Security Target EAL3+ for eHealth Terminal ST-1506

Zertifizierung ID:	**[BSI-DSZ-CC-1124-V3]**
Version:	**5.5**
Date:	**2023-04-19**

DOCUMENT HISTORY

Version	Date	Description
1.0	2019-06-29	Initial release version
1.1	2019-07-03	Updated for (missed) review comments
1.2	2019-09-23	OR
1.3	2020-01-09	Updated according to OR v2
1.4	2020-01-13	Updated errors and re-worked application notes
1.5	2020-02-04	Updated according to evaluator feedback, adjusted to gematik specification release R3.1.2 from 26/11/2019
1.6	2020-03-06	Updated according to OR v3
1.7	2020-04-30	Updated according to OR v4
1.8	2020-15-05	Updated according to OR v5
1.9	2020-05-19	Updated according to OR v6
2.0	2020-07-06	Updated according to 1124_ZK_ASE_V1
2.1	2020-07-31	Adjusted FPT_PHP.3, minor corrections
2.2	2020-09-04	Updated according to OR v9
2.3	2020-09-16	Revised ch.1.4
2.4	2020-09-24	Updated according to OR v10
2.5	2020-10-16	Updated secure element details
2.6	2020-11-06	Small corrections added
2.7	2020-12-04	Adjustments in ch.3 to better match PP wording, added cipher-suites for remote management access
2.8	2020-12-17	Added reference to BSI-CC-PP-0098-2020
2.9	2020-12-17	Added reference to NSCIB-CC-180212-CR2
3.0	2020-12-18	Corrected reference to NSCIB-CC-180212-CR2

3.1	2021-01-25	Adjusted TOE summary specification
3.2	2021-02-19	Updated checksum for guidance documentation
3.3	2021-03-10	Updated AGD reference
3.4	2021-05-26	Layout update, minor corrections. Changes for gematik release 4.0.2. USB host for PIN-Pad accessory.
4.0	2021-10-04	First draft version FW 3.0.0 Update of references and deletion of unused cipher suites Accessory support not in this version
4.1	2021-10-18	Introduction of VPN connection to a Konnektor and remote SMC-B PIN entry via management interface Deletion of all descriptions for an accessory
4.2	2021-11-08	Minor corrections in accordance with OR v1
4.3	2021-11-23	Update of “Zertifizierung ID”
4.4	2021-12-20	Corrections in accordance with OR v3
4.5	2022-01-17	Changes in accordance with OR v4 Deletion of unused algorithm with SM-KT (ch. 6.1.1.5)
4.6	2022-03-08	Integration of PCB version from maintenance for STUSB4500_5.1k_Replacement
4.7	2022-03-23	Adding application note to FDP_IFF.1.4/NET
4.8	2022-04-06	New hash values and preferences for AGD updates
5.0	2022-08-09	First draft version FW 4.0.0 USB host and additions for PIN-Pad accessory
5.1	2022-10-11	Changes of PIN-Pad scope Minor corrections
5.2	2022-11-28	Corrections in accordance with OR v1
5.3	2023-02-09	Minor corrections in accordance with OR_ADV_v2
5.4	2023-03-06	Updates for new AGD
5.5	2023-04-19	Note for 6.1.4.6 FMT_SMF.1

TABLE OF CONTENTS

Document History 2
Table of Contents 4
1 ST Introduction 6
1.1 ST Reference 6
1.2 TOE reference 6
1.3 TOE Overview 6
1.3.1 TOE type 7
1.3.2 Required non-TOE hardware/software/firmware 8
1.4 TOE Description 8
1.4.1 TOE major security features for operational use 10
1.4.2 TOE Reset Administrator authentication 12
1.4.3 Physical Scope of the TOE 13
1.4.4 Logical Scope of the TOE 13
2 Conformance Claims 14
2.1 ST Claim 14
2.2 PP Claim 14
2.3 Package Claim 14
2.4 Conformance Claim Rationale 15
2.5 Assumptions 15
3 Security Problem Definition 16
3.1 Introduction 16
3.2 Assets 16
3.3 Threats 18
3.4 Organizational Security Policies 20
3.5 Assumptions 20
4 Security Objectives 23
4.1 Security Objectives for the TOE 23
4.2 Security Objectives for the Operational Environment 27
4.3 Security Objectives Rationale 30
4.3.1 Countering the threats 30
4.3.2 Covering the OSPs 32
4.3.3 Covering the assumptions 32
5 Extended Components Definition 32
6 Security Requirements 33
6.1 Security Functional Requirements for the TOE 33
6.1.1 Cryptographic Support (FCS) 35

6.1.2 User data protection (FDP) 39
6.1.3 Identification and Authentication (FIA) 48
6.1.4 Security Management (FMT) 51
6.1.5 Protection of the TSF (FPT) 55
6.1.6 TOE Access 56
6.1.7 Trusted path/channels (FTP) 56
6.2 Security Assurance Requirements for the TOE 58
6.3 Security Requirements Rationale 59
6.3.1 Security Functional Requirements Rationale 59
6.3.2 SFR Dependency Rationale 62
6.3.3 Security Assurance Requirements Rationale 65
6.3.4 Security Requirements – Mutual Support and Internal Consistency 65
7 TOE summary specification (ASE_TSS) 66
7.1 Trusted Communication Channels 66
7.2 Identification & Authentication 66
7.3 Secure PIN-entry 68
7.4 Network Connections 68
7.5 Secure Update 69
7.6 Secure Data Deletion 69
7.7 Secure Management Functions 70
7.8 Self-Test 73
7.9 Secure Fail-State 73
7.10 Physical Protection of the TOE 73
7.11 SFR Implementation Overview 74
8 Glossar 75
9 References 76

1 ST INTRODUCTION

1.1 ST REFERENCE

Certification ID	BSI-DSZ-CC-1124-V3
CC-Version	3.1
Protection Profile Reference	**BSI-CC-PP-0032-V2-2015-MA01 (21.09.2016)**
Evaluation Assurance Level	EAL 3, augmented by **ADV_FSP.4**, **ADV_IMP.1**, **ADV_TDS.3**, **ALC_TAT.1** and **AVA_VAN.4**
Document	**Security Target for the eHealth Terminal ST-1506**
Document Issue	5.5
Date	2023-04-19

1.2 TOE REFERENCE

Target of evaluation	eHealth Card Terminal with Touchscreen Display
Product-ID:	ST-1506 AFxZ *The TOE has different certified variants, 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, ST-1506 AFHZ for white and ST-1506 AFEZ for black color. Every variant has the same TOE version. The TOE version is 4.0.0:4.0.0. It consists of the firmware version (4.0.0) and the hardware version (4.0.0) and can be displayed by user's request.* *The TOE hardware in version 4.0.0 has different variants of the internal PCB of the mainboard, due to different placement options without changing the functionality. The TOE hardware version 4.0.0 consists of the PCB versions 2.2.7 or 2.2.8.*
TOE Version	4.0.0:4.0.0
Developer and Manufacturer	Theobroma Systems Design und Consulting GmbH
Brand/Vendor	Cherry Digital Health GmbH

1.3 TOE OVERVIEW

This Security Target defines the security objectives and requirements for the Electronic Health Card Terminal (eHCT) eHealth Terminal ST-1506 based on the regulations for the German healthcare system. It uses a 5" touchscreen display (720x1280) for user-interaction and pin-entry.

For further information about card compatibility, please see [gemSpec_KT].

It addresses the security services provided by this terminal:

- The access to one or more slots for smart cards
- Secure network connectivity
- Secure PIN entry functionality
- Encryption of communication
- User authentication
- Management functionality including update of Firmware
- Passive physical protection
- Active physical protection

1.3.1 TOE TYPE

The TOE is a stand-alone desktop card terminal for stationary use and thus the physical scope of the TOE comprises:

- The terminal hardware provides the following physical interfaces:
  - card slot (ID-1) for a eGK,
  - card slot (ID-1) for a HPC,
  - 2 card slots (ID-000) for SMC-B and gSMC-KT,
  - 720x1280 (portrait) touchscreen display,
  - status LED to signal secure pin-entry mode,
  - 10/100 Ethernet interface (RJ45),
  - USB host interface for optional PIN-Pad accessory,
  - USB device interface,
- the update file with application firmware and
- related guidance documents.

