

- *Have a length of at least 8 characters,*
- *Be composed of at least the following characters: “0”-“9”,*
- *Not contain the User ID/logon name shall not be a part of the password for the management interface,*
- *Not be saved on programmable function keys*
- *Not be displayed as clear text during entry*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 15: Note that the requirements on passwords hold for all management interfaces. Passwords for management interfaces (user authentication mechanism) shall be implemented separately for each management interface.[31]

6.1.3.4 FIA_UAU.1/Management Timing of authentication for management

FIA_UAU.1.1 The TSF shall allow

[

- *Display the product version number of the TOE*
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [*Reset the TOE settings to factory defaults (unauthorized reset to factory defaults[32])*]

[

- *Self-Test*
- *View serial number of the TOE*

]

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

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

[31] In order to describe the application note more precisely, the underlined part has been refined by the ST author.

[32] Note that an unauthorized reset to factory defaults can technically be performed by every user but shall only be performed by the TOE administrator. Therefore, an unauthorized reset to factory defaults, executed by unauthorized personnel, results in an insecure state which will make it necessary for the administrator to replace the TOE. This potentially insecure state will be indicated by the TOE. The Guidance documentation describes how a user can indicate this insecure state and advice the administrator which steps has to be taken for reprocessing of the TOE. Please refer to Application Note 8 for further information.

6.1.3.5 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1

The TSF shall provide
[
- *A password based authentication mechanism*
- *A remote authentication mechanism using the SICCT interface*
- *An authentication mechanism for the TOE Reset Administrator*
- *[An authentication mechanism using the remote management interface]*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [**following**]**:**
[
- *The local authentication mechanism is used for authentication of TOE administrators for management and other users*
- *The remote authentication mechanism is used for authentication of TOE administrators for management, if applicable*
- *The remote authentication for the SICCT interface is used for authentication of TOE administrators for management*
- *The authentication mechanism for the TOE Reset Administrator is used to authenticate the TOE Reset Administrator who alone is able to reset the TOE settings to factory defaults (fallback) when the management credentials are lost*
- *[none]*

]

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 16: Please note that FIA_UID.1 and FIA_UAU.1 refer to the authentication of TOE administrators, TOE Reset Administrator and users of the TOE. According to [14] this should not be seen as a requirement to maintain the ID of the current user for access control. The scope of these requirements is to determine to which group the current user belongs as the access control mechanism of the TOE primarily works on the basis of the user role.[33]

[33] Second and third paragraph of the original application note from the PP has been deleted by the ST author

6.1.3.6 FIA_UAU.7 Protected authentication feedback

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

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

Application Note 17: This SFR covers the management authentication feedback.

6.1.3.7 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow
[
- *Display the product version number of the TOE*
- *View card terminal name for card terminal*
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [*Reset to TOE settings to factory defaults (unauthorized reset to factory defaults)*[34]]
[
- *TOE Self-Test*
- *View serial number of the TOE*

]

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

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

Hierarchical to: No other components

Dependencies: No dependencies

Application Note 18: The assignments in FIA_UAU.1.1/Management and FIA_UID.1.1/Management have to be performed in a way that none of the TSP of the TOE is violated.[35]

[34] Note that an unauthorized reset to factory defaults can technically be performed by every user but shall only be performed by the TOE administrator. Therefore, an unauthorized reset to factory defaults, executed by unauthorized personnel, results in an insecure state which will make it necessary for the administrator to replace the TOE. This potentially insecure state will be indicated by the TOE. The Guidance documentation describes how a user can indicate this insecure state and advice the administrator which steps has to be taken for reprocessing of the TOE. Please refer to Application Note 8 for further information.

[35] Application note has been uniquely defined by the ST author.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 /Terminal Management of security attributes for Terminal SFP

FMT_MSA.1.1 /Terminal

The TSF shall enforce the [*Terminal SFP*] to restrict the ability to [*modify*] the security attributes [*Enable/Disable the functionality of an unauthorized reset to factory defaults*[36]] to [*authenticated TOE administrators (excluding SICCT interface*[37]*)*].

Hierarchical to: No other components.

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

6.1.4.2 FMT_MSA.1 /Management Management of security attributes for Management SFP

FMT_MSA.1.1/ Management

The TSF shall enforce the [*Management SFP*] to restrict the ability to
[

- query,
- modify,
- delete
- *[none]*

]
the security attributes *[manageable objects i.e. all management functions] to [TOE administrators]*

Hierarchical to: No other components.

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

6.1.4.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [*roles(s)*[38]].

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

[36] i.e. its configuration status

[37] i.e. the standard interface to the connector using the SICCT-Protocol

[38] Role(s) as defined in 6.1.4.7

6.1.4.4 FMT_MSA.3 /Terminal Static attribute initialisation for Terminal SFP

FMT_MSA.3.1 /Terminal	The TSF shall enforce the [*Terminal SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 /Terminal	The TSF shall allow the [*no roles*] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

6.1.4.5 FMT_MSA.3 /Management Static attribute initialisation for management SFP

FMT_MSA.3.1 /Management	The TSF shall enforce the [*Management SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 /Management	The TSF shall allow the [*no roles*] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

Application Note 19: *Restrictive* specifically means that remote update functionality for firmware update and remote management functionality are disabled by default.

6.1.4.6 FMT_SMF.1 Specification of Management Functions

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

[

- *Manage local and remote management login credentials*[39]
- *Perform the pairing process(initial pairing, review of pairing information and maintenance-pairing) with the connector*
- *Secure deletion of pairing information from all three possible pairing processes*
- *Manage the list of TSP CAs*[40]
- *View/set card terminal name*[41] *for card terminal*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*[42]
- *Reset the TOE settings to factory defaults (fallback)*[43]
- *Display the product version number of the TOE*
- *Display the installed firmware group version*

[39] On first start-up the TOE forces the administrator to specify a password for local management.

[40] Management of TSP-CAs includes the update of TSP-CA lists as described in [14] as well as a selection of a particular TSP-CA list to be used in case of multiple TSP-CA lists residing in the firmware (e.g. a separate TSP-CA list for test purposes).

[41] The card terminal name is a unique identifier for the card terminal. Note that the terminal name shall not be set using dhcp.

[42] Note that after a reset to factory defaults the TOE is supposed to be in its initial state, and the administrator's local management credentials have to be set again.

[43]The fallback solution for reset of TOE settings is necessary in case the credentials for management are lost.

