Security Target
for the Evaluation of the Product
ORGA 6141 online
of
Ingenico Healthcare GmbH
according to the Common Criteria 3.1
Level EAL3+
Certification Id:
BSI-DSZ-CC-0519 - V3

Version: 4.1.11

Date: 26.01.2020

Table of Contents

1 ST Introduction

1.1 ST Reference

Certification Id:	**BSI-DSZ-CC-0519 - V3**
CC-Version:	**3.1**
Evaluation Assurance Level:	EAL 3, augmented by **ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1** and **AVA_VAN.4**
Title	Security Target for the Evaluation of the Product ORGA 6141 online of Ingenico Healthcare GmbH according to the Common Criteria 3.1 Level EAL3+
Document Version:	4.1.11
Date:	26.01.2020

1.2 TOE Reference

Target of Evaluation:	Card Terminal with graphical display (ORGA 6141 online)
Herstellcode:	HC 03000000010301 HC 03000000020301
Firmware-Version	3.8.0
Hardware-Version	1.2.0
Manufacturer / Vendor:	Ingenico Healthcare GmbH, Flintbek

1.3 TOE Overview

This Security Target defines the security objectives and requirements for the Electronic Health Card Terminal (eHCT) ORGA 6141 online based on the regulations for the German healthcare (GHC) system. Furthermore the TOE can be irreversibly configured to be used as a secure PIN entry device controlled by a Signature Application Component (SAC).

1.3.1 TOE Description

The TOE is a card terminal with 2 ID1 Slots (HPC and eGK) und 2 SMC Slots (SM-KT (supporting SMC-B and SMC-KT cards), 20 key keypad, USB and LAN interfaces for the use in the German healthcare system with KVK, HPC and eGK generation 1+ and generation 2. Connection to a connector/SAC is possible via LAN and TCP/IP-protocol.

The ORGA 6141 online is a card terminal with graphical display:

Figure 1.1 ORGA 6141 online

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 [7] for further information about card compatibility.

The TOE fulfils the requirements to be used as a secure PIN entry device for applications according to [6], [7] and [9] (i.e. SAC), which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.

This terminal is based on the specification for a "Secure Interoperable Chip-Card terminal" ([6]) extended and limited by the specifications for the e-health terminal itself (see [7]). In its core functionality the TOE is not different from any other smart card terminal which provides an interface to one or more smart cards including a mean to securely enter a PIN.

Additionally the TOE provides a network interface which allows routing the communication of a smart card to a remote IT product (i.e. SAC) 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.[1]
- Passive and active physical protection

1 A firmware downgrade is not implemented in the TOE. However, it is possible to install a previous version of a firmware if the firmware image has been assigned a new version number.

The TOE for use in the GHC system or with a SAC is based on the specification SICCT [6], which is adapted for operation by profiling as eHealth card terminal (see [7]).

The TOE works with a cryptographic key for i.e. 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 gSMC-KT cards. IPv4 is supported. *To ensure the sustainability of the TOE, it is technically able to support IPv6 in addition or instead of IPv4 by a future certified firmware update. For the recent TOE version IPv6 functionality is outside of the TOE scope.*

In its environment, the TOE communicates either with a so called connector or a SAC. The connector is the secure connection between the local network of the medical supplier and the remote network of the telematic infrastructure. It provides the medical supplier with secure access to the services of the telematic infrastructure. The SAC is the secured connected controlling instance for signature generation using signature creation devices (typically electronic signature smart cards) by the /Signature user.

For the connection of the TOE to a connector/SAC via the LAN interface, the protocol with the SICCT commands is mandatory.The interfaces of the TOE are provided in Figure 1.2: TOE Boundary, showing a schematic representation:

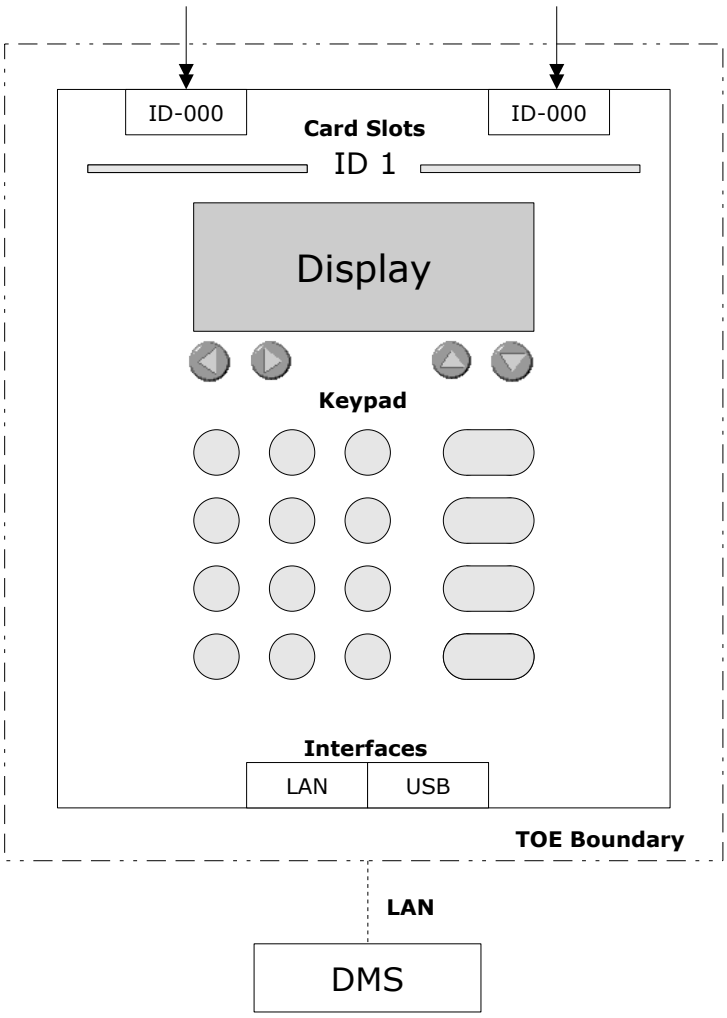

Figure 1.2: TOE Boundary

1.3.2 TOE major security features for operational use

To protect the communication between the connector/SAC 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 (see also [7]).