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

The SM-KT is a necessary requirement in the operational environment of the TOE as the TOE relies on the services of the SM-KT for its cryptographic functionality.

During the delivery and setup phase the SM-KT has to be installed into the card terminal. Functionality that is relying on the SM-KT for secure operation will not work as intended before the SM-KT is installed. The setup procedure requires a remote connection to the TOE. The cryptographic functionality for securing communication of the remote management interface is only available after the SM-KT has been inserted into the TOE.

The cryptographic identity of the TOE is provided by the SM-KT, as is functionality for encryption/decryption, signature generation and signature verification.

An integrated secure element is used as generator for secure random numbers which in turn are used to generate secure cryptographic keys for secure connections and to store the pairing secrets.

The guidance documentation is an integral part of the TOE as it describes in detail the requirements on a secure environment for the TOE setup process and it describes in detail how to perform a secure setup.

1.3.1.1 Secure Element

The secure element is a NXP SE050, i.e. a micro controller and a software stack which is stored on the micro controller and which can be executed by the micro controller. The software stack provides a Java Card Virtual Machine [JAVACARD], that serves as a execution environment for a project specific Java Card applet.

The SE050 includes a DRG.3 compliant pseudo-random number generator according to [BSI_AIS20_AIS31], which can be accessed by the Java Card applet. The applet provides an API to other system components to obtain the entropy from that PRNG. The generated random numbers are used as entropy source for generation of cryptographic keys in the TOE.

The secure element has the following properties:

- Name: JCOP 4 SE050 v4.7 R2.00.11
- Certification ID: NSCIB-CC-180212-CR5 [JCOP4_CC]
- Certification level: EAL6+ (HW and Java Card runtime)
- DRG.3 compliant pseudo-random number generator according to [BSI_AIS20_AIS31]

1.3.2 Required non-TOE hardware/software/firmware

The TOE can be managed via a web interface. To operate the web interface the user has to be able to establish a TLS secured connection to the TOE via LAN and IPv4 and has to use a web browser that can establish a TLS connection.

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. Although this secure module is physically placed within the case of the TOE it does not belong to the logical and physical scope of the TOE.
- a host system (eHealth Konnektor) which is necessary for a secure communication between the local network and the remote network of the telematics infrastructure.
- Local Area Network (LAN)

The security function *SF.Secure_Communication* is only available after a SM-KT is installed because of the cryptographic identities of the SM-KT.

1.4 TOE Description

The TOE is the card terminal eHealth Terminal ST-1506 with 2 ID1 Slots (HPC and eGK) und 2 SMC Slots (SM-KT (supporting SMC-B and SMC-KT cards) and SMC-A), 720p touchscreen (also used for secure pin entry) and LAN interfaces for the use in the German healthcare system with HPC and eGK.

Connection to a host computer is via LAN and TCP/IP-protocol (IPv4), by a connection using an eHealth Konnektor.

FIGURE 1.1: TOE

The Target of Evaluation (TOE) described in this Security Target is a smart card terminal which fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system. Please refer to see [gemSpec_KT] for further information about card compatibility. This terminal is based on the specification for a “Secure Interoperable Chip-Card terminal” ([SICCT]) extended and limited by the specifications for the e-Health terminal itself (see [gemSpec_KT]).

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 means to securely enter a PIN. The TOE provides a network interface which allows routing the communication of a smart card to a remote IT product outside the TOE.

The TOE provides the following main functions:

- Access to one or more slots for smart cards
- Secure network connectivity
- Secure PIN entry functionality
- Enforcement of the encryption of communication
- User authentication
- Management functionality including update of Firmware
- Passive and active physical protection

The TOE for use in the German health care is based on the specification SICCT [SICCT], which is adapted for operation by profiling as eHealth card terminal (see [gemSpec_KT]).

The TOE works with a cryptographic key for authentication, integrity assurance and to ensure the confidentiality of data transmitted over the LAN interface. Due to the very high protection requirements of the information objects transmitted over the LAN interface, a secure key store (SM-KT) is required for the key. As physical characteristics of the SM-KT the TOE supports SMC-B and gSMC-KT cards.

The interfaces of the TOE are provided in Figure 1.2: TOE-Boundary showing a schematic representation:

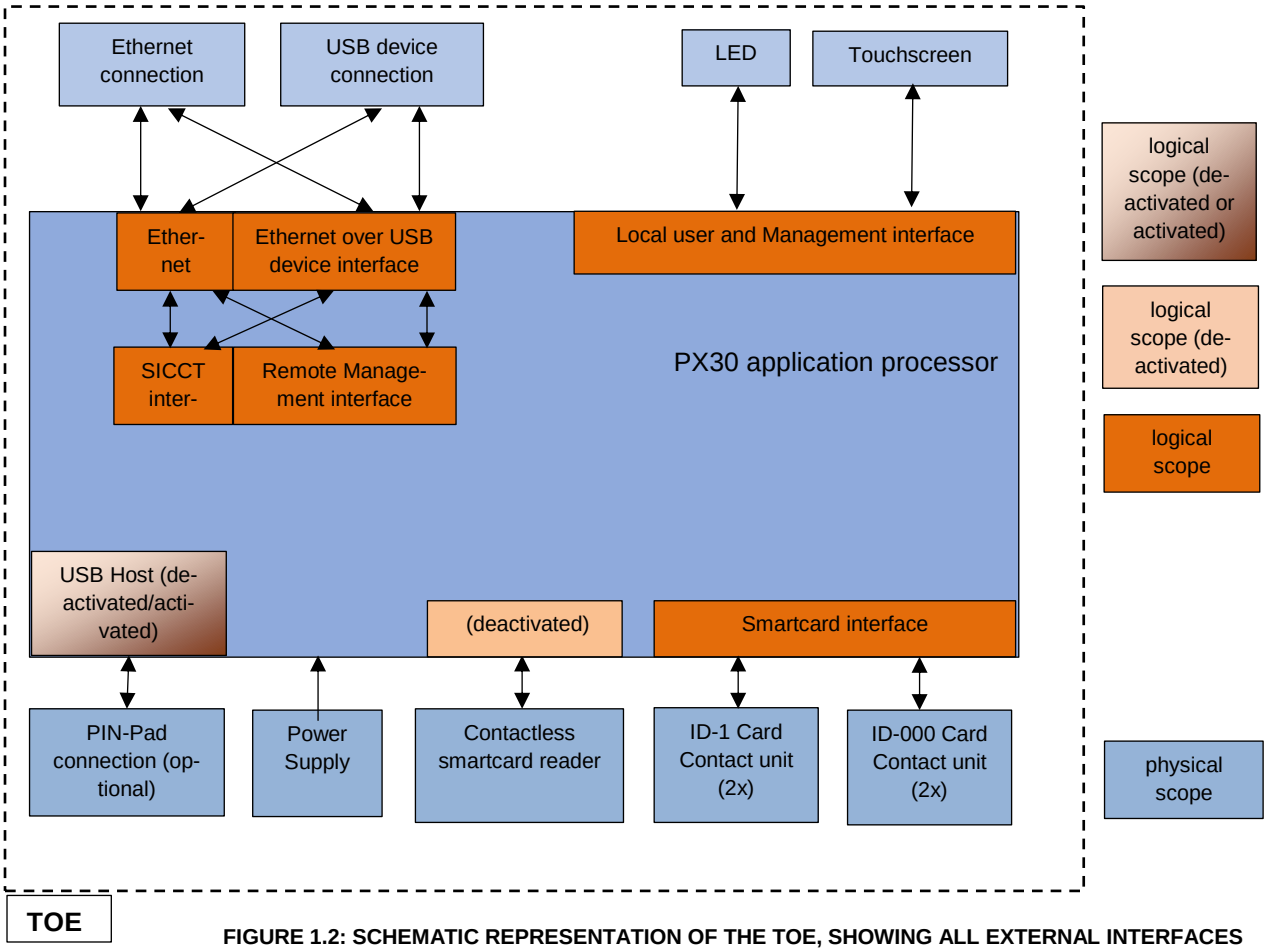

FIGURE 1.2: SCHEMATIC REPRESENTATION OF THE TOE, SHOWING ALL EXTERNAL INTERFACES

1.4.1 TOE MAJOR SECURITY FEATURES FOR OPERATIONAL USE

To protect the communication between the connector and the TOE the TOE has to possess a cryptographic identity (in form of a X.509 certificate) and functionality for encryption/decryption as well as signature creation based on RSA or ECC (see also [gemSpec_KT]).