- *Return self-assessment through the user interface of the administration interface*
- *Enable/disable remote management functionality*
- [*Managing network configuration*]
- [*Enable/Disable remote update functionality for firmware update*]
- [*Enable/Disable the functionality of an unauthorized reset to factory defaults.*[44]]
- [*Choose, which reset to factory defaults mechanism (reset the TOE settings to factory defaults or unauthorized reset to factory defaults) to perform.*[45]]
- [*Display the MAC-address(es) of the TOEs network interface(s)*][46]
- [*Change the PUK*][47]
- *[Enable/Disable administrative SICCT commands]*

].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 20: FDP_ACF.1/Management and FDP_ACC.1/Management further define which management functions are executable for the various user roles.

Please note, that relevant data like failure counters for management interfaces and the shared secret shall not be reset when the firmware is updated.

As the reset to factory defaults (fallback) shall only be possible for authenticated TOE administrators (see FDP_ACF.1/Management), a reset without authentication can only be done under the conditions as describes in [14] if the management credentials are lost.

Note that remote update functionality for firmware update shall only be implemented as a PUSH service described in [14]. This requires an update component located in the local network of the medical supplier which is under the control of the TOE administrator (see OE.PUSH_SERVER). The administrator approves and releases the firmware update that should be pushed by the update component. The update component logs card terminal identifier, the time of update, the version of the firmware to install, and the result of the update for each single update process.

For further details about the implementation of the update process see Chapter 7.1 “SF.4_Secure_Update”

The TOE administrators shall be able to Enable/Disable the functionality of an unauthorized reset to factory defaults in case this functionality is implemented by the TOE.

Further only authenticated TOE administrators shall be able to choose, which reset to factory defaults mechanism (reset the TOE settings to factory defaults or unauthorized reset to factory defaults) to perform when performing a reset.

Those SFRs refer to all Management interfaces and have to be refined accordingly. Those include mandatory local and SICCT as well as the optional remote management interface.[48]

[44] In case this functionality is implemented it must be disabled by default. Please also refer to Application Note 8 for further information

[45] Note that an unauthorized reset to factory defaults executed by unauthorized personnel shall lead into an insecure state of the TOE which will make it necessary to send the TOE back to the developer. Please refer to Application Note 8 for further information

[46] Another option would be to attach the MAC-address(es) to the body of the card terminal.

[47] A reset to factory defaults shall be performed in the way described in [14].

[48] In order to describe the application note more precisely, the underlined part has been refined by the ST author.

6.1.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- *user,*
- *TOE administrator,*
- *TOE Reset Administrator*
- *[none]*

].

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_FLS.1 Failure with preservation of secure state

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

- *disconnection of connector*[49]*,*
- *failure during firmware update,*

[

- *failure during TOE self-test*
- *disconnection of the SM-KT,*
- *failure of the casing protection*

]

].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 21: As [14] does not define the list of errors for which a secure state has to be preserved, the assignment in FPT_FLS.1.1 has been done by the ST author. As a minimum the failure of any of the self-tests as defined in FPT_TST.1 and failure of firmware updates has been considered for this assignment.[50]

[49] When the TLS connection to the connector is lost, the secure state is preserved by resetting all plugged smart cards .

[50] In order to describe the application note more precisely, the underlined part has been refined by the ST author.

6.1.5.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [

- disclosure,
- modification]

when it is transmitted between separate parts of the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 22: This SFR is easily fulfilled as the TOE does not comprise of physically separated parts.[51]

6.1.5.3 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 whether physical tampering with the TSF’s devices or TSF’s elements has occurred.

Hierarchical to: No other components

Dependencies: No dependencies

Application Note 23: FPT_PHP.1 has been augmented by FPT_PHP.2 to require an active protection mechanism against physical manipulation.
The dependency to FMT.MOF.1 required by FPT_PHP.2 has been considered.[52]

6.1.5.4 FPT_PHP.2 Notification of physical attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For
[*all TSF devices / elements which protect the*

- *smart card interfaces*
- *I/O circuits necessary for the internal transfer of the PIN and TSF-Data*
- *Memory chips for the storage of TSF-Data*

], the TSF shall monitor the devices and elements and notify [*all roles*] when physical tampering with the TSF's devices or TSF's elements has occurred.

Hierarchical to: FPT_PHP.1

Dependencies: FMT_MOF.1 Management of security functions behavior.

[51] Application note has been uniquely refined by the ST author

[52] Application note has been uniquely refined by the ST author.

6.1.5.5 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self-tests

[

- during initial start-up,
- at the conditions

  [

  - *every restart*
  - *after user's request*

  ]

]

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 [

- *the TOE software*
- *the TSP-CA list*
- *the firmware group list*].

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

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 24: Please note that [14] does not define any concrete requirements for the minimum functionality that has to be covered by the self-test of the TOE. The focus of this requirement is to demonstrate the correct operation of the complete TSF.
FPT_TST.1.2 and FPT_TST.1.3 can be fulfilled firstly by checking the integrity of the complete TOE software. Additional a periodically check of the integrity of the casing protection and the battery state is implemented. At every start-up a check of the cryptographic functions is realized.[53]

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_TAB.1/SEC_STATE Default TOE access banners for secure state

FTA_TAB.1.1/SEC_STATE Before establishing a user session, the TSF shall display **a message indicating, whether the TOE is in a secure state or not.**

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 25: In the context of FTA_TAB.1/SEC_STATE the term "Before establishing a user session" refers to every situation a user is about to use the TOE.

Application Note 26: This SFR is used to meet O.STATE. The "secure state" refers to a mode of operation in which all TSPs of this ST are met and no additional value-added module functionality (as allowed by [14]) is active that could compromise a TSP. Specifically the TOE will guarantee a secure PIN entry within such a secure state.

[53] In order to describe the application note more precisely, the underlined part has been added or refined by the ST author.

For example, according to [14] a TOE could in principle accept unencrypted communications by a third party for applications that are outside the scope of the German Healthcare System. However as long as an unencrypted connection is established the TOE cannot be considered being in a secure state.

Due to the fact, that the TOE doesn’t provide any additional functionality than the functionality, required by the PP, this SFR can be seen as fulfilled.[54]

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_ITC.1/Connector Inter-TSF trusted channel for connector communication

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

FTP_ITC.1.2 /Connector The TSF shall permit [the connector] to initiate communication via the trusted channel.

FTP_ITC.1.3 /Connector The TSF shall initiate communication via the trusted channel for [*all communication functions used by eHealth applications*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 27: The SFR covers the authentication of the connector by the TOE using the connector certificate of an already paired connector. The TOE also verifies that the connector certificate is trusted by the TSP CA using signature verification of FCS_COP.1/SIG. The trusted channel will only be active when the TOE is in “secure state”. Otherwise it will be dropped.
There is only one connection to one connector at a time.
The TOE authenticates itself with the shared secret and the certificate of the SM-KT. It has to be ensured that no security threat arises when the SM-KT is unplugged (e.g. by dropping the TLS connection).