For its cryptographic functionality the TOE relies on the services of the so called SM-KT[2].

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 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 it does not belong to the logical and physical scope of the TOE as to see in Figure 1.2: TOE Boundary. More information about the SM-KT can be found in the Protection Profile Card Operating System 2 (PP COS G2) [20] and the gematik specification on the gSMC-KT object system [24].

According to the gematik release OPB3 specifications the TOE is capable to support RSA and alternatively ECC cryptography for TLS connectivity (see [21] ECC migration). The ability to support ECC encryption/decryption and ECDSA for signature creation and approval depends on the SM-KT provided functionality as defined by [7], [24] and [25].

For the case the TOE uses a DF.KT of a gSMC-KT as SM-KT, which is addressable via the connector/SAC, the TOE is accessing this DF.KT via the base-channel 0. During use of the SM-KT by the TOE the terminal card commands of the TOE have to be priorized and the processing of possibly existing client SICCT commands have to be interrupted and continued only after completion of the internal command sequence. The connector/SAC has to make sure that a DF.KT of a gSMC-KT as SM-KT which is addressable via the connector/SAC shall only be accessed by the TOE and not be used by any other system than the TOE.

The TOE provides functionality to update its firmware. This firmware update is done with the PULL method, i.e. the TOE actively "pulls" the firmware update from a TFTP server. The configuration is preserved and indicated after a firmware update (see [7] for further information).

Firmware update can also be triggered remotely from a trusted Push Server in the internal network of the medical supplier/Signature user. The TOE allows initiating batch signatures for the creation of more than one signature at a time without providing the PIN for each signature process. Batch signature is a functionality of the signing card.

In addition to the cryptographic identity of the TOE, the TOE stores a shared secret which is generated by the connector/SAC and transferred to the TOE during the pairing process of TOE and connector/SAC. 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/SAC is

2 Please note that the SM-KT is only responsible for the core functions of the asymmetric cryptography (RSA and ECC) and for random number generation. The TOE will be responsible for negotiating the session with the connector/SAC and for encryption/decryption using a symmetric AES key. More details can be found in [7] and the following chapters.

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/SAC by using shared secret between card terminal and SM-KT
- Review of pairing- information:
  The connector/SAC 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/SAC certificate on the card terminal by using a known shared secret. Please see [7]) for further information on the pairing process.

In addition to [7] and [PP] the TOE provides a restricted VPN Client for optional establishment of a single VPN tunnel to a remote VPN gateway in front of a remote connector/SAC. The usage of the VPN client is restricted and dedicated only to secure state condition and to be additionally used for the network connectivity. The VPN tunnel relies on IPsec over IPv4 and is completely transparent for the remote connector/SAC. Please note that the mentioned establishment of a single VPN tunnel is not part of the TSF.

The TOE is also able to send/receive a PIN to/from a remote card terminal. This communication is routed via the connector/SAC. The connector/SAC never sees the PIN in clear text, as the authorized cards (SMC-B, HPC) in the local and the remote card terminal are used to encrypt/decrypt the PIN. In this SAC operation still all SFRs are valid.

The TOE receives Trusted Service Provider certificate authority lists (TSP CA lists) by management functionality. Such a TSP CA list is configuration data with a white list which lets the TOE decide which TLS-certificate to accept or refuse when a connector/SAC is opening a secure communication channel. By default the TOE is pre-configured to accept certificates from the eHealth CA driven on behalf of gematik. To be used in the SAC context the TOE is capable to be once irreversibly configured for such operation by loading an alternative TSP CA list especially built by the TOE vendor holding CA certificates from selected known and trusted SAC vendors. After this alternative configuration the TOE is not able to accept TLS-certificates from the eHealth CA anymore."

1.3.3 TOE type and Physical Scope

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

- All hardware components, cage and interfaces,
- the update file with application firmware and
- the related guidance documents
  - user guide version 20.6.1 (Bedienungsanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0)
  - brief instruction version 20.2.1 (Kurzanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.0) for installation of the TOE.

Three seals are attached to the cage 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.

Note, that the SM-KT is a necessary requirement in the operational environment of the TOE. During the delivery and setup phase the SM-KT may have to

be installed into the card terminal. Functionality that is relying on the SM-KT for secure operation may not work as intended before the SM-KT is installed.

1.3.4 Required non-TOE hardware/software/firmware

The TOE is intended to be used as 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.

The following non-TOE hardware is required for the use of the TOE:

- An ID-000 smart card as a secure module representing the cryptographic identity of the TOE in form of an X.509 certificate. The secure module can be a DF.KT of a gSMC-KT as SM-KT. Although this secure module is usually physically placed within the cage of the TOE it does not belong to the logical and physical scope of the TOE.
- A connector as a secure connection between the local network of the medical supplier and the remote network of the telematic infrastructure. The connector further observes the TOE and is the only entity in the context of the GHC which can interact with a DF.KT of a gSMC-KT as SM-KT as mentioned above.

Furthermore, the TOE requires a TFTP server to update its firmware.

1.3.5 Optional non-TOE hardware/software

Following an option of the [PP] the TOE can be used as secure PIN entry device controlled by a SAC instead of a eHealth connector. In this optional case the following non-TOE hardware is required for the use of the TOE:

- A secure connected Signature Application Component (SAC) instead of a connector. The SAC observes the TOE and is the only entity in the context of signature creation processes outside the GHC which can interact with a DF.KT of a gSMC-KT as SM-KT as mentioned above.