For its cryptographic functionality the TOE relies on the services of the so called SM-KT.

The SM-KT (Secure Module Kartenterminal) is a secure module that represents the cryptographic identity of the TOE in form of a X.509 certificate.

This module - in form of an ID-000 smart card – provides:

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

Though this SM-KT will be physically within the body of the TOE (inserted into one of the 2 ID-000 contact card slots) it does not belong to the logical and physical scope of the TOE as to see in Figure 1.2. More information about the SM-KT can be found in the corresponding gematik card specification.

The TOE supports RSA and ECC cryptography for a TLS connection, see [gemSpec_Krypt], ch. 5.8. The usage of ECC cryptography for encryption/decryption and signature creation depends on the version of the SM-KT in the TOE.

For the case the TOE uses a DF.KT of a gSMC-KT or SMC-B as SM-KT, which is addressable via the connector, the TOE accesses this DF.KT via the base-channel 0. During use of the SM-KT by the TOE, the terminal card commands of the TOE are preferential and the processing of possibly existing client SICCT commands is interrupted and continued only after completion of the internal command sequence.

The TOE provides functionality to update its firmware. The configuration, such as terminal type, IP address or pairing-information is preserved and indicated after a firmware update (see [gemSpec_KT] for further information). The TOE does not provide functionality to downgrade its firmware. If the TOE is provided a firmware downgrade, the TOE refuses to change the firmware. Therefore no administrator warning in case of downgrade is necessary.

Firmware update can also be triggered remotely from a trusted Push Server in the internal network of the medical supplier.

In addition to the cryptographic identity of the TOE, the TOE stores a shared secret which is generated by the connector and transferred to the TOE during the pairing process of TOE and connector. This shared secret is not stored in the SM-KT, but in a separate storage area of the TOE. As the SM-KT might be removed and placed into another card terminal, the shared secret is necessary to ensure that communication to the connector is performed using the already paired card terminal (the TOE). The whole identity of the TOE is therefore represented by the SM-KT certificate AND the shared secret. Please note that as part of the pairing process, there are three processes:

- Initial pairing: This provides a logical connection from the perspective of the connector by using shared secret between card terminal and SM-KT
- Review of pairing-information: The connector checks as a second step of authentication, if the card terminal is in the possession of the shared secret after establishing the TLS connection.
- Maintenance-pairing: Announcement of a new connector certificate on the card terminal by using a known shared secret. Please see [gemSpec_KT]) for further information on the pairing process.

Not part of [eHCT-PP] is the functionality of the TOE to provide a restricted VPN client for the establishment of a single VPN connection to a remote connector behind a VPN gateway. The VPN tunnel uses IPsec with EAP-TLS or EAP-MSCHAPv2 authentication and is transparent for the remote connector behind the gateway. The usage of the VPN client is restricted to the admin user of the TOE and is not part of any TSF, because the additional VPN did not affect the existing security between the TOE and a connector that consists on the TLS connections in combination with a pairing process between the components. The VPN is only an additional transparent transport layer without impact on the internal security between TOE and connector and can be established outside the TOE (e.g. VPN router) also.

The TOE can be connected to a PIN-Pad accessory compliant with gematik specification [gemSpec_KT], ch. 2.3.20. The PIN-Pad is connected to the TOE via the USB host interface of the TOE or via LAN (PIN-Pad connected via USB to a local PC). Because the PIN-Pad itself is not CC evaluated in compliance with the gematik specification [gemSpec_KT], the TOE is only be evaluated with deactivated PIN-Pad functionality, which is the default configuration of the TOE. The enabling of the PIN-Pad also enables the USB-Host interface, in the default configuration (PIN-Pad disabled) the USB-Host is disabled also. After enabling of the PIN-Pad the TOE is not in a certified mode.

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 cards (SMC, HPC) in the local and the remote card terminal are used to encrypt/decrypt the PIN.

Cryptographic assets and PINs are handled such that when the asset can be deallocated, the memory used is also cleansed. This is often referred as good crypto hygiene and required by the PP.

To ensure secure operation during start-up self-tests are executed to test TSFs being operational.

When a security error is detected the TOE enters a secure fail-state. In this state the TOE disables services to ensure that no security breach is possible. This state is also entered in case of a tamper event.

The TOE defines three users:

1. The TOE Administrator is allowed to configure the device and change security related objects.
2. The TOE Reset Administrator is a user that may execute a factory reset even when the TOE Administrators Credentials are lost.
3. The User is allowed to use the primary services provided by the TOE, i.e. to access a smart card which has been put into one of the slots of the TOE before.

1.4.2 TOE Reset Administrator authentication

In case the TOE Administrator credentials are lost, a Reset to Factory defaults can be executed as follows:

1. The TOE generates a challenge (at least 64 Bit random number) with a restricted life-time.
2. The owner contacts and authenticates at the customer-support-service.
3. The owner transmits the challenge along with the device serial number to the customer-support-service.
4. The customer-support-service uses the challenge **and** device serial number to generate the response and transmits it back to the owner.
5. The owner enters the response.
6. The device checks the response and authenticates the current user as TOE Reset Administrator.

1.4.3 Physical Scope of the TOE

The TOE is a stand-alone desktop card terminal for stationary use and thus the physical scope of the TOE comprises:

- The hardware is the smart card terminal with the physical interfaces:
  - card slot (ID-1) for a eGK,
  - card slot (ID-1) for a HPC,
  - 2 card slots (ID-000) for SMC-B and SM-KT,
  - 5” touchscreen display with 720x1280 resolution,
  - Status LEDs,
  - 1 LAN interface (RJ45),
  - USB host interface for PIN-Pad accessory,
  - USB device interface and
- further parts of the TOE:
  - Quick Guide for Users (64410078) [AGD Quick]

The related Administrator Manual (64410079) [AGD] 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 Adminstrator 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.

The checksum values are as follows:

- for [AGD Quick]:
  e5ad4f7ff69dfed340a3de7e5bdf1cb7dedb29f35c337bc4a26c48b5564dba57
- for [AGD]:
  0dc1d4953fd740e398b13f24286bad9e5e007c5b1751dd328ffe0550b2602d51

1.4.4 Logical Scope of the TOE

The logical scope of the TOE is represented by its core security features:

- Access to one or more slots for smart cards,
- Secure network connectivity
- Secure PIN entry functionality,
- Enforcement of the encryption of communication,
- User authentication,
- Management including update of Firmware
- Passive physical protection

and is limited by the functionality for which the TOE relies on the services of the SM-KT.

As an augmentation of the logical scope of the TOE listed above, the functionality of the TOE comprises:

- Active physical protection of the TOE against probing and drilling attacks. It reacts by raising an alarm to prevent usage of a potentially attacked device.

2 CONFORMANCE CLAIMS

2.1 ST CLAIM

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5, 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 5, 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, 2017

as follows:

- Part 2 conformant,
- 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.

The design of the TOE takes into account the [TR-03120] concerning security seals and case design.

2.2 PP CLAIM

This Security Target is strictly conformant to the Protection Profile *Common Criteria Protection Profile Electronic Health Terminal (eHCT), BSI-CC-PP-0032-V2-2015-MA01, Version 3.7, 21.09.2016*.