6.1.7.2 FTP_TRP.1/Management Trusted path for remote management

FTP_TRP.1.1 /Management The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification or disclosure, [*none*]].

FTP_TRP.1.2 /Management The TSF shall permit [remote users] to initiate communication via the trusted path

FTP_TRP.1.3 /Management The TSF shall require the use of the trusted path for [

- *authentication of TOE administrators,*
- *remote management*].

Hierarchical to: No other components.

Dependencies: No dependencies.

[54] In order to describe the application note more precisely, the underlined part has been refined by the ST author.

6.2 Security Assurance Requirements for the TOE

The following table lists the assurance components which are required by the PP.

Assurance Class	Assurance Components
ADV: Development	ADC_ARC.1: Security Architecture Description
	ADV_FSP.4 Complete Functional Specification
	ADV_IMP.1 Implementation Representation of the TSF
	ADV_TDS.3 Basic Modular Design
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedure
ALC: Life-cycle support	ALC_CMC.3 Authorisation Control
	ALC_CMS.3 Implementation Representation CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of Security Measures
	ALC_LCD.1 Developer Defined Life-Cycle Model
	ALC_TAT.1 Well-defined Development Tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance Claims
	ASE_ECD.1 Extended Components Definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security Objectives
	ASE_REQ.2 Derived Security Requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE Summary Specification
ATE: Tests	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: Basic Design
	ATE_FUN.1 Functional Testing
	ATE_IND.2 Independent Testing – Sample
AVA: Vulnerability assessment	**AVA_VAN.4** Methodical Vulnerability Analysis

Table 10: Chosen Evaluation Assurance Requirements

These assurance components represent EAL 3 augmented by the components marked in bold text. The complete text for these requirements can be found in 3.1, Revision 4, September 2012 [3]

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FCS_CKM.1 / Connector					X		
FCS_CKM.1 / Management				X			
FCS_CKM.4				X	X		X
FCS_COP.1/ Con_Sym					X		
FCS_COP.1/ SIG					X		
FCS_COP.1/ Management				X			
FCS_COP.1/ SIG_FW				X			
FCS_COP.1/ SIG_TSP				X			
FDP_ACC.1 / Terminal	X	X		X			
FDP_ACC.1 / Management				X			
FDP_ACF.1 / Terminal	X	X		X			
FDP_ACF.1 / Management				X			
FDP_IFC.1/PIN		X					
FDP_IFF.1/PIN		X					
FDP_IFC.1/NET					X		
FDP_IFF.1/NET					X		
FDP_RIP.1							X
FIA_AFL.1			X				
FIA_ATD.1			X				
FIA_SOS.1				X			
FIA_UAU.1			X				
FIA.UAU.5			X				

Table 11: Security Functional Requirements Rationale

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FIA_UAU.7		X					
FIA_UID.1			X				
FMT_MSA.1 / Terminal	X			X			
FMT_MSA.1 / Management				X			
FMT_MSA.2				X	X		
FMT_MSA.3 / Terminal	X			X			
FMT_MSA.3 / Management				X			
FMT_SMF.1				X			
FMT_SMR.1			X				
FPT_TST.1							X
FPT_FLS.1							X
FPT_ITT.1							X
FPT_PHP.1							X
FPT_PHP.2							X
FTA_TAB.1/SEC_STATE						X	
FTP_ITC.1 / Connector					X		
FTP_TRP.1 / Management				X			

Table 12: Coverage of Security Objective for the TOE by SFR

The Security Objective **O.ACCESS_CONTROL** is met by a combination of the SFR *FDP_ACC.1/Terminal, FDP_ACF.1/Terminal*, *FMT_MSA.1/Terminal* and *FMT_MSA.3/Terminal*. *FDP_ACC.1/Terminal* defines the access control policy for the terminal and *FDP_ACF.1/Terminal* defines the rules for the access control policy. It is specifically defined in *FDP_ACF.1/Terminal* that nobody must be allowed to read out the PIN or private cryptographic keys from the terminal. *FMT_MSA.1/Terminal* defines, who will be allowed to manage the attributes for the access control policy while *FMT_MSA.3/Terminal* defines that the terminal has to provide restrictive default values for the access control policy attributes.

The Security Objective **O.PIN_ENTRY** is met by a combination of the SFR *FDP_ACC.1/Terminal, FDP_ACF.1/Terminal, FDP_IFC.1/PIN, FDP_IFF.1/PIN,* and *FIA_UAU.7.* As part of the access control policy of the terminal *FDP_ACC.1/Terminal* and *FDP_ACF.1/Terminal* define that nobody must be able to read out the PIN from the terminal, which is required by O.PIN_ENTRY. *FPD_IFC.1/PIN* and *FDP_IFF.1/PIN* build an information flow control policy for the PIN and define that the PIN, which is entered by the user will only be sent to the card slot as indicated. Finally, *FIA_UAU.7* requires that the PIN digits are presented as asterisks on the display.

The Security Objective **O.I&A** is met by a combination of *FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1 and FMT_SMR.1*. *FIA_AFL.1* requires that the password policy is enforced. *FIA_UID.1* and *FIA_UAU.1* require each user to be authenticated and identified before allowing any relevant actions on behalf of that user.

Further the objective requires that the TOE will at least maintain the roles TOE administrator and TOE Reset Administrator. This is defined in *FMT_SMR.1*, which defines the roles and *FIA_ATD.1*, which defines the user attribute for the role. *FIA_UAU.5* defines all the authentication mechanism that shall or can be implemented by the TOE, in particular for local and remote management.

The Security Objective **O.MANAGEMENT** is met by a combination of *FCS_CKM.1/Management, FCS_CKM.4, FCS_COP.1/Management, FCS_COP.1/SIG_FW, FCS_COP.1/SIG_TSP, FDP_ACC.1/Terminal, FDP_ACF.1/Terminal, FDP_ACC.1/Management, FDP_ACF.1/Management, FIA_SOS.1, FMT_MSA.1/Terminal, FMT_MSA.1/Management, FMT_MSA.2, FMT_MSA.3/Terminal, FMT_MSA.3/Management, FMT_SMF.1, and FTP_TRP.1/Management. FCS_CKM.1/Management* requires that adequate keys are generated for remote management communication. *FCS_CKM.4* requires that keys are adequately destroyed. *FCS_COP.1/Management* requires that remote management shall enforce TLS. *FCS_COP.1/SIG_FW* is used to define the mechanism to check the authenticity of a firmware update. *FCS_COP.1/SIG_TSP* is used to define the mechanism to check the authenticity of a TSP CA list update. The access control policy defined in *FDP_ACC.1/Terminal* and *FDP_ACF.1/Terminal* define the rules under which a firmware update is possible. *FDP_ACC.1/Management* and *FDP_ACF.1/Management* define the access control policy that determines under what circumstance a particular management function is accessible and by whom. *FIA_SOS.1* defines the password policy for management credentials. FMT_MSA.1/Terminal and FMT_MSA.1/Management define, which roles are allowed to administer the attributes of the access control and the information flow control policies. *FMT_MSA.2* requires that only secure values are accepted for security attributes. *FMT_MSA.3/Terminal* defines that the terminal has to provide restrictive default values for the terminal access control policy attributes. *FMT_MSA.3/Management* defines that the terminal has to provide restrictive default values for the management access control policy attributes. *FMT_SMF.1* describes the minimum set of management functionality, which has to be available according to the Security Objective. Finally, FTP_TRP.1/Management defines the trusted path between the TOE and the management client.