The following non-TOE hardware is optional for the use of the TOE:

- An USB stick as an external temporarily storage medium for the administrator in order to import FW images and configuration data (i.e. VPN gateway credential data) as well to export configuration data for installation protocol and control purposes.
- A Smartphone App for the administrator to read out a Quick Response (QR) Code in order to display configuration and internal statistical data. An optional external WEB Site in order to receive, interpret and display configuration and internal statistical data.

1.3.6 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.

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, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 5, April 2017

as follows:

- Part 2 conformant,
- Part 3 conformant.

The

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

is 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-MA-01, Version 3.7, 21.09.2016*.

2.3 Package Claim

The current 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, Version 3.7, 21.09.2016*.

- Compared to the PP, there is a further threat (**T.F-SAC**) in the ST for the secure PIN entry device configuration.
  Signature Application Component (SAC) is introduced next to the connector subject.
- OSPs in the ST are identical to the OSPs in the PP. In addition to the "medical suplier", the “signature user” (subject) is introduced.

- Compared to PP, there is another assumption (**A.SAC**) in ST for the SAC configuration. In addition to the "medical suplier", the "signature user" (subject) is introduced.
- Compared to PP, there is another security objective (**OE.SAC**) in ST for the SAC environment which is introduced as Security Objectives **OE.SAC** for the environment

3 Security Problem Definition

3.1 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**/SAC**. 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. **The administrator PIN has the attribute "administrator PIN validity", which indicates whether the current PIN is valid. The PIN is only invalid directly after delivery, after successfully performing a Challenge & Response operation with the TOE and after or during a reset to factory defaults. Under these circumstances the attribute ensures that the TOE forces the administrator to set a valid management interface PIN in order to prevent an attacker from gaining easy access to management functionality. The modification of the validity of the management interface PIN is tied to the change of the management interface PIN. By setting the PIN, the administrator changes the validity of the PIN to valid.**
Shared secret	The TOE stores a shared secret which is generated by the connector**/SAC** 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**/SAC**. The TOE has to ensure the confidentiality and integrity of the shared secret. This asset is TSF data.
Patient Data	In the context of the GHC 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

Asset	Description
	its slot. The TOE has to ensure the confidentiality and authenticity of this data. This asset is user data.
SAC Data	**In the context of the SAC usage this data comprises user data that is related to the signature creation process. The TOE gets SAC data from the cards in its slots, encrypts this data and sends it to the SAC. Further the TOE accepts SAC data from the SAC decrypts it, and sends it to the corresponding smart card 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**/SAC**. This data comprises at least patient/user data and PINs for remote-PIN verification. The TOE has to ensure the confidentiality and authenticity of this data. 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 management and remote management and the list of TSP CAs. The TOE has to ensure the integrity, confidentiality, and authenticity of the management credentials. It has to ensure integrity and authenticity of the list of TSP CAs This asset is user data.
TSF Data	The TOE stores TSF data which is necessary for its own operation. The TOE has to ensure the confidentiality and authenticity of this data. This asset is TSF data.
Statistics Data	**The TOE is capable to store statistical data on its own operation which is only available to the administrator PIN and helpful in case of operational troubleshooting. The statistical data consists of data alike i.e. uptime, cumulated number of card-in events, which is user data that does not contain personnel or secure data content. The TOE has to ensure the integrity and confidentiality of this data.** **This asset is user data.**
Challenge	**The TOE generates challenge data to perform the challenge/response operation to reset the administrator PIN.**
Response	**The TOE processes response data to perform the challenge/response operation to reset the administrator PIN.**

Table 1: Assets

3.2 Subjects

The following subjects are interacting with the TOE:

Subject	Description
TOE Administrator	The TOE administrator is in charge of managing the security functions of the TOE.

Subject	Description
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify application sensitive information. The attacker has a moderate level attack potential.
Authorized card	Authorized cards (HPC, SMC-B) are able to perform card-to-card authentication which is used for remote-PIN verification.
Card	The TOE is handling the communication for one or more smart cards in its card slots.
Connector	In the context of the GHC the connector is the only entity in the environment of the TOE (except for users of the management interface) which is foreseen to communicate with the TOE. It is the interface for the TOE to securely communicate with the telematic infra-structure of the German healthcare system.
SAC	**In the context of the SAC usage the SAC is the only entity in the environment of the TOE (ex-cept for users of the management interface) which is foreseen to communicate with the TOE.**
Medical supplier	In the context of the GHC 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 re-sponsible for the secure operation of the TOE.
Patient	In the context of the GHC the patient uses the TOE together with his eHC. The patient uses the TOE for other services of the eHC. A patient will never use the services of the TOE alone but will always be guided by the medical supplier.
Signature user	**In the context of the SAC usage the Signature user uses the TOE together with his signature creation device (signature smart card). The Sig-nature user does not use the services of the TOE alone but services of the SAC which controls the eHCT operation.**
Push Server	The Push Server is a trusted entity in the internal net-work of the medical supplier**/Signature user** which updates firmware on card terminals that are connected to that network. The Push Server uses the SICCT in-terface or another network interface of the card ter-minal for remote update. See A.PUSH_SERVER for as-sumptions 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 certific-ate and provides : • Protection of the private key • Cryptographic functions for encryption/decryp-tion and signature creation • A random number generator • A function to read out the public key

Subject	Description
TOE Reset Administrator	The TOE Reset Administrator is the only user role that is able to perform a reset of the TOE settings when management credentials are lost. The type of authentication for this role depends on the particular implementation. The TOE Reset Administrator could be the developer himself.
User	A user is communicating with the TOE in order to use its primary services, i.e. to access a smart card which has been put into one of the slots of the TOE before. The TOE is used by different kinds of users including medical suppliers, patients, **Signature users** and administrators.

Table 2: Subjects

3.3 Threats

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

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

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

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

Summarizing this means that an attacker with a moderate attack potential has to be assumed.