2.3 PACKAGE CLAIM

The Security Target is conformant to the following security requirements package:

- Assurance package EAL3 augmented by
  - ADV_FSP.4,
  - ADV_IMP.1,
  - ADV_TDS.3,
  - ALC_TAT.1, and
  - AVA_VAN.4.

2.4 Conformance Claim Rationale

This Security Target is strictly conformant to the Protection Profile *Common Criteria Protection Profile Electronic Health Terminal (eHCT), BSI-CC-PP-0032-V2-2015-MA01, Version 3.7, 21.09.2016*.

- Threats in the ST are identical to the threats in the PP.
- OSPs in the ST are identical to the OSPs in the PP.

2.5 Assumptions

Assumptions in the ST are identical to the Assumptions in the PP.

3 Security Problem Definition

3.1 Introduction

3.2 Assets

The following assets need to be protected by the TOE as long as they are in the scope of the TOE:

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 and further: firmware update data, certificates, data to be signed, card commands, SICCT commands including display messages. This asset is user data.
Configuration data	Data on which the TOE relies on for its secure operation. This data comprises at least the management credentials for local and remote management and the list of TSP CAs. This asset is user data.

Asset	Description
	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.
TSF Data	The TOE stores TSF data which is necessary for its own operation: shared secrets, public key for firmware update validation, and the TOE software. The TOE has to ensure the confidentiality and authenticity of this data. This asset is TSF data.

Table 1: Assets

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) 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 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

Subject	Description
	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 based on RSA or ECC 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.[1] 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.

[1] The functionality offered to the TOE Reset Administrator is always a complete reset to factory settings, not resetting specific TOE settings only.

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 paths 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 Organizational Security Policies

The TOE shall be implemented according to the following specifications:

Policy	Description
OSP.PIN_ENTRY	The TOE shall fulfil the requirements to be used as a secure PIN pad entry device for applications according to [gemKPT_Arch_TIP]. 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: Organisational 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.

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 a mutual authentication. It is assumed that the connector has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [Konn-PP]. 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. The developer may queue the interrupts internally or implement error messages as answers to the commands. 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 (TOE (according to [TR-03120]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [COS-PP] and complies with the specification [gemSpec_gSMC-KT_ObjSys] or [gemSpec_gSMC-KT_ObjSys_G2.1][2].
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 [gemSpec_KT]. 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

[2] For the COS Protection Profile and the Object System Specification the current versions were chosen by the ST author, as the versions referenced in [eHCT-PP] are outdated.

4 SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the environment of the TOE.

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 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[3].

[3] It should be noted that the scope of the identification and authentication 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, a TLS secured remote management interface, and management over SICCT interface. A firmware consists of two parts: firstly the so-called “firmware list” and secondly the “firmware core” which includes the whole firmware except the firmware list. Firmware lists and cores have to versioned independently. The firmware list states all firmware core versions to which a change is allowed: An update of the firmware core is only allowed if the core version is included in the firmware list. 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.[4] • The configuration, such as terminal type, IP address or pairing-information shall be preserved and indicated after a firmware update ~~or a downgrade~~ (see [gemSpec_KT] 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.

[4] As the TOE does not support firmware downgrade, the objective O.MANAGEMENT was modified not to require firmware downgrade.

Objective	Description
	The developer- specific update component shall warn the administrator about taking the responsibility in case of performing a downgrade.[5] 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 telematics 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 [gemSpec_KT]. The TOE 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. Only functions to identify the TOE in the network (service discovery) may be available without a secure channel.
O.STATE	In principle it would be possible that a card terminal compliant to the Protection Profile [eHCT-PP] realises more than just the necessary set of functionality as required by the [eHCT-PP]. However, additional functionality that is not security functionality (e.g. value-added modules) may lead to an insecure state of the TOE as the user may be not aware of the fact that they are using a functionality, which doesn't fall into the scope of the certified

[5] This part of the objective will be fulfilled trivially, as the TOE does not support firmware downgrade.

Objective	Description
	TOE or because a part of the security functionality as required by this PP is not working during its use. Thus the TOE shall be able to indicate whether it is currently in a secure state, i.e. whether all TSF as required by this PP are actually enforced.[6]
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[7]. It has to be ensured that any kind of physical tampering that might compromise the TSP 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 • 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.

[6] This objective is trivially fulfilled as 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] Please note that the SM-KT provides its own physical protection for the stored keys. However according to [eHCT-PP] 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.

Table 6: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

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

Objective	Description
OE.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, • 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, see also [Konn-PP].
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),

Objective	Description
	• 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). • That the administrator checks the secure state of the TOE regularly[8].
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 Profile [Konn-PP][9]. 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.

[8] The secure state is indicated by messages and LED displayed by the TOE, as defined within the Guidance documentation [AGD].

[9] BSI-CC-PP-0098-2018 (version 1.5.4) was chosen by the ST author, as the PP version referenced in [eHCT-PP] is not consistent with the Konnektor specification version matching [gemSpec_KT].

Objective	Description
	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]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [COS-PP] and complies with the corresponding object system specification [gemSpec_gSMC-KT_ObjSys] or [gemSpec_gSMC-KT_ObjSys_G2.1][10].
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 [gemSpec_KT]. 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

[10] For the COS Protection Profile and the Object System Specification the current versions were chosen by the ST author, as the versions referenced in [eHCT-PP] are outdated.

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

Table 8: Security Objective Rationale

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.[11] 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

[11] Technically, the threat T.F-CONNECTOR is not applicable to this device, since unauthorized reset to factory defaults is not implemented. As the rationale for this threat is more general, and to ensure conformance to [eHCT-PP], this passage is copied from the [eHCT-PP] unchanged.

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 fulfil the requirements to be used as a secure PIN entry device for applications according to [gemKPT_Arch_TIP] (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 (as the TOE has more than one card slot) 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 Extended Components Definition

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

6 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 [CCpart2] are written in italics for assignments, underlined for selections and bold text for refinements. Furthermore the [brackets] from [CCpart2] 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 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	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.3	Resistance to 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 9: Security Functional Requirements for the TOE

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 [*Ephemeral Diffie–Hellman key exchange using TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA; DH group for RSA: 14*; *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1]* and specified cryptographic key sizes *[AES: 128 bit, 256 bit, HMAC-SHA1: 160 bit*] that meet the following: [*[gemSpec_KT], **[gemSpec_Krypt]***].

Hierarchical to: No other components.

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

Referring to application note 1:

The cryptographic session keys, generated by FCS_CKM.1/Connector are used for the TLS encryption/decryption between the TOE and the connector (for further information see [gemSpec_KT] also chapter 6.1.1.4). The generation (actually negotiation) of this key is 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 [gemSpec_KT]) and validation of a shared secret. The TOE determines the role from the connector certificate presented during the buildup of the TLS connection. The TOE checks that the determined role corresponds with the role "Signature Application Component (SAC)" (see [gemSpec_KT]).

The TOE uses the built-in secure element for Random Number generation. It uses the SM-KT for signature generation.

The connection to network based management interfaces will always be secured with TLS Version 1.2.[12]

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 [*Ephemeral Diffie-Hellman key exchange using TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_EC-DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_EC-DHE_RSA_WITH_AES_256_GCM_SHA384; TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA; TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA; DH group for RSA: 14; TLS_ECDHE_EC-DSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_EC-DSA_WITH_AES_256_GCM_SHA384 and curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1*] and specified cryptographic key sizes [AES: *128 bit, 256 bit, HMAC-SHA1: 160 bit, HMAC-SHA256: 256 bit, HMAC-SHA384: 384 bit*], that meet the following: [[*gemSpec_KT*] ,***[gemSpec_Krypt]***].

Hierarchical to: No other components.

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

Referring to PP application Note 2:

The cryptographic session keys, generated by FCS_CKM.1/Management are used for the TLS encryption/decryption for remote management (for further information see [gemSpec_KT] (see also chapter 6.1.1.6). The generation (actually negotiation) of this key is done in accordance with the TLS handshake protocol (for further information see [RFC 5246]), extended and limited by [gemSpec_KT].