The Security Objective **O.SECURE_CHANNEL** is met by a combination of the SFR *FCS_CKM.1/Connector, FCS_CKM.4, FCS_COP.1/Con_Sym, FCS_COP.1/SIG, FDP_IFF.1/NET and FDP_IFC.1/NET., FMT_MSA.2*, and *FTP_ITC.1/Connector. FCS_CKM.1/Connector*, *FCS_COP.1/Con_Sym, and FCS_COP.1/SIG* define the cryptographic operations, which are necessary for this objective. *FCS_CKM.1/Connector* defines that the TOE has to be able to generate (negotiate) cryptographic keys, which can be used to secure the communication with the connector. *FCS_CKM.4* defines the functionality to securely destroy cryptographic keys. The information flow control policy in *FDP_IFF.1/NET* and *FDP_IFC.1/NET* defines that at the network interface only a command to locate the TOE may be available without an encrypted connection and that all other communications must only be accepted if the secure channel to the connector has been established before. *FMT_MSA.2* defines that only secure values shall be used for security attributes. Finally *FTP_ITC.1* defines the trusted channel itself, which is used to secure the communication between the TOE and the connector.

O.STATE is directly and completely met by *FTA_TAB.1/SEC_STATE* as this SFR requires that the TOE shall be able to indicate, whether it is working in a secure state.

The Security Objective **O.PROTECTION** is met by a combination of the SFR *FCS_CKM.4 FDP_RIP.1, FPT_ITT.1, FPT_PHP.1, FPT_PHP.2, FPT_FLS.1 and FPT_TST.1.*

FCS_CKM.4 defines that cryptographic keys have to be securely deleted when they are no longer used. *FDP_RIP.1* defines the same additionally for the PIN and also ensures that an attacker cannot read other protected information from the TOE even if the TOE is no longer in its protected environment. *FPT_ITT.1* defines that the TOE has to protect TSF data when it is transmitted between physically separated parts of one TOE. *FPT_PHP.1 and FPT_PHP.2* builds the physical protection for the stored assets. *FPT_TST.1* defines the necessary test functionality for the underlying abstract machine. *FPT_FLS.1* defines a list of failures in the TSF for which the TOE has to preserve a secure state. Finally *FPT_TST.1* defines that the TSF have to run a suite of self-tests to demonstrate the correct operation of the TSF at start-up and during the normal operation of the TOE.

6.3.2 Dependency Rationale

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

SFR	Dependencies	Support of the Dependencies
FCS_COP.1/Management	[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/Management, FCS_CKM.4
FCS_COP.1/SIG_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 6.3.3 for FDP_ITC.1 and FCS_CKM.4
FCS_COP.1/SIG_TSP	[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 6.3.3 for FDP_ITC.1 and FCS_CKM.4
FDP_ACC.1 / Terminal	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/Terminal
FDP_ACC.1 / Management	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/Management
FDP_ACF.1 / Terminal	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/Terminal and FMT_MSA.3/Terminal
FDP_ACF.1 / Management	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Fulfilled by FDP_ACC.1/Management and FMT_MSA.3/Management
FDP_IFC.1/PIN	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/PIN
FDP_IFF.1/PIN	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/PIN See chapter 6.3.3 for FMT_MSA.3
FDP_IFC.1/NET	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/NET

SFR	Dependencies	Support of the Dependencies
FDP_IFF.1/NET	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/NET See chapter 6.3.3 for FMT_MSA.3
FDP_RIP.1	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled
FIA_UAU.5	No dependencies	-
FIA_UAU.7	FIA_UID.1 Timing of identification	Fullfiled
FIA_UID.1	No dependencies	-
FMT_MSA.1/Terminal	[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 FDP_ACC.1/Terminal, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1/Management	[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 FDP_ACC.1/Management, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FPD_ACC.1/Terminal, FPD_ACC.1/Management FDP_IFC.1/PIN, FDP_IFC.1/NET, FMT_MSA.1/Terminal, and FMT_SMR.1
FMT_MSA.3/ Terminal	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FMT_MSA.1/Terminal and FMT_SMR.1
FMT_MSA.3 /Management	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FMT_MSA.1/Management and FMT_SMR.1
FMT_SMF.1	No dependencies	-
FMT_SMR.1	FIA_UID.1 Timing of identification	Fullfiled
FPT_TST.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_ITT.1	No dependencies	-
FPT_PHP.1	No dependencies	-

SFR	Dependencies	Support of the Dependencies
FPT_PHP.2	FMT_MOF.1 Management of security functions behaviour	See chapter 6.3.3 for the dependencies FMT_MOF.1
FTA_TAB.1/SEC_STATE	No dependencies	-
FTP_ITC.1 /Connector	No dependencies	-
FTP_TRP.1 / Management	No dependencies	-

Table 13: Dependencies of the SFR for the TOE

6.3.3 Justification for missing dependencies

The dependencies of the information flow policies FDP_IFF.1/PIN and FDP_IFF.1/NET to FMT_MSA.3 was considered to be not applicable as both information flow policies do not require initialization of their security attributes.

The dependencies FDP_ITC.1 and FMT_MSA.2 of FCS_COP.1/SIG_FW and FCS_COP.1/SIG_TSP result out of the original scope of FCS_COP.1 to specify the implementation of encryption functionality within a TOE. These dependencies deal with the import (or creation) and destruction of a secret key that is needed for encryption. However, as in the context of this ST FCS_COP.1/SIG_FW and FCS_COP.1/SIG_TSP are used for a requirement on signature verification for which no secret key is necessary these dependencies do not need to be considered.

The dependencies FMT_MOF.1 Management of security functions behaviors of and FPT_PHP.2 was considered to be not applicable because the TSF supporting FPT_PHP.2 does not provide the ability to manage security functions behavior.

6.3.4 Security Assurance Requirements Rationale

The Evaluation Assurance Level for this Security Target is EAL 3 augmented by AVA_VAN.4 (and consequently with its dependencies ADV_FSP.4, ADV_IMP.1, ADV_TDS.3 and ALC_TAT.1).