The assets that are threatened and the 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**/SAC** in order to gain knowledge about communication data which is transmitted between the TOE and the connector**/SAC** or in order to manipulate this communication. As part of this threat an authorized user, who is communicating with the TOE (via a connector**/SAC**) 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**/SAC** • Communication data that is received from a card and stored within the terminal before it is submitted to the connector**/SAC**.

Threat	Description
	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	In the GHC context 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

T.F-SAC Threat **T.F-SAC** (outside the scope of [PP])

In the context of the SAC usage unauthorized personnel may try to initiate a pairing process with a fake SAC after an unauthorized reset to factory defaults, e.g. to initiate an unauthorized signature creation or to receive confidential (Signature user) data.

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 entry device for applications according to [22]. 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**/Signature user** 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 percept-

Assumption	Description
	ible, • 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**/Signature user** checks the sealing and the physical integrity of the TOE regularly before it is used, • That the network of the medical supplier**/Signature user** is appropriately secured so that authorized entities are trustworthy, see also [23].
A.ADMIN	The administrator of the TOE and the medical supplier**/Signature user** shall be non- hostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier**/Signature user** 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**/Signature user** 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**/Signature user** 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 Profiles. 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 have to be interrupted and continued only after completion of the internal command sequence. The developer may queue the interrupts internally or imple-

Assumption	Description
	ment 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 (according to TR-03120 [TR-03120] and its appendix [TR-03120-A]). The secure module has undergone an evaluation and certification process in compliance with the corresponding gematik card Protection Profile [20] and complies with the specification [24].
A.PUSH_SERVER	It is assumed that the internal network of the medical supplier**/Signature user** is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [7]. 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 smart cards 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

A.SAC Assumptions SAC (outside the scope of [PP])

The SAC 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. 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 SAC, 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 have 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 SAC makes sure that a DF.KT of a gSMC-KT as SM-KT which is addressable via the SAC can only be accessed by the TOE and cannot be used by any other system than the TOE.
In this SAC context the SAC acts logically like a connector in the way that it provides and performs the same secure network connectivity functionality including authentication, pairing and enforcement of encryption of communication. Because the SAC does not provide a SM-K security module it uses its own secure X.509 certificate and key store for authentication instead.

Further, it is assumed that the SAC periodically monitors the pairing state with the TOE and provides warning mechanisms to indicate unexpected results like paired terminals which lack the shared secret.

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 local card slots. For remote-PIN verification the PIN shall be encrypted, so that it can only be decrypted by the receiving smart card (HPC or SMC-B).

Objective	Description
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 two distinct roles: administrators and users[3].
O.MANAGEMENT	In order to protect its configuration the TOE shall provide only an authenticated and authorized administrator with the necessary management functions. The TOE shall enforce an access control policy for management functions, as some functions shall only be accessible by administrators authenticated by the local management interface. Further, the following management functions can be used by unauthenticated users • Display the product version number of the TOE • View card terminal name for card terminal The TOE shall provide a local management interface, and management over SICCT interface. A firmware consists of two parts: (1) the so-called "firmware list" and (2) the "firmware core" which includes the whole firmware except the firmware list. Firmware lists and cores have to versioned independently. The firmware list states all firmware core versions to which a change is allowed: An update of the firmware core is only allowed if the core version is included in the firmware list. A firmware update of the TOE shall only be possible after the integrity and authenticity of the firmware has been verified and the following holds: • The TOE provides functionality to update and downgrade its firmware. This includes both the change to a newer firmware as a downgrade to a firmware which is approved with the concept of firmware-group. • The configuration, such as terminal type, IP address or pairing- information shall be preserved and indicated after a firmware update or a downgrade (see [7] for further information). • The developer of the TOE shall ensure that in case of a downgrade of the firmware the TOE must warn the Administrator (e.g. within the Guidance) before the installation that the action to be performed is not an upgrade. The TOE must offer a chance to cancel the installation. The developer- specific update component shall warn the administrator about taking the responsibility in case of performing a downgrade. The administrator shall be able to manage the list of TSP CAs which is used to verify the authenticity of connectors**/SAC**. 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,

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
	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 update component the TOE supports update features of the SICCT specification, whereby a trigger component is able to update the TOE (e.g. the Configuration and Software Repository- Service (KSR) of the telematic infrastructure).
O.SECURE_CHANNEL	When establishing a connection between the TOE and the connector**/SAC** both parties shall be aware of the identity of their communication partner. Thus the TOE has to provide a mean to authenticate the connector**/SAC** and to authenticate itself against the connector**/SAC** in accordance with [7]. The TOE shall only have one connection to one connector**/SAC** at a time. For all communications which fall into either the context of the electronic health card or **SAC** 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	The TOE shall be able to indicate whether it is currently in a secure state, i.e. whether all TSP as required by this Security Target are actually enforced.
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[4]. 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**/Signature user**. 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**/SAC** 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**/SAC** (except the shared secret) in a secure way when it is no longer used. In case a TOE comprises physically separated parts,

4 Please note that the SM-KT provides its own physical protection for the stored keys. However according to [7] it has to be ensured that the SM-KT is securely connected with the TOE. Thus the physical protection provided by the TOE has to cover the SM-KT.

Objective	Description
	the TOE shall prevent the disclosure and modification of data when it is transmitted between physically separated parts of the TOE.

Table 6: Security Objectives for the TOE

4.2 Security Objectives for the 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**/Signature user** checks the sealing and the physical integrity of the TOE regularly before it is used, • The medical supplier**/Signature user** sends the TOE back to the developer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel, and • That the network of the medical supplier**/Signature user** is appropriately secured so authorized entities are trustworthy, see also [23].
OE.ADMIN	The administrator of the TOE and the medical supplier**/Signature user** shall be non- hostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier/**Signature user** 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**/Signature user** 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 med-

Objective	Description
	ical supplier**/Signature user** 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), and • that the administrator checks the secure state of the TOE regularly[5].
OE.CONNECTOR	The connector in the environment has to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication. The connector has to undergo an evaluation and certification process in compliance with the corresponding Protection Profiles. Further the connector has to periodically check the pairing state with the TOE and warn the administrator accordingly.
OE.SM	The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate. It is assumed that the cryptographic keys in this module are of sufficient quality and the process of key generation and certificate generation is appropriately secured to ensure the confidentiality, authenticity and integrity of the private key and the authenticity and integrity of the public key/certificate. The random number generator of the SM-KT shall provide entropy of at least 100 bit for key generation. It is further assumed that the secure module is secured in a way that protects the communication between the TOE and the module from eavesdropping and manipulation and that the SM-KT is securely connected with the TOE (according to TR-03120 [TR-03120] and its appendix [TR-03120-A]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [20] and complies with the specification [24].
OE.PUSH_SERVER	The internal network of the medical supplier**/Signature user** is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [7]. 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.