The TOE uses the functionality of the built-in secure element for random number generation.

[12] TLS Version 1.2 was chosen by the ST author, as the TLS version 1.1 mandated in [eHCT-PP] is no longer allowed by [gemSpec_KT], but TLS Version 1.2 is mandatory.

The connection to network based management interfaces will always be secured with TLS Version 1.2.

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 [*writing the memory to be deallocated with 0x00]* that meets the following: [*no standard*].

Hierarchical to: No other components.

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

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

FCS_COP.1.1/Con_Sym

The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-CBC*] and cryptographic key sizes [*128 bit or 256 bit*] that meet the following: [*[gemSpec_KT],* ***[gemSpec_Krypt]***].

Hierarchical to: No other components.

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

Referring to application Note 3:

The symmetric cryptographic algorithm in FCS_COP.1/Con_Sym is used to establish the trusted channel with a connector. The cryptographic functionality complies with the requirements of the PKCS#1.

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 [*RSASSA-PKCS1-v1_5 or ECDSA using the curves brainpoolP256r1]* and cryptographic key sizes [*2048 bit for RSA, 256 bit for ECDSA*] that meet the following: [*[gemSpec_KT],* ***[gemSpec_Krypt]***].

Hierarchical to: No other components.

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

Referring to application Note 4:

The signature generation in FCS_COP.1/SIG to establish the trusted channel with the connector is done using the SM-KT (whereas the built-in secure element is used for random number generation, see 6.1.1.1). Further the TOE also verifies 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, AES-GCM*] and cryptographic key sizes [*128bit or 256bit*] that meet the following: [*[gemSpec_KT],* ***[gemSpec_Krypt]***].

Hierarchical to: No other components.

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

Referring to application Note 5:

The cryptographic functionality in FCS_COP.1/Management and FCS_CKM.1/Management is used to establish the trusted path for remote management. The cryptographic functionality complies with the requirements of the PKCS#1 standard.

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 [*ECDSA using the curve brainpoolP384r1]* and cryptographic key sizes [*384 bit*] that meet the following: [*[gemSpec_KT]* **and [TR-03111]**].

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

Referring to PP application Note 6:

The functionality for signature verification is used to check the integrity and authenticity of a potential firmware update. This functionality relies on hashing and encryption using a public key. The public key is part of the installed firmware. The cryptographic functionality complies with the requirements of the PKCS#1 standard.

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 [*ECDSA using the curve brainpoolP384r1*] and cryptographic key sizes [*384 bit*] that meet the following: [*[gemSpec_KT]* **and [TR-03111]**].

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

Referring to PP application Note 7:

The functionality for signature verification is used to check the integrity and authenticity of a potential TSP CA list update. This functionality relies on hashing and encryption using a public key. The public key is part of the installed firmware. The cryptographic functionality complies with the requirements of the PKCS#1 standard.

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
[*notification of physical attacks*]
Operations: read, modify, [*none*]].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

Application Note ST.1: The object “notification of physical attacks” is read-only, therefore no further operations are defined.

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[13]

Objects: PIN, shared secret, management credentials, firmware, cryptographic keys, attribute: firmware version~~***, Enable/Disable the functionality of an unauthorized reset to factory defaults***~~

[TSP CA list, attribute: TSP CA list version]

].

Application Note ST.2: Since “Unauthorized reset to factory defaults” is not implemented, the object is deleted.

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. For the use in the German Healthcare System the named versions must also be approved by the gematik.*

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

- *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[14].*
- *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.[15]

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

- *[none]*

[*none*]

].

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 change its own management credentials.*
- *Only an authorized user should be able to delete the Shared Secret.*

]

[14] Note: This part of the SFR FDP_ACF.1/TERMINAL will be fulfilled trivially, as the TOE does not support firmware downgrade

[15] Note: This part of the SFR FDP_ACF.1/TERMINAL will be fulfilled trivially, as the TOE does not support firmware downgrade

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.*

].

Referring to PP application note 8:

No more objects are subject to Access Control so no more granular rules for Access Control are needed. Unauthorized reset to factory defaults is not implemented.

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[16]*, [none]*
Objects: management functions,
Object attributes: none

].

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*
- *[no selection]Display the MAC-address(es) of the TOEs network interface(s)*
- *[no selection]*
- *[no further management functions]*

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

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

- *[Manage the available network configuration]*
- *[Set card terminal name for card terminal]*
- *[no selection]*
- *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*
- *[no selection]*
- *[no further management functions]*

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

- *Enable/disable the remote management interface* ~~***(if applicable)***~~
-
- *Perform the initial pairing processes with the connector*
- *[No further management functions]*

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

- *Reset the TOE settings to factory defaults (fallback)*

[No further rules]]

].

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 initialisation

Referring to PP application Note 9:

FDP_ACF.1/Management was used to define the access control for management functionality of the TOE. Only management functions from the PP are implemented, thus no enhancement of further management functions and necessary privileges was executed. It applies to all local, remote or SICCT interfaces, which are capable of management functionality.

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[17]
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[18] , *[none]*].

[17] A remote card terminal either sends or receives a PIN for remote-PIN verification.
[18] This is the slot the user plugged his smart card in

Application Note ST.3: Since the PIN entered is always dedicated to be sent either to a specific ICC or to the Connector (for remote-PIN verification) the slot identifier is sufficient for PIN SFP.

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 authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5/PIN

The TSF shall explicitly deny an information flow based on 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

Referring to application Note 10:

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.

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

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 the 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[19]

The TOE shall have only one connection to one connector at a time.

].

FDP_IFF.1.3/NET

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

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*

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

- *SICCT CT DOWNLOAD DATA*
- *SICCT CT DOWNLOAD FINISH*

The TOE shall additionally accept the following EHEALTH commands arriving at the network interface if no pairing process is established but a valid connector certificate[20] 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.

].

Application Note ST.4: If a connector certificate is not valid because of an error during the mathematical check of the signature (e.g. wrong private key used), the TOE disconnects the TLS connection for security reasons (possible attack assumed). In this case none of the listed SICCT commands can be send to the TOE.

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

Referring to 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 connections are not covered by this policy.

Further, according to [gemSpec_KT] the terminal is free to accept unencrypted communications for other applications, which may be additionally realized by the terminal (or during the migration phase).

[20] For the steps in verifying signatures of the certificate application component see [gemSpec_KT], Table 16

In these cases, the terminal indicates to the user that it is working in an insecure state.

Please note that as a limitation to [SICCT] 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.

Referring to Application Note 12:

The functionality, defined in FDP_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. The remaining part of this application note is not applicable: no batch Signatures implemented.

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 been [met, surpassed], the TSF shall [*lock the particular management interface for that account for a time period according to Table 10 depending on the number of consecutive unsuccessful authentication attempts*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

Table 10: Lockout Times

Referring to PP application note 13:

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

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, [*none*]].

Hierarchical to: No other components.

Dependencies: No dependencies

Referring to PP application Note 14:

No further user attributes are needed for any policy of the TOE.

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

Referring to PP application note 15:

The above requirements on passwords hold for all management interfaces.

6.1.3.4 FIA_UAU.1 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)*]*
- *[no selection]*
- *[Self-Test]*

]

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

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*
- *[A remote authentication mechanism via TLS]*

] to support user authentication.

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

- *The **password based authentication mechanism** is used for authentication of TOE administrators for management* ~~***and other users***~~
- *The **remote authentication mechanism via TLS** 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*

- *[no additional rules]*

]

Hierarchical to: No other components.

Dependencies: No dependencies

Referring to PP application note 16:

The authentication mechanism for the TOE Reset Administrator is based on a challenge-response mechanism as described in 1.4.2. As the challenge is a large random number, replay attacks are not possible.

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

Referring to PP application note 17: no further action required.

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)]*
- *[no selection]*
- *[Self-Test]*

] 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.

Referring to application Note 18:

No further TSF mediated actions are allowed without having the user successfully authenticated before.

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*] to [*authenticated TOE administrators (excluding SICCT interface)*].

Hierarchical to: No other components.