The main decision about the Evaluation Assurance Level has been taken:

- based on the fact that the TOE described in this Security Target shall serve as a secure PIN entry device (see also OSP.PIN_ENTRY) and
- based on the fact that the TOE is used in a controlled environment but also needs to provided an adequate level of protection for its assets.

This lead to an Evaluation Assurance Level of 3 augmented by the following components:

- AVA_VAN.4

These components have the following direct and indirect dependencies, which have to be satisfied within the evaluation:

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1 (required by ADV_IMP.1)

6.3.5 Security Requirements – Mutual Support and Internal Consistency

The core TOE functionality in this Security Target is represented by the requirements for access control (FDP_ACC.1 and FDP_ACF.1) and information flow control (FDP_IFC.1/PIN, FDP_IFF.1/PIN, FDP_IFC.1/NET and FDP_IFF.1/NET).

Further functionality to protect the communication is defined by the requirements for cryptographic support and the trusted channel.

In the end this Security Target contains a set of SFRs which deal with the detection and defeating of attacks to the TOE, resp. SFRs which are used to show that the TOE is working correctly (e.g. FPT_PHP.1, FPT_TST.1). By this way the SFRs mutually support each other and form a consistent whole.

From the details given in this rationale it becomes evident that the functional requirements form an integrated whole and, taken together, are suited to meet all security objectives. Requirements from [2] are used to fulfil the security objectives.

7. ASE_TSS - TOE summary specification

This chapter describes the TOE summery specification under chapter 7.1 as well as the TOE security measures under chapter 7.2. All assurance measures will be described under chapter 7.3

7.1 TOE Security Functions

The TOE is designed for the use within the Telematikinfrastruktur (TI) of the German Healthcare-System.

The TOE will be used as a part of a signature application component for the creation of qualified signatures and for the processing and storage of personal data on healthcards.

The Protection of personal identification data (PIN), the secure transmission of data and the secure firmware update are the main features.

The following security functions are implemented to guarantee these features of the TOE:

SF.1_Secure_Communication

A secure communication with the connector requires an encrypted connection and a successful finished Pairing process according to [14].

The shared secret, created during the pairing process, is stored in a secure storage of the TOE.

The TOE accepts without encrypted connection only commands for locating the terminal (Service Discovery).

The encrypted connection will be established according to TLS 1.2 by using the Cipher Suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA or TLS_DHE_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1.

Diffie-Hellman method will be used for key exchange by using the prime number (p) defined by the DH group 14 with a key size of 2048 bit.

A mutual authentication is preferred to establish the TLS secured connection between the connector and the TOE by using asymmetric keys and X.509 certificates.

The X.509 certificate of the connector can be verified by the TOE by means of a secure stored TSP CA list.

For all TLS connections only the random number generator of the SM-KT will be used.

Without a successful finished pairing process and without a mutual authentication during the establishing of a TLS secured connection the TOE will only accept the following SICCT commands via an encrypted connection:

- *SICCT CT INIT CT SESSION*
- *SICCT CT CLOSE CT SESSION*
- *SICCT GET STATUS*
- *SICCT SET STATUS*
- *SICCT CT DOWNLOAD INIT*
- *SICCT CT DOWNLOAD DATA*
- *SICCT CT DOWNLOAD FINISH*

The TOE accepts the following EHEALTH command after successful mutual authentication during the TLS connection establishment without valid pairing information.

- *EHEALTH TERMINAL AUTHENTICATE*

Only after mutual validation of the device certificate and the corresponding pairing information the TOE is in a trustworthy secure state.

The secure state of the TOE, were all SICCT and EHEALTH commands will be executed, is indicated by a closed padlock symbol in the display.

The TOE will just establish and maintain one connection to a host via the SICCT-Interface.

The TOE holds up the context between the secure connection and the managed smart cards. This means that the TOE resets the smart cards after aborting of a connection.

Connections for TOE management can be established by using the SICCT- Interface or by using the https- Interface.

The establishing of a connection for the remote management interface requires a one-sided authentication of the TOE against the Client (e.g. web browser).

The TOE accepts for remote management TLS secured connections per TLS 1.2 by using the Cipher Suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA or TLS_DHE_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA or TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. After closing or aborting of a secure connection the corresponding session key will be deleted securely.

The TOE does not support any value-added services or other functionalities outside of eHealth applications.

Even an attacker with moderate attacking potential is not able to bypass this security function. Because of the mutual authentication and the pairing of the communication partner is the trustworthiness of the communication secured.

SF.2_Memory_Rework

All data from a connector or a smart card stored in the TOE which is not necessary for the operation of the TOE, will be deleted securely after the object is released.
After the TOE receives a command for secure PIN entry it will be stored temporarily.
The memory area for the PIN data will be reworked after transfer of the command to the smart card, after removing the card, after cancellation by the user, after a timeout during PIN entry and during start-up procedure.
Session Key for the encryption of a secure connection will be deleted after closing or aborting the secure connection.

Even an attacker with moderate attacking potential cannot bypass this security function because of the implementation of this function exists no possibility to manipulate this security function.

SF.3_Secure_PIN_Entry

Before every query of a Smart Card PIN or a Remote PIN the TOE will be set into the secure PIN entry mode, to guarantee that the PIN will only be forwarded to the smart card in the corresponding smart card slot.
The secure PIN entry mode will be activated regarding the requirements of the SICCT command set.
Following are the permitted SICCT commands listed:

- SICCT PERFORM VERIFICATION
- SICCT MODIFY VERIFICATION DATA

This SICCT commands contains amongst others the addressed of the smart card interface and the Command-To-Perform Data Object. This encodes a template where the TOE embeds a smart card APDU or a part of a smart card APDU.
The smart card APDU can contain the following Instruction bytes.

INS- Byte:	Designation:	Standard:
20h	VERIFY	ISO 7816-4 table 65
24h	CHANGE REF. DATA	ISO 7816-4 table 65
26h	DISABLE CHV	ISO 7816-8

28h	ENABLE CHV	ISO 7816-8
2Ah	PERFORM SECURITY OPERATION	ISO 7816-8 5.9 table 13
2Ch	RESET RETRY COUNTER	ISO/IEC 7816-8

Table 14: Instructionbytes [ISO 7816]/[EMV 2000]

The security function recognizes the command for PIN entry, sent by the host, and inserts the PIN data entered over the keypad to the corresponding place in the command.
The TOE sends the command with the PIN to the smart card after PIN entry.
The command of a Remote PIN query will be send directly to the connector.