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

Objective	Description
OE.ID000_CARDS	All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE[6]. 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

Security Objectives OE.SAC for the environment (outside the scope of [PP])

The SAC 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. Further the SAC has to periodically check the pairing state with the TOE and warn the administrator accordingly.

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.SAC**	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				
T.F-SAC								X	X		X			
OSP.PIN_ENTRY		X				X	X							
A.ENV								X						
A.ADMIN									X					
A.CONNECTOR										X				
A.SAC											X			
A.SM												X		
A.PUSH_SERVER													X	
A.ID000_CARDS														X

Table 8: Security Objective Rationale

6 Please see TIP1-A_3192 in [7].

Note: **T.F-SAC, A.SAC** and **OE.SAC** are outside the scope of [PP].

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/SAC 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/SAC. This objective basically ensures that an attacker is not able to intercept the communication between the TOE and the connector/SAC 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/SAC. This authentication is part of the establishment of the secure communication between the TOE and the connector/SAC and contributes to removing the threat. O.PROTECTION ensures that each communication of the TOE with a connector/SAC 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/Signature user 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/Signature user 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/Signature user 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/Signature user 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/Signature user 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/Signature user checks the sealing and the physical integrity of the TOE regularly before it is used and that the user only enters the card PIN when the TOE indicates a secure state.

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

Note: Threat **T.F-SAC** and **OE.SAC** are outside [PP].

The threat **T.F-SAC** which describes that unauthorized personnel may try to initiate a pairing process with a fake **SAC** after an unauthorized reset to factory defaults, is countered by a combination of OE.ENV, OE.ADMIN and **OE.SAC**. OE.ENV ensures that the Signature user 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.SAC** ensures that the **SAC** in the environment is trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication. **OE.SAC** further ensures that the **SAC** periodically checks the pairing state with the TOE and warns the administrator accordingly.

4.3.2 Covering the OSPs

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

The secure PIN entry device is specified in O.PIN_ENTRY. This objective defines that the TOE has to provide a function for secure PIN entry and (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/Signature user, 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.

Note: Assumption **A.SAC** and Security Objective **OE.SAC** are outside [PP].

The assumption **A.SAC** is covered by **OE.SAC** 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 [2] are written in italics for assignments, underlined for selections and bold text for refinements. Furthermore the [brackets] from [2] are kept in the text.

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/SAC 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/SAC 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/PIN	Authentication failure handling
FIA_AFL.1 / C&R	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/SAC 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/SAC communication

FCS_CKM.1.1/Connector

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Diffie–Hellman ephemeral (DHE_RSA) key exchange using DH-group 14, ECDHE*] and specified cryptographic key sizes [*AES (128 bits) and AES (256 bits), HMAC (512 bits)*] that meet the following: [[7] **under consideration of [15] Appendix F.1.1.3 compliance**.]

Hierarchical to: No other components.

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

Application Note 1: The cryptographic session keys, generated by FCS_CKM.1/Connector are used for the TLS encryption/ decryption between the TOE and the connector/SAC (for further information see [7] 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/SAC based on certificate validation (see [7]) and validation of a shared secret. The TOE determines the role from the connector/SAC certificate presented during the build-up of the TLS connection. The TOE checks that the determined role corresponds with the role "Signature Application Component (SAC)" (see [7]).

The TOE uses the SM-KT for Signature generation and Signature Verification (see also A.SM) or/and its own functionality required by FCS_COP.1/SIG. For random number generation the TOE does not rely on the SM-KT. Instead it uses the Linux blocking random number generator which is continuously seeded during operation of the TOE by a certified TPM [ST33TPHF20].

The connection to network based management interfaces is always secured with TLS Version 1.2 [15][7].

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 [*Diffie–Hellman ephemeral (DHE_RSA) key exchange using DH-group 14*] and specified cryptographic key sizes [*AES_128 and AES_256*] that meet the following: [7].

Hierarchical to: No other components.

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

7 Contrary to the TLS 1.1 requirement indicated in the [PP], the support of TLS 1.1 is dropped in consideration of the Gematik eHealth KT Specification [7] - (TIP1-A_3415 - Securing network communication).

Application Note 2:

According to [PP, Application Note 20] the Remote Management functionality is optional. Therefore this SFR is also optional and not relevant for the TOE.

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: [*none*].

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 operation for connector/ SAC communication (symmetric algorithm)

FCS_COP.1.1/Con_Sym

The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-CBC, AES-GCM*] and cryptographic key sizes [*128 bit and 256 bit*] that meet the following: [[7] **and RFC3268, RFC5289, FIPS-197**].

Hierarchical to: No other components.

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

Application Note 3:

The symmetric cryptographic algorithm in FCS_COP.1/ Con_Sym is used to set up the trusted channel with a connector/SAC. 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, ECDSA*] and cryptographic key sizes [RSA*2048, SHA256, SHA384*] that meet the following: [*[7]* ***and [17]***].

Hierarchical to: No other components.

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

Application Note 4: The signature generation/verification in FCS_COP.1/SIG to establish the trusted channel with the connector/SAC is done using the SM-KT, see chapter *6.1.1.1*. Further the TOE verifies that the connector/SAC 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*] and cryptographic key sizes [*128bit and 256bit*] that meet the following: [7 and RFC3268, FIPS-197].