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

Application Note ST.5: According to Application Note 8 in [eHCT-PP], the functionality of an unauthorized reset to factory defaults is optional. The management function to enable/disable this functionality is only required if this functionality is implemented. The TOE does not implement the functionality of an unauthorized reset to factory defaults; therefore this SFR is trivially fulfilled.

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 [**change_default**, query, modify, delete, [*no other operations*]] 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 [*role(s)*[21]].

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

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

[21] Role(s) as defined in chapter 6.1.4.7

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

Referring to PP application note 19:

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*[22]
- *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*
- *View/set card terminal name*[23] *for card terminal*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*[24]
- *Reset the TOE settings to factory defaults (fallback)*[25]

[22] On first start-up the TOE forces the administrator to specify a password for local management.
[23] The card terminal name is a unique identifier for the card terminal. Note that the terminal name shall not be set using dhcp.
[24] 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.
[25] The fallback solution for reset of TOE settings is necessary in case the credentials for management are lost.

- *Display the product version number of the TOE*
- *Display the installed firmware group version*
- *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]*
- *[no selection]*
- *[no selection]*
- *[Display the MAC-address(es) of the TOEs network interface(s)]* [26]

[

- *Enable/Disable the usage of a PIN-Pad accessory incl. enable/disable of the USB-Host interface* [27]
- *Enable/Disable a VPN connection to a remote gateway with a connector*
- *PIN-entry for a SMC-B over the remote management interface]*.

Hierarchical to: No other components.

Dependencies: No dependencies.

Referring to PP application note 20:

Failure counters for management interfaces and the shared secret are not reset on firmware update. The TOE can be reset to factory defaults when the management credentials are lost using the mechanism described in 1.4.2. The additional security functionality necessary for this was modelled in this SFR.

Note that a firmware update can also be triggered remotely from a trusted PUSH Server in the internal network of the medical supplier according to the push update mechanism described in [gemSpec_KT]. The PUSH Server 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.

[26] The [PP] states that “Another option would be to attach the MAC-address(es) to the body of the card terminal.” This option is not chosen by the developer.

[27] Enabling of this functionality sets the TOE into a non-CC-certified mode.

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*[28]*, failure during firmware update, [*

- *failure during self-test*
- *an alarm condition indicates possible tampering*

]].

Hierarchical to: No other components.

Dependencies: No dependencies

Minimum requirements of PP application Note 21 are met: failure of self-tests and failure of firmware updates were included in the list of assignments.

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

Referring to PP Application Note 22: TOE is one physical part.

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

Referring to PP Application Note 23: FPT_PHP.3 added with active detection.

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

6.1.5.4 FPT_PHP.3 RESISTANCE TO PHYSICAL ATTACK

FPT_PHP.3.1 The TSF shall resist [*opening, drilling and probing*] to the [*SFR-enforcing areas protected by full volumetric protection covers*] by responding automatically such that the SFRs are always enforced.

Hierarchical to: No other components.

Dependencies: No dependencies

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, when activated by an authorised user*]] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [[*public key for firmware update validation, the TOE software*]].

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

Referring to application Note 24:

The ST author has described test functionality for all important aspects of all Security Functions that the TOE provides.

6.1.6 TOE ACCESS

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.

Referring to application Note 25 and 26:

The term “Before establishing a user session” refers to every situation a user is about to use the TOE. The TOE will indicate whether it's in a secure state or not. This SFR is used to meet O.STATE. The “secure state” refers to a mode of operation in which all TSFs of this ST are met and no additional value-added module functionality (as allowed by [17]) is active that could compromise a TSF. Specifically the TOE will guarantee a secure PIN entry within such 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 is regarded as implicitly fulfilled.

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.

Referring to 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 is ensured that the TLS connection will be dropped when the SM-KT is unplugged.

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, [*no other types of integrity or confidentiality violation*]].

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.

6.2 Security Assurance Requirements for the TOE

The following table lists the assurance components which are applicable to this Security Target:

Assurance Class	Assurance Components
ADV: Development	ADV_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 procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	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 11: 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 [CCpart3].

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			
FSP_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				
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

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FPT_FLS.1							x
FPT_ITT.1							x
FPT_PHP.1							x
FPT_PHP.3							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 F*DP_ACF.1/Terminal* define the rules under which a firmware update is possible. *FDP_ACC.1/Management* and F*DP_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. F*CS_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.3, 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.3 build the physical protection for the stored assets. FPT_PHP.3 will automatically respond on detecting opening the SFR-enforcing areas protected by full volumetric protection covers and drilling or probing attacks on all sides of these areas and guarantee that the SFRs are always enforced, *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 SFR 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 and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Fulfilled by the use of FCS_CKM.1/Connector and 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 and 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 and FCS_CKM.4
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 and 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 6.3.2.1 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 6.3.2.1 for FDP_ITC.1 and FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
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 6.3.2.1 for FMT_MSA.3
FDP_IFC.1/NET	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/NET
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 6.3.2.1 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 by FIA_UID.1
FIA_UAU.5	No dependencies	-
FIA_UAU.7	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UID.1	No dependencies	-
FMT_MSA.1/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

SFR	Dependencies	Support of the Dependencies
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	Fulfilled by FIA_UID.1
FPT_TST.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_ITT.1	No dependencies	-
FPT_PHP.1	No dependencies	-
FPT_PHP.3	No dependencies	-
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

6.3.2.1 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 initialisation 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 Security Target 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.

6.3.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The Evaluation Assurance Level for this Security Target is EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4.

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 according to [gemKPT_Arch_TIP] (see also OSP.PIN_ENTRY).

This leads to an Evaluation Assurance Level of 3 augmented by the following component:

- 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)

6.3.4 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 in this Security target 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 [CCpart2] are used to fulfil the security objectives.

7 TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1 TRUSTED COMMUNICATION CHANNELS

The TOE meets the requirements of **FTP_ITC.1/Connector** (keys to be used for TLS encryption/decryption) and **FTP_TRP.1/Management** as for all communication functions to the connector and remote users used by eHealth applications except service discovery the TOE will always establish a trusted communication channel to the connector or remote user. It will be logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The TOE will permit the connector and remote users to initiate communication via the trusted channel.

For the establishment of a secure communication channel to the connector or for remote management, the TOE will use the Diffie-Hellman key exchange algorithm with cryptographic key sizes of 128 or 256 bit, meeting the requirements of **FCS_CKM.1/Connector** and **FCS_CKM.1/Management**.

For secure communication to the connector or for remote management the TOE will use signature verification with RSA with 2048 bit keys or ECDSA (meeting the requirements of **FCS_COP.1/SIG**) and AES-CBC with 128 bit or 256 bit keys for encryption and decryption, meeting the requirements of **FCS_COP.1/Con_Sym** and **FCS_COP.1/Management**.

7.2 IDENTIFICATION & AUTHENTICATION

To perform the secured management functions, the administrator of the TOE first must identify and authenticate himself.

The TOE provides several authentication mechanisms for administrators and for other users:

- a password based local authentication mechanism for the TOE administrator
- a password based remote authentication mechanism via TLS using the Ephemeral Diffie–Hellman key exchange using 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 cipher suites with key sizes of 128 bit or 256 bit where the secure element is used for random number generation,
- a remote authentication mechanism for the SICCT-interface using the Ephemeral Diffie–Hellman key exchange using TLS_DHE_RSA_WITH_AES_128_CBC_SHA or TLS_DHE_RSA_WITH_AES_256_CBC_SHA or TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suites with key sizes of 128 bit or 256 bit. The key generation / negotiation includes a mutual authentication of the TOE and the connector based on certificate validation. Additionally, the remote authentication mechanism for the SICCT-interface includes a password based mechanism (SICCT password).

- an authentication mechanism for the TOE reset administrator using a challenge generated by the TOE and a response generated and transmitted by the customer support service:

    1. The TOE generates a challenge (at least 64 Bit random number) with a restricted life-time.

    2. The owner contacts and authenticates at the customer-support-service.

    3. The owner transmits the challenge along with the device serial number to the customer-support-service.

    4. The customer-support-service uses the challenge and device serial number to generate the 8-digit response and transmits it back to the owner.