The upper part of the Display, which is only controlled by the TOE, indicates the secure PIN entry mode to the user.
A red flashing Status LED beside the corresponding smart card slot (eHC- and HPC-Slot) indicates the secure PIN entry mode, too in case of the verification against an inserted smart card.

The user can choose between two different ways to enter the PIN.

The PIN can be entered by using the arrow keys (left arrow, right arrow).

Thereby, the lower part of the display shows the numbers 0 to 9, the active number is marked with the course. It is intended to select the active number with the arrow keys and confirm the selection with the enter key. The start position of the course is selected randomly by the TOE.

The second way to enter the PIN is by using the numeric key area of the TOE.

It is recommended to enter the PIN with the arrow keys of the editing section.

After entering the complete PIN or after aborting the secure PIN entry mode will be finished.

Aborting of the procedure comprises the removing of the card, pressing the cancel key and the exceeding of the allowed entry time.

The PIN entry progress is represented by displaying „*“ to the user.

Even an attacker with moderate attacking potential cannot bypass this security function or is able to get in possession of the PIN.

SF.4_Secure_Update

This security function guarantees the integrity and authenticity of a firmware update by verification of the signature with an asymmetric RSA algorithm with a bit length of 2048 and the hash-algorithm SHA-256 [10].
The firmware will be stored in the non-active part of the flash memory for verification of the signature. Subsequently starts the verification of the signature and the version of the firmware list.
The public key for verification of the signature is stored in the active part of the flash memory.
Only after successful signature verification and after successful verification of the firmware core version the new firmware will be accepted. A restart of the TOE will be enforced to activate the new firmware.
The TOE accepts only firmware versions listed in the valid firmware list.
In case of downgrades of the firmware the update progress will be stopped and the administrator will be warned about the downgrade. The administrator must confirm the downgrade to proceed with the update.

The firmware update can be processed via the TLS secured SICCT interface only, in form of a push update as described in [14].

Only the following SICCT commands are allowed for firmware updates:

- *SICCT CT INIT CT SESSION*
- *SICCT CT DOWNLOAD INIT*
- *SICCT CT DOWNLOAD DATA*
- *SICCT CT DOWNLOAD FINISH*
- *SICCT CT CLOSE CT SESSION*

Only a user with administrator rights can perform a firmware update.
The integrity of the active firmware will be check by calculating the hash value of the firmware (SHA256) during every restart.
This check can also be initiated be every user.
Every firmware provided for update has attached a current user documentation of the TOE.

Stored TSP CA lists can be updated by an authorized administrator. Only by Cherry Digital Health GmbH signed TSP CA lists with an equal or higher version as stored will be accepted by the TOE.
Signature verification of the TSP CA lists will be done with RSA with a key size of 2048bit and SHA 256.

Even an attacker with moderate attacking potential cannot bypass this security function or is able to get in possession of the private key.

SF.5_User _Authentication

At the first start-up, the TOE enforces to set an administrator PIN and a PUK to perform a reset to factory defaults when the administrator login credentials are lost.
The PIN can only be entered via the local management interface. The administrator can also choose a password as administrator PIN.
All interfaces, except of the display and the key matrix, of the TOE are disabled until an administrator PIN is set.

A user has always the possibility to change his management credentials including the PIN or password.

The following requirements will be sustained by the TOE to management PINs and passwords:

- Have a length of at least 8 characters,
- Be composed of at least the following characters: „0“ –„9“,
- Not contain the user ID/Logon name shall not be a par tot the password for the management interface,
- not be saved on a programmable function keys,
- not be displayed as clear test during entry,

The authentication progress will be represented by showing asterisks for the password characters.

The following lockout times for invalid password entries are realized to secure the management interface. Every management interface (local and remote) has its own error counter.

Consecutive unsuccessful authentication attempts	Lockout time
3-6	1 Minute
7-10	10 Minuten
11-20	1 Stunde
ab 21	1 Tag

Table 15: Lockout time

To guarantee, that only authorized users has the ability to change secure values of the TOE different user profiles with different rights will be provided by the TOE.

The following profiles are provided by the TOE for user management:

- User
- Administrator
- TOE Reset Administrator

After reset to default settings of the TOE the entry of administrator PIN will be enforced again. All interfaces disabled again until a new administrator PIN is set.

SF.6_TOE_Management

The TOE can be managed via the local and the remote management interface.

The following management functions are executable by all roles

- Display the product version number of the TOE
- View the card terminal name of card terminal
- Display the MAC address of the TOEs network interface
- Perform a TOE self-test
- View the serial number of the TOE

The following management functions are only executable by authenticated TOE administrators:

- Management of available network configuration
- Set card terminal name of card terminal
- Manage local and remote management login credentials
- Deletion of Pairing information from all three possible pairing processes
- Manage the list of TSP CAs
- Perform a firmware update
- Enable/Disable the remote management interface
- Enable/Disable reset to factory defaults without user authentication
- Perform the possible pairing process with the connector
- Enable/Disable administrative SICCT commands (e.g. perform firmware update)

The following management function is executable by authenticated TOE administrators using the SICCT Interface:

- Perform a firmware update
- Perform a TSP CA list update

The following management functions are executable by authenticated TOE administrators only by using the local management interface:

- Enable/disable the remote management interface
- Perform the possible pairing processes with the connector
- Enable/disable reset to factory defaults without user authentication
- Enable/disable administrative SICCT commands (e.g. perform firmware update)
- Reset to factory defaults

The following management functions are executable only by authenticated TOE administrators using the remote management interface (Web interface)

- Manage remote management login credentials (for the Web interface)
- Manage remote management login credentials (for the SICCT interface)

The TOE ensures that only secure values are accepted for security settings. Security relevant settings by default disabled after initial start-up and can only by enabled by an authorized TOE administrator.

The following settings are by default disabled after initial start-up

- Remote management interface
- Remote firmware update functionality
- Reset to default settings without authentication

The following management function is executable only by authenticated TOE Reset administrators using the local management interface:

- Reset to factory defaults (fallback)

The management function “reset to factory defaults” can be executed without authentication but it is organizational reserved for authorized TOE administrators only. [5]

SF.7_Protection_against_Counterfeiting

At initial start-up and at every restart of the TOE, the following self-test will be executed:

- check whether the SM-KT is active and an access to the card is possible
- calculating and checking of the hash value of the implemented firmware
- known answer test of cryptographic algorithm

The integrity check of the implemented firmware can be initiated by any user.

Different TSF elements protect the following sensitive parts of the TOE.

- *smart card interfaces*
- *I/O circuits necessary for the internal transfer of the PIN and TSF-Data*
- *Memory Chip for the storage of TSF-Data*

After disconnection from the mains the monitoring of the TSF elements is furthermore powered by batteries.

A detected intrusion leads to a message to the user on the display.

A reset of this message is not possible. Security relevant functions of the TOE are no longer available.