Hierarchical to: No other components.

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

Application Note 5:

The cryptographic functionality in FCS_COP.1/Management and FCS_CKM.1/Management is used to establish the trusted path for remote management. The cryptographic functionality complies with the requirements of the PKCS#1 standard. This SFR can implicitly be fulfilled by the mechanisms for cryptographically secured communication with the connector/SAC, see FCS_COP.1/Con_Sym.

According to [PP, Application Note 20] the Remote Management functionality is optional. Therefore this SFR is also optional and not relevant for the TOE.

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 [RSASSA-PKCS1-V1_5, SHA256] and cryptographic key sizes [RSA4096] that meet the following: [7].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Application Note 6: The functionality for signature verification is used to check the integrity and authenticity of a potential firmware up-

date. The functionality relies on hashing and a public key operation. The public key is part of the installed firmware.

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 [*RSASSA-PKCS1-v1_5*] and cryptographic key sizes [RSA*4096, SHA256*] that meet the following: [*[7] and [17]*].

Hierarchical to: No other components.

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

Application Note 7:

Potential updates of the TSP CA list are performed only as part of a firmware update with signature verification according to *6.1.1.7*. As the vendor chooses to provide TSP_CA list updates via the firmware update mechanism, this SFR will be fulfilled accordingly.

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 lists, shared secret, management credentials, firmware, cryptographic keys, Communication data [*none*] *Operations: Read, modify,* [*none*]].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.2 FDP_ACC.1/Management Subset access control for management

FDP_ACC.1.1/Management

The TSF shall enforce the [*Management SFP*] on [
Subjects: users, [none]
Objects: manageable objects, i.e. management functions
Operations: execute].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1.1/Terminal

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

Subjects: all subjects, attribute: user role[8]

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

[administrator PIN validity attribute]

].

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.*
  - *In case of downgrades of the firmware the TOE must warn the administrator before the installation that he is doing a downgrade, not an upgrade. The TOE must offer him the chance to cancel the installation.*
  - *In case of a common update the TOE has to install the new firmware list at first. The new list is used to decide whether an update to the accompanying firmware core is allowed.*

8 The role of the user (e.g. medical supplier/Signature user, TOE administrator)

- *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 ensures that in case of a downgrade of the firmware the TOE must warn the Administrator (e.g. within the Guidance) before the installation that the action to be performed is not an upgrade. The TOE must offer a chance to cancel the installation. A downgrade of the TOE shall only be possible after warning the administrator about the risks of this action. This warning shall be performed by the developer- specific update component.

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

- *[none]*

[none]

].

FDP_ACF.1.3/Terminal

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*Authorise the administrator to set the security attribute "validity of the management interface PIN" to "not valid" after successfully performing a Challenge & Response operation with the TOE.*]

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**, i.e. the administrator PIN is set to "valid"**.*
- *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 .*

].

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 by the developer.

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[9]*, [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*[10]
- *[View the available network configuration]*
- *[Display the MAC-address(es) of the TOEs network interface(s)]*

[
- *generate challenge data for a C&R operation*
- *enter response data for a C&R operation]*

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]*
- *[Enable/Disable remote update functionality for firmware update]*
- *Manage local and remote management login credentials*
- *Secure deletion of pairing information from all three possible pairing processes (initial pairing, review of pairing- information and maintenance-pairing)*
- *Manage the list of TSP CA*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*

[none]

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

9 The subject attribute management interface specifies the interface from which the user is connecting (local, remote, SICCT).
10 The TOE offers no unauthorized reset to factory default

- *[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/SAC*

[none]

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

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

[none]

].

FDP_ACF.1.3/Management

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

FDP_ACF.1.4/Management

The TSF shall explicitly deny access of subjects to objects based on the following additional rules [***none***]

Hierarchical to: No other components.

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

Application Note 9: FDP_ACF.1.2/Management has been amended.

According to [PP, Application Note 20] the Remote Management functionality is optional. Therefore the remote management parts of this SFR are also optional and not relevant for the TOE.

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, SAC, remote card terminal[11]
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[12] , *[none]*].

FDP_IFF.1.2/PIN

The TSF shall permit an information flow between a con-

11 A remote card terminal either sends or receives a PIN for remote-PIN verification.
12 This is the slot the user plugged his smart card in

trolled 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/SAC 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

Application Note 10:

For local PIN entry feedback the display of the TOE is used. For remote-PIN verification the TOE may send the PIN to another card terminal via the connector/SAC. 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/SAC. Therefore, it is responsible to select the participating card terminals and to initiate card-to-card authentication between both. Communication between TOE and connector/SAC 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, SAC, 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, SAC

Information: Passwords, patient data, SAC 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/SAC must only be accepted if the communication path is encrypted and the connector/SAC has been successfully authenticated[13]

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

].

FDP_IFF.1.3/NET

The TSF shall enforce **that** [
for PIN verification (SICCT PERFORM VERIFICATION) and PIN modification (SICCT MODIFY VERIFICATION DATA) only the Format-2 PIN-Block format is permitted].

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/SAC certificate is presented:

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

The TOE shall additionally accept the following EHEALTH commands arriving at the network interface if no pairing process is established but a valid connector/SAC certificate[14] *is presented:*

- *EHEALTH TERMINAL AUTHENTICATE*

13 See the trusted channel in section 6.1.7.1 and the verification section 6.1.1.5.
14 For the steps in verifying signatures of the certificate application component see [7], Table 2.

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

].

FDP_IFF.1.5/NET

The TSF shall explicitly deny an information flow based on the following rules: [

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

].

Hierarchical to: No other components.

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

Application Note 11:

Please note that the information flow policy defined in FDP_IFC.1/NET and FDP_IFF.1/NET is focused on the communications, which fall into the scope of the application for the electronic health card and which happen between the connector/SAC and the TOE.