    5. The owner enters the response.

    6. The device checks the response and authenticates the current user as TOE Reset Administrator.

The TOE reset administrator is only allowed to reset the TOE to its factory defaults, thus meeting the requirements of **FIA_UAU.5** and **FIA_ATD.1**.

The TOE will detect unsuccessful authentication attempts for each of the authentication mechanisms. On at least 3 consecutively unsuccessful authentication attempts the TOE will lock the authentication mechanism for a period of time depending on the number of consecutive unsuccessful authentication attempts, specified in Table 14: Lockout Intervals (TSF):

Unsuccessful authentication attempts	Lockout interval
3-6	1 minute
7-10	10 minutes
11-20	1 hour
> 20	24 hours

TABLE 14: LOCKOUT INTERVALS (TSF)

meeting the requirements of **FIA_AFL.1**.

The TOE ensures that passwords for management

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

thus meeting the requirements of **FIA_SOS.1**.

7.3 SECURE PIN-ENTRY

The TOE provides for a secure PIN entry that can only be activated by the TOE itself and it will be indicated to the user by a LED and a red card symbol that it is in secure PIN-Entry mode, thereby meeting the requirements of **FTA_TAB.1/SEC_STATE**.

PINs for a card in a slot of the TOE, for the connector or for a remote card terminal will never be stored in a non-volatile memory of the TOE when the PIN is entered. To mitigate indirect access to the pin (gathered by touch coordinates), the position of the PIN user interface is randomized. The PIN entered by the user will only be sent to the card in the card slot of the TOE or via a TLS secured connection to the connector to a remote card terminal for remote-PIN verification, thereby meeting the requirements of **FDP_IFC.1.1/PIN** and **FDP_IFF.1.1/PIN**.

During PIN entry, the TOE provides only asterisks for password characters to the user while the authentication is in progress, thereby meeting the requirements of **FIA_UAU.7**.

7.4 NETWORK CONNECTIONS

The TOE only allows one connection to one connector at a time and will accept any information arriving at the network interface from the connector only if the communication path is encrypted and the connector has been successfully authenticated. Commands to identify the TOE in the network (service discovery) will be accepted and processed even without an encrypted or authenticated connection.

The TOE enforces that *the control byte for the bits b2..b1 of the Command-To-Perform Data Object CMD DO does not contain other values than {b 2 = 1, b1 = 0} or {b 2 = 1, b1 = 1}.*

The TOE accepts 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

and additionally, accepts the following eHealth command arriving at the network interface if no pairing process is established but a valid connector certificate is presented:

- EHEALTH TERMINAL AUTHENTICATE.

Further the TOE restricts information flow based on the following rules:

- Passwords for management interfaces will never leave the TOE
- a shared secret never leaves the TOE in clear text (even over trusted channel)
- patient data will never be transferred via the management interfaces**.**

The TOE thereby meets the requirements of **FDP_IFC.1/NET** and **FDP_IFF.1/NET**.

7.5 SECURE UPDATE

The TOE enforces that a modification of the firmware of the TOE only is allowed after the integrity and authenticity of the firmware has been verified by checking the signature over the update file. Signature verification on the new update file containing the new firmware signed by the manufacturer uses the cryptographic ECDSA algorithm with the curve brainpoolP384r1 and a size of the cryptographic key of 384 bit.

Non-authentic transmissions will be recognized.

The transmission mechanism detects transmission errors independently.

An update of the firmware of the TOE only is allowed by an authenticated administrator where

- A firmware consists of two parts: the so-called “firmware list” and the “firmware core” (which includes the whole firmware except the firmware list). The firmware list states all firmware core versions to which a change is allowed. Firmware lists and cores are versioned independently.
- An update of the firmware core is only allowed if the core version is included in the firmware list. Firmware lists only contain version numbers of firmware cores which are certified according this Security Target.
- The TOE does not support firmware downgrade, therefore all requirements warning the administrator in case of downgrades are fulfilled trivially. .
- In case of a common update the TOE will install the new firmware list at first. The new list is then 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.
- No subject can modify the public key for the signature verification for firmware updates

Thus the TOE is meeting the requirements of **FDP_ACC.1/Terminal** and **FDP_ACF.1/Terminal.**

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, thus meeting the requirements of **FCS_COP.1/SIG_FW**.

Potential updates of the TSP CA list are part of a firmware update; see application note on FCS_COP.1/SIG_TSP. Thereby the TOE also meets the requirements of **FCS_COP.1/SIG_TSP**.

7.6 SECURE DATA DELETION

The TOE ensures that memory no longer used for storage of PINs, passwords, health data, cryptographic data and all information that is received by a card in a slot of the TOE or by the connector (except the shared secret) will be erased by overwriting with 0x00 before it is deallocated and then be made available for further use. Memory areas for PINs will be overwritten with 0x00 as soon as the PIN has been sent to the chip card, thus meeting the requirements of **FDP_RIP.1** and **FCS_CKM.4**.

When selected by an authenticated TOE administrator (excluding SICCT interface) pairing information from all three possible pairing processes (initial pairing, review of pairing- information and maintenance-pairing) and management credentials (including PINs) will securely deleted and written with 0x00 before it is deallocated. Thereby the TOE meets the requirements of **FDP_ACC.1/Management** and **FDP_ACF.1.2/Management**.

7.7 SECURE MANAGEMENT FUNCTIONS

The TOE is aware of three roles: administrators, the TOE Reset Administrator, and user (meeting **FMT_SMR.1**). To identify and authenticate these roles the TOE provides PIN based identification and authentication. The secure management functions are only available to the TOE administrator after successful identification and authentication. Details are as described:

Unless the TOE administrator's local management PIN has been set (thereby changing the PIN validity attribute from *not valid* to *valid*) no subject can access any object under TOE control. The TOE offers no functionality to read out the PIN or management credentials while they are temporarily stored in the TOE. Thereby the TOE meets the requirements of **FDP_ACC.1/Terminal** and **FDP_ACF.1/Terminal.**

The TOE allows the TOE administrator to perform the following management functions:

- Manage local and remote management login credentials
- 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
- View/set card terminal name for card terminal
- Perform a firmware update
- Reset the TOE settings to factory defaults
- Display the product version number of the TOE
- Display the installed firmware group version
- Return self-assessment through the user interface of the administration interface by verifying the integrity of the TSF data and the TSF
- Enable/disable remote management functionality
- Managing network configuration
- Enable/Disable remote update functionality for firmware update
- Display the MAC-address of the TOEs network interface
- Enable/Disable a VPN connection to a remote gateway with a connector
- PIN-entry for a SMC-B over the remote management interface
- Enable/Disable the usage of the PIN-Pad accessory

The following management functions are executable by all roles:

- Display the product version number of the TOE
- Manage login credentials

- View card terminal name for card terminal
- Display the MAC-address of the TOEs network interface

The following management functions are executable by authenticated TOE administrators (excluding SICCT interface):

- 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)
- Perform a firmware update
- Reset the TOE settings to factory defaults

The following management functions are executable by TOE administrators that were authenticated using the SICCT interface:

- Set card terminal name for card terminal
- Perform a firmware update

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

- Enable/disable the remote management interface
- Perform the initial pairing possible pairing processes with the connector

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

- Reset the TOE settings to factory defaults (fallback)

Before identification and authentication of the user the card terminal allows to

- Display the product version number of the TOE
- Display the MAC-address of the TOEs network interface

and requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

The TOE restricts the ability to change_default, query, modify, and delete security attributes to the TOE administrator in a way that only secure values are accepted for roles and restrictive default values for security attributes that are used to enforce the security functions.

To guarantee a reliable mutual identification and authentication of connector and TOE a pairing process as specified in [gemSpec_KT], chapter. 3.7.2] will be performed.

FMT_SMR.1 is satisfied as the TOE is aware of three roles: administrators, the TOE Reset Administrator, and user.