Even an attacker with moderate attacking potential has not the ability to bypass this security function.

7.2 TOE Security measures

SM.1_Sealing

The housing is sealed by means of authentic and unforgeable security seals, which will be destroyed during removal.
The nature (destruction property) of the seal ensures that it cannot be removed and reapplied undamaged.
The used seal is unforgeable, has authenticity features and fulfills the security level 2 regarding BSI 7586 (Anforderungen und Prüfbedingungen an Sicherheitsetiketten) and is listed under BSI 7500 product list.
Sealing surfaces provided at the smart card slots for SMC-B and SM-KT.
These surfaces are so designed that an administrator can seal the slots and the seals are in the visible range of the user during operation condition.

7.3 Rationales

7.3.1 Rationale of the TOE summery specification

7.3.1.1 Security Functions and Security Requirements

FCS_CKM.1 /Connector
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by using RSA, ECC and SHA 256 with appropriate key size for key generation used for a secure connection of the SICCT- Interface.

FCS_CKM.1 /Management
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by using RSA, ECC and SHA 256 with appropriate key size for key generation used for a secure connection of the management interface.

FCS_CKM.4
The TSF ***SF.1_Secure_Communication*** satisfies this SFR through the implementation of a secure key destruction method by overwriting the key values with zero values.

FCS_COP.1/Con_Sym
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by using AES with appropriate key size for symmetric cryptographic operations.

FCS_COP.1/SIG
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by using RSA and ECC with appropriate key size for signature verification.

FCS_COP.1/Management
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by using AES with appropriate key size for encryption of the communication via the remote management interface.

FCS_COP.1/SIG_FW
The TSF ***SF.4_Secure_Update*** satisfies this SFR by using RSA and SHA256 with appropriate key size for signature verification during the firmware update process.

FCS_COP.1/SIG_TSP
The TSF ***SF.1 SF.1_Secure_Communication*** satisfies this SFR by using RSA and SHA256 with appropriate key size for signature verification of TSP CA lists.

FDP_ACC.1 /Terminal
The TSF ***SF.1_Secure_Communication***, ***SF.3_Secure_PIN_entry*** and the TSF ***SF.4_Secure_Update*** satisfy this SFR by enforcing the terminal SFP. The TSF allows all subjects to read or modify defined objects.

FDP_ACC.1 /Management
The TSF ***SF.5 User_Authentication*** and the TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Management SFP. The TSF allows defined user execute explicit management functions.

FDP_ACF.1 /Terminal
The TSF ***SF.1_Secure_Communication***, ***SF.3_Secure_PIN_entry*** and the TSF ***SF.4_Secure_Update*** satisfy this SFR by enforcing the terminal SFP. The TSF allows users with defined roles to access determined objects.
FDP_ACF.1 /Management
The TSF ***SF.5_User_Authentication*** and the TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Management SFP. The TSF allows users with defined roles to execute explicit management functions via defined management interfaces.

FDP_IFC.1/PIN

The TSF ***SF.3_Secure_PIN_entry*** satisfies this SFR by enforcing the PIN SFP. The TSF enforces the SFP on the defined subjects for an entered PIN.

FDP_IFF.1/PIN
The TSF ***SF.3_Secure_PIN_entry*** satisfies this SFR by enforcing the PIN SFP. The TSF ensures that a PIN will be forwarded only to the related smart card and will never leave the TOE by other ways.

FDP_IFC.1/NET
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by enforcing the NET SFP. The TSF enforces the SFP on the defined subjects for all information arriving the network interface.

FDP_IFF.1/NET
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by enforcing the Net SFP. The TSF enforces, that sensitive information arriving at the network interface will only be accepted after establishing a trusted channel.

FDP_RIP.1
The TSF ***SF.2_Memory_Rework*** satisfies this SFR by ensuring that information will be deleted after deallocation of the resource

FIA_AFL.1
The TSF ***SF.5_User_Authentication*** satisfies this SFR by detecting unsuccessful authentication attempts. Defined lockout times will be realized after a defined number of unsuccessful authentication attempts for different user interfaces.

FIA_ATD.1
The TSF ***SF.5_User_Authentication*** satisfies this SFR by maintaining different roles to individual users.

FIA_SOS.1
The TSF ***SF.5_User_Authentication*** satisfies this SFR by providing a mechanism to verify that the entered password for TOE management meet the specified requirements.

FIA_UAU.1
The TSF ***SF.6_TOE_Management*** satisfies this SFR by requiring no authentication of the user for defined TSF mediated actions.

FIA_UAU.5
The TSF ***SF.6_TOE_Management*** satisfies this SFR by providing different authentication mechanism for different management interfaces.

FIA_UAU.7
The TSF ***SF.5_User_Authentication*** satisfies this SFR by providing only protected authentication feedback during authentication. The TSF ensures that only asterisks will be displayed during authentication is in progress.

FIA_UID.1
The TSF ***SF.6_TOE_Management*** satisfies this SFR by requiring no identification of the user for defined TSF mediated actions.

FMT_MSA.1 /Terminal
The TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Terminal SFP. The TSF restricts the ability of authorized roles to manage all security attributes of the Terminal SFP.

FMT_MSA.1 /Management
The TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Management SFP. The TSF restricts the ability of TOE administrators to manage the security attribute roles.

FMT_MSA.2
The TSF ***SF.6_TOE_Management*** satisfies this SFR by accepting only secure values for roles.

FMT_MSA.3 /Terminal
The TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Terminal SFP. The TSF provide restrictive default values for security attributes. The TSF allows no roles to specify alternative initial values.

FMT_MSA.3 /Management
The TSF ***SF.6_TOE_Management*** satisfies this SFR by enforcing the Management SFP. The TSF provide restrictive default values for security attributes. The TSF allows no roles to specify alternative initial values.

FMT_SMF.1
The TSF ***SF.6_TOE_Management*** satisfies this SRF by providing only specific management functions.

FMT_SMR.1
The TSF ***SF.5_User_Authentication*** satisfies this SFR by maintaining the roles user, administrator and TOE Reset Administrator.

FPT_FLS.1
The TSF ***SF.1_Secure_Communication*** and ***SF.4_Secure_Update*** satisfies this SFR by preserving a secure state of the TOE in fact of identified failures. The TSF preserve a secure state after disconnecting of the connector, failure during firmware update, failure during TOE self-test, disconnection of the SM-KT.

FPT_ITT.1
This SFR is satisfied by the design of the TOE. The TOE does not comprise of physically separated parts.

FPT_PHP.1
This SFR is satisfied by the security measure ***SM.1_Sealing***. The used seals are sufficient to detect whether the housing of the TOE has been opened.