Connections for administration of the TOE may not be initiated by a connector/SAC. Therefore such connections are not covered by this policy.

Further, according to [7] the terminal is free to accept unencrypted communications for other applications, which may be additionally realized by the terminal (or during the migration phase). In these cases the terminal indicates to the user that it is working in an insecure state.

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}.

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/SAC (except the shared secret),* [*none*]].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 12 is not applicable: no batch Signatures implemented.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1/PIN Authentication failure handling

FIA_AFL.1.1/PIN

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

FIA_AFL.1.2/PIN

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

Application note 13:

Both, the PIN-based authentication mechanism (see FIA_AFL.1/PIN above) and the authentication mechanism for the C&R interface (see FIA_AFL.1/C&R below) have their own counter for unsuccessful authentication attempts.

6.1.3.2 FIA_AFL.1/C&R Authentication failure handling

FIA_AFL.1.1/C&R

The TSF shall detect when [*5*] unsuccessful authentication attempts occur related to [*performing the Challenge&Response operation with the TOE with the same Challenge*].

FIA_AFL.1.2/C&R

When the defined number of unsuccessful authentication attempts has been [met, *surpassed*], the TSF shall [*block any response data entry unless a new challenge has been generated by the TOE*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

6.1.3.3 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [
TOE Administrator[15]*, [administrator PIN], TOE Reset Administrator, [Challenge]*].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 14: list of assignments is not empty.

6.1.3.4 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet **the following**:

[

Passwords for management shall

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

].

Hierarchical to: No other components.

Dependencies: No dependencies

Application note 15: All PINs / Passwords fulfill FIA_SOS.1.

6.1.3.5 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)]*
- *[*
  - *generation of challenge data for a C&R operation*
  - *response data input for a C&R operation*[16]
  - *shutdown the TOE*
  - *display product status, feature and health information]*

] 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.

15 The role of the user (e.g. medical supplier/Signature user, TOE administrator).
16 No unauthorised Reset to factory defaults ist implmented by the TOE.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

6.1.3.6 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1

The TSF shall provide [

- *A password based authentication mechanism,*
- *A remote authentication mechanism using the SICCT interface*
- *An authentication mechanism for the TOE Reset Administrator*
- *[an interface for authentication of the TOE reset administrator by performing a Challenge & Response operation with the TOE.]*

] to support user authentication.

FIA_UAU.5.2

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

- *The local authentication mechanism is used for authentication of TOE administrators for management and other users*
- *The remote authentication mechanism is used for authentication of TOE administrators for management (if applicable)*
- *The remote authentication for the SICCT interface is used for authentication of TOE administrators for management*
- *The authentication mechanism for the TOE Reset Administrator is used to authenticate the TOE Reset Administrator who alone is able to reset the TOE settings to factory defaults (fallback) when the management credentials are lost*
- *[The TOE provides for an interface to perform a Challenge & Response operation with the TOE reset administrator for authentication and accepts input of a matching response value to TOE generated challenge value for the authentication of the administrator.]*

]

Hierarchical to: No other components.

Dependencies: No dependencies

Application note 16:

For each C&R operation a TOE produces a distinct and unique challenge. The response token that has to be presented to the TOE is valid only for five unsuccessful attempts. After five unsuccessful attempts and after a successful attempt this response token is not longer valid and a new challenge has to be generated, requiring a new response.

6.1.3.7 FIA_UAU.7 Protected authentication feedback

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

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

Application note 17: no further action required.

6.1.3.8 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)]*
- *[*
  - *generation of challenge data for a C&R operation*
  - *response data input for a C&R operation*[17]
  - *shutdown the TOE*
  - *display product status, feature and health information]*

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

FIA_UID.1.2

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

Hierarchical to: No other components

Dependencies: No dependencies.

Application note 18:

With a C&R operation in operation (thus response entry pending) only the operations stated in FIA_UID.1/Management are possible prior to identification of the user.

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.

17 No unauthorised Reset to factory defaults ist implmented by the TOE.

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:

According to Application Note 8 in [19], an unauthorized reset mechanism is optional, and the management function to enable/disable the mechanism is only required if it is implemented (which is not the case for the current TOE). 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 [*query, modify, delete, [set and reset]*] the security attributes [*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)*].

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 to override the default values when an object or information is created.

Hierarchical to: No other components.

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

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

FMT_MSA.3.1/Management

The TSF shall enforce the [*Management SFP*] to provide

[*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Management

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

Hierarchical to: No other components.

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

Application note 19:

Remote update functionality for firmware update 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*[18]
- *Perform the pairing process (initial pairing, review of pairing- information and maintenance-pairing) with the connector/SAC*
- *Secure deletion of pairing information from all three possible pairing processes*
- *Manage the list of TSP CAs*[19]
- *View/set card terminal name*[20] *for card terminal*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*[21]
- *Reset the TOE settings to factory defaults (fallback)*[22]
- *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]*

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

19 Management of TSP-CAs includes the update of TSP-CA lists as described in [7] as well as a selection of a particular TSP-CA list to be used in case of multiple TSP-CA lists residing in the firmware (e.g. a separate TSP- CA list for test purposes).

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

21 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.

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

- *[Display the MAC-address(es) of the TOEs network interface(s)]* [23]

[

- *generate challenge data for a C&R operation*
- *enter response data for a C&R operation].*

Hierarchical to: No other components.

Dependencies: No dependencies.

Application note 20:

No Failure counter for any management interface is reset on firmware update.

According to [PP, Application Note 20] the Remote Management functionality is optional. Therefore the remote management parts of this SFR are also optional and not relevant for the TOE.

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/SAC*[24]*, failure during firmware update*[25]*, [*

- *failure during self-test*[26]
- *an alarm condition indicates possible tampering*[27]
- *disconnection of gSCM-KT*

]].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 21 are met, see Footnotes 24 - 27.