FDP_ACC.1/Terminal and **FDP_ACF.1/Terminal** are satisfied as the TOE enforces setting of the administrator PIN first and no functionality exists to read out PINs or management credentials and the TOE enforces that only an authorized user is able to change its own management credentials, to perform a firmware update or to delete the Shared Secret.

FMT_SMF.1 is satisfied as the TOE enforces that the TOE administrator is allowed to perform the defined management functions.

FDP_ACC.1/Management and FDP_ACF.1/Management are satisfied as the TOE enforces that

- some management functions are executable by all roles, and
- some are only executable by authenticated TOE administrators (excluding SICCT interface),
- some are only executable by TOE administrators that were authenticated using the SICCT interface and
- some are only executable by TOE administrators that were authenticated using the local management interface

and the TOE Reset Administrator is only able to execute the following management function:

- Reset the TOE settings to factory defaults (fallback).

FIA_UAU.1, FIA_UID.1 are satisfied as the TOE enforces that before identification and authentication of the user the card terminal allows to

- Display the product version number of the TOE
- Display the MAC-address of the TOEs network interface
- Self-Test

and requires each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

FMT_MSA.1/Management, **FMT_MSA.2**, **FMT_MSA.3/Terminal** and **FMT_MSA.3/Management** are satisfied by the TOE as it enforces that the TOE restricts the ability to change_default, query, modify, and delete security attributes to the TOE administrator in a way that only secure values are accepted for roles and restrictive default values for security attributes that are used to enforce the security functions and to guarantee a reliable mutual identification and authentication of connector and TOE a pairing process will be performed.

According to Application Note 8 in [eHCT-PP], the functionality of an unauthorized reset to factory defaults is optional. The management function to enable/disable this functionality is only required if this functionality is implemented. The TOE does not implement the functionality of an unauthorized reset to factory defaults; therefore **SFR FMT_MSA.1/Terminal** is trivially fulfilled.

7.8 SELF-TEST

The TOE performs self-tests during initial start-up and after activation by an authorised user to demonstrate the correct operation of the TSF. The self-tests include tests of the cryptographic primitives for the AES and the hash algorithms and the RSA and ECC verification algorithms by performing known answer tests. Authorised users of the TOE have the option to test the integrity of TSF data and the TSF by running a test that checks the integrity of the FLASH memory of the TOE. The TOE thereby meets the requirements of **FPT_TST.1**.

7.9 SECURE FAIL-STATE

The TOE ensures that it maintains a secure fail state when

- an alarm condition indicates possible tampering or if a
- self-test detects an error.

The TOE will then turn to an unrecoverable non-functional state and has to be sent in for service.

In case of a failure during firmware update the TOE will be put into a secure fail state by falling back to the last version of the firmware.

When the TOE detects a disconnection of connector all plugged smart cards will be reset.

Thus, the requirements of **FPT_FLS.1** are met.

7.10 PHYSICAL PROTECTION OF THE TOE

The TOE is constructed as one part and is protected against opening attacks to the casing of the TOE by using full volumetric protection covers.

For active protection against probing and drilling attacks, the TOE has an alarm function constantly checking a drill and probing protection foil for alarm conditions which are a short-cut or interruption of the circuit paths on the foil caused by drilling and probing attacks. On alarm (indicating possible tampering) the alarm function will display a message on the TOE display and will put the TOE in a secure non-functioning state. The alarm condition remains after a TOE restart. Thus the TOE meets the requirements of **FPT_PHP.3, FPT_PHP.1 and FPT_ITT.1**.

Seals placed over the jointing of the body parts add to the protection against opening attacks to the casing of the TOE. Seal positions, their look and how to identify broken security seals will be described in the guidance documents. The seals will be visibly destroyed on attempts to tamper with the TOE body, contributing to the requirements of FPT_PHP.1.

7.11 SFR IMPLEMENTATION OVERVIEW

SFR / Chapter	Trusted Communication Channels	Identification & Authentication	Secure PIN-entry	Network Connections	Secure Update	Secure Data Deletion	Secure Management Functions	Self-Test	Secure Fail-State	Physical Protection of the TOE
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					
FDP_ACC.1/Terminal					X		X			
FDP_ACC.1/Management						X	X			
FDP_ACF.1/Terminal					X		X[29]			
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				
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			
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			
FPT_TST.1								X		
FPT_FLS.1									X	
FPT_ITT.1										X
FPT_PHP.1										X
FPT_PHP.3										X
FTA_TAB.1/SEC_STATE			X							
FTP_ITC.1/Connector	X									
FTP_TRP.1/Management	X									

Table 15: Overview of SFR implementation

[29] Trivially fulfilled as unauthorized reset is not implemented, see application note to FMT_MSA.1/Terminal in chapter 6.1.4.1.

8 GLOSSAR

AES	Advanced Encryption Standard
BCS	Basic Command Set
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
eGK	elektronische Gesundheitskarte
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
EAL	Evaluation Assurance Level
HPC	Health Professional Card
ID	Identity
KVK	Krankenversichertenkarte
LAN	Local Area Network
LED	Light Emitting Diode
MAC-Address	Media Access Control-Address
PIN	Personal Identification Number
PIN-Pad	Accessory connected to an eHCT
PRNG	Pseudo Random Number Generator
RFID	Radio-Frequency Identification
SFP	Security Function Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable Chip Card Terminal
SMC	Security Module Card
SM-KT	Security Module Kartenterminal
ST	Security Target
TBD	to be defined
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	Trust-Service Provider that issues connector certificates

9 REFERENCES

Common Criteria

[CCpart2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 5, 2017.

[CCpart3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, 2017.

Specifications

[BSI_AIS20_AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS), BSI, AIS 20, Version 3.0, 15.05.2013
Anwendungshinweise und Interpretationen zum Schema (AIS), BSI, AIS 31, Version 3.0, 15.05.2013

[FIPS-186-4] Federal Information Processing Standards Publication 186-4, (FIPS-186-4), July 2013, Digital Signature Standard (DSS)

[FIPS 197] Federal Information Processing Standards Publication 197, (FIPS-197), November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES)

[gemKPT_Arch_TIP] Konzept Architektur der TI-Plattform, Version 2.10.0, Stand 02.03.2020

[gemSpec_gSMC-KT_ObjSys] gematik - Spezifikation der gSMC-KT Objektsystem, Version: 3.9.0, 24.08.2016

[gemSpec_gSMC-KT_ObjSys_G2.1] Spezifikation der gSMC-KT Objektsystem, Version: 4.3.0, 12.05.2022

[gemSpec_Krypt] gematik - Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.22.0, Stand 01.03.2022

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

[JAVACARD] "Javacard specification", Oracle v3.0.5

[RFC 5246] RFC 5246, The TLS Protocol, Version 1.2

[RFC 5289] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

[RFC 8017] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2

[RFC 8422] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier

[SICCT] SICCT - Secure Interoperable ChipCard Terminal, Version 1.2.3, 30.09.16 incl. ERRATA Version 1.0 from 05.05.2021

[TR-03111] Technical Guideline BSI TR-03111 Elliptic Curve Cryptography, Version 2.10, 01.06.2018

[TR-03120] BSI - Technische Richtlinie Sichere Kartenterminalidentität, Version 1.1, 09.07.2010

Protection Profiles

[COS-PP] Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), Version 2.1, 10.07.2019

[eHCT-PP] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V2-2015-MA01, Version 3.7, 21.09.2016.

[Konn-PP] Common Criteria Protection Profile Schutzprofil 2: Anforderungen an den Konnektor BSI-CC-PP-0098, Version 1.5.9, 15.04.2021

Certificates

[JCOP4_CC] Certification Report JCOP 4 P71, TÜV Rheinland Nederland B.V., 26 September 2022, NSCIB-CC-180212-CR5

Guidance documents

[AGD Quick] AGD documentation, Quick Guide for Users (64410078-05), Mar 2023, Cherry Digital Health GmbH

[AGD] AGD documentation, Administrator Manual (64410079-07), Feb 2023, Cherry Digital Health GmbH