FPT_PHP.2
The TSF ***SF.7_ Protection_ against_Counterfeiting*** satisfies this SFR by notifying all users after detecting of a physical tampering.

FPT_TST.1
The TSF ***SF.7_Protection_against_Counterfeiting*** satisfies this SFR by enforcing self-test of cryptographic algorithm and checking of the hash value of the firmware.

FTA_TAB.1/SEC_STATE
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by displaying a closed padlock symbol to the user, to indicate that the TOE is in a secure state.

FTP_ITC.1 /Connector
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by establishing an encrypted channel to a connector by mutual authentication which is only used by eHealth applications.

FTP_TRP.1 /Management
The TSF ***SF.1_Secure_Communication*** satisfies this SFR by providing an encrypted communication channel for authorizes user to manage the TOE.

	SF.1_ Secure_Communication	SF.2_ Memory_ Rework	SF.3_ Secure_ PIN_	SF.4_ Secure_ Update	SF.5_ User_ Authentication	SF.6_ TOE_	SF.7_ Protection_

			entry			Manage-ment	against_ Counterfeiting
Cryptographic Support							
FCS_CKM.1 /Connector	X	-	-	-	-	-	-
FCS_CKM.1 /Management	X	-	-	-	-	-	-
FCS_CKM.4	X	-	-	-	-	-	-
FCS_COP.1/Con_Sym	X	-	-	-	-	-	-
FCS_COP.1/SIG	X	-	-	-	-	-	-
FCS_COP.1/Management	X	-	-	-	-	-	-
FCS_COP.1/SIG_FW	-	-	-	X	-	-	-
FCS_COP.1/SIG_TSP	X	-	-	-	-	-	-
User data protection							
FDP_ACC.1 /Terminal	X	-	X	X	-	-	-
FDP_ACC.1 /Management	-	-	-	-	x	x	-
FDP_ACF.1 /Terminal	X	-	X	X	-	-	-
FDP_ACF.1 /Management	-	-	-	-	x	x	-
FDP_IFC.1/PIN	-	-	X	-	-	-	-
FDP_IFF.1/PIN	-	-	X	-	-	-	-
FDP_IFC.1/NET	X	-	-	-	-	-	-
FDP_IFF.1/NET	X	-	-	-	-	-	-
FDP_RIP.1	-	X	-	-	-	-	-
Identication and Authen.							
FIA_AFL.1	-	-	-	-	X	-	-
FIA_ATD.1	-	-	-	-	X	-	-
FIA_SOS.1	-	-	-	-	X	-	-
FIA_UAU.1	-	-	-	-	-	X	-
FIA_UAU.5	-	-	-	-	-	X	-
FIA_UAU.7	-	-	-	-	X	-	-
FIA_UID.1	-	-	-	-	-	X	-
Security Management							
FMT_MSA.1 /Terminal	-	-	-	-	-	X	-
FMT_MSA.1 /Management	-	-	-	-	-	X	-
FMT_MSA.2	-	-	-	-	-	X	-
FMT_MSA.3 /Terminal	-	-	-	-	-	X	-
FMT_MSA.3 /Management	-	-	-	-	-	X	-
FMT_SMF.1	-	-	-	-	-	X	-
FMT_SMR.1	-	-	-	-	X	-	-
Protection of the TSF							
FPT_FLS.1	X	-	-	X	-	-	-
FPT_ITT.1	-	-	-	-	-	-	-
FPT_PHP.1	-	-	-	-	-	-	-
FPT_PHP.2	-	-	-	-	-	-	X
FPT_TST.1	-	-	-	-	-	-	X
TOE Accesss							
FTA_TAB.1/SEC_STATE	X	-	-	-	-	-	-
Trusted path /channels							
FTP_ITC.1 /Connector	X	-	-	-	-	-	-
FTP_TRP.1 /Management	X	-	-	-	-	-	-

Table 16: Mapping of Security Requirements to Security Functions

7.3.1.2 Security requirements and security measures

	Sicherheits-maßnahmen	Sicherheits-anforderungen	Kommentar

SM.1	SM.1_Sealing	FPT_PHP.1 FPT_ITT.1	In addition to the security function SF.7_Protection_against_counterfeiting" is the requirement "Protection against physical manipulation" of the TOE guaranteed by the security measure (SM.1)

Table 17: Security measures / Security requirements

8. Glossary and Acronyms

Term	Definition
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
DF.KT	Dedicated File Kartenterminal
eHC	Electronic Health Card
gSMC-KT	Gerätespezifisches Security Module Card Type Kartenterminal
ITE	Information Technology Equipment
HPC	Health Professional Card
KSR	Configuration and Software repository- Service of the telematic infrastructure
LAN	Local Area Network
PP	Protection Profile
SOF	Strenght of Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable ChipCard Terminal
SM-KT	Sicherheitsmodul Kartenterminal
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	Trust-Service Provider that issues connector certificates

9. Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; 3.1, Revision 4, September 2012

[4] AGD documentation, Quick Guide for Users (6440649-04, DE, Feb. 2018)

[5] AGD documentation, Administrator Manual (6440650-04, DE, Feb. 2018)

Cryptography

[6] BSI TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 3.17 10.09.2013

[7] RFC 4346 The Transport Layer Security (TLS) Protocol. Version 1.1

[8] RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

[9] RFC 5246 The Transport Layer Security (TLS) Protocol, Version 1.2

[10] Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2012 March

[11] RFC 2104 HMAC: Keyed-Hashing for Message Authentication

[12] Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082. Bundesamt für Sicherheit in der der Informationstechnik (BSI)

[13] Common Criteria Protection Profile – Schutzprofil 2: Anforderungen an den Konnektor Online Rollout (Stufe 1), BSI-CC-PP-0046, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Specifications

[14] gematik - Spezifikation eHealth-Kartenterminal, Version 3.15.0, 16.05.2022

[15] TeleTrusT SICCT-Spezifikation as referenced by [14]

[16] BSI TR-03120 “Sichere Kartenterminalidentität” Version 1.1 vom 09.07.2010

[17] BSI TR-03120 „Anhang: Sichere Kartenterminalidentität“ zur Technischen Richtlinie BSI TR-03120; Version 1.0.2 vom 04.04.2008.

[18] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT); BSI-CC-PP-0032-V3-2016; Version 3.7 vom 21. September 2016.

[19] gematik - Übergreifende Spezifikation Operations und Maintenance, Version 1.14.0, 26.06.2020

[20] gematik - Spezifikation der gSMC-KT Objektsystem, Version 4.3.0, Stand: 12.05.2022

[21] Konzept Architektur der TI- Plattform, Version 1.5.0 Stand 23.07.2015

[22] Regulation No 910/2014 of the European Parliament of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

[23] gematik - Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.23.0, 20.09.2022