23 Another option would be to attach the MAC-address(es) to the body of the card terminal.
24 When the TLS connection to the connector/SAC is lost, the secure state is preserved by resetting all plugged smart cards
25 Failure during self-test results in an error message and a TOE rendered unusable.
26 Failure during update causes the use of the old version of the firmware.
27 When an alarm condition is detected an existing TLS-connection to the connector/SAC is terminated and all plugged smart cards are reset. Commands to the card reader result in an error code response.

6.1.5.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 22: 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

Application Note 23: FPT_PHP.3 added with active detection.

6.1.5.4 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1

The TSF shall resist [opening the TOE housing and drilling and probing] to the [*the bottom side, left and right side and rear side of the TOE*] 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* [*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 [[*TSP CA certificates*]].

FPT_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of [[*TSF-relevant applications*]].

Hierarchical to: No other components.

Dependencies: No dependencies

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.

Application Notes 25 and 26:

The term "Before establishing a user session" refers to every situation a user is about to use the TOE. The TOE indicates whether it's in a secure state or not by showing on the display that the user is in a secure state.

This SFR is used to meet O.STATE. The "secure state" refers to a mode of operation in which all TSPs of this ST are met and no additional value-added module functionality (as allowed by [7]) is active that could compromise a TSP. Specifically the TOE guarantees a secure PIN entry within such a secure state.

According to [7] a TOE could in principle accept unencrypted communications by a third party for applications that are outside the scope of the German Healthcare System. However as long as an unencrypted connection is established the TOE cannot be considered being in a secure state.

This SFR is implicitly fulfilled in case the TOE doesn't provide any additional functionality than the functionality, required by this ST and can't operate in an insecure state.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_ITC.1/Connector Inter-TSF trusted channel for connector/ SAC 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*[28]] 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, all communication functions used by the SAC*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 27:

28 Regarding trusted path/channel the SAC behaves the same as the connector.

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/SAC 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*, [*none*]].

FTP_TRP.1.2/Management

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

FTP_TRP.1.3/Management

The TSF shall require the use of the trusted path for [*authentication of TOE administrators*, *remote management*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note: According to [PP, Application Note 20] the Remote Management functionality is optional. Therefore this SFR is also optional and not relevant for the TOE.

6.2 Security Assurance Requirements for the TOE

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

Assurance Calss	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

Assurance Calss	Assurance Components
	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 [3].

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

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

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FCS_CKM.1/Connector[29]					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					

29 Regarding trusted path/channel the SAC behaves the same as the connector.

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FDP_IFF.1/PIN		x					
FDP_IFC.1/NET					x		
FDP_IFF.1/NET					x		
FDP_RIP.1							x
FIA_AFL.1/PIN			x				
FIA_AFL.1/C&R			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
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[30]					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

30 Regarding trusted path/channel the SAC behaves the same as the connector.

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/PIN*, FIA_AFL.1/C&R, *FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1* and *FMT_SMR.1*. *FIA_AFL.1/PIN* 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. 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 management. FIA_AFL.1/C&R defines the authentication failure for the Challenge & Response operation.

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/SAC. 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/SAC.

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 TOE housing and drilling or probing attacks on the bottom side, left, right and rear side of the TOE 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 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

SFR	Dependencies	Support of the Dependencies
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
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/PIN	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_AFL.1/C&R	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled
FIA_UAU.5	No dependencies	-
FIA_UAU.7	FIA_UID.1 Timing of identification	Fulfilled
FIA_UID.1	No dependencies	-
FMT_MSA.1/Terminal	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FDP_ACC.1/Terminal, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1/Man-	[FDP_ACC.1 Subset access control, or	Fulfilled by

SFR	Dependencies	Support of the Dependencies
agement	FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	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
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.

For the case that the ST author would extend these information flow policies in a way that they require security attributes they shall consider the dependency to FMT_MSA.3.

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.

6.3.2.2 Security Assurance Requirements Rationale

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

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

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

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)

6.3.3 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 [2] are used to fulfil the security objectives.

7 TOE summary specification (ASE_TSS)

7.1 Security Functions

7.1.1 SF_1: Trusted Communication Channels

For all communication functions used by eHealth/SAC applications to the connector/SAC and remote users via the trusted channel the TOE will always establish a trusted communication channel to the connector/SAC or remote user 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.

The card terminal permits the connector/SAC and remote users to initiate communication via the trusted channel.

The TOE only allows one connection to one connector/SAC at a time.

According to the gematik release OPB3 specifications the TOE is capable to support RSA and alternatively ECC cryptography for TLS connectivity (see [21] ECC migration). The ability to support ECC encryption/decryption and ECDSA for signature creation and approval depends on the SM-KT provided functionality as defined by [7], [24] and [25].

The cryptographic keys will be destroyed by writing of 0x00 to the memory before it is deallocated.

All SICCT communication, except service discovery will be encrypted.

(FTP_ITC.1/Connector, FTP_TRP.1/Management, FCS_CKM.1/Connector, FCS_CKM.1/Management, FCS_COP.1/SIG, FCS_COP.1/Con_Sym, FCS_COP.1/Management, FDP_IFC.1/NET, FDP_IFF.1./NET, FCS_CKM.4)

7.1.2 SF_2: Identification & Authentication

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

- a PIN based local authentication mechanism
- a remote authentication mechanism for the SICCT-interface
- an interface for authentication of the administrator by performing a Challenge & Response operation with the TOE

To perform the secured management function (see 7.1.7) the administrator of the TOE first must identify and authenticate himself.

On at least 3 consecutively unsuccessful authentication attempts the TOE will lock the authentication mechanism for a period of time, specified in Table 14:

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

Table 14: Lockout Intervals (TSF)

On delivery, after reset to factory defaults and after successfully performing a Challenge / Response operation between TOE and administrator the validity of the administrator PIN (management interface PIN) is set to *not valid*. When

the validity of the administrator PIN is set to *not valid* the administrator is forced by the TOE to set the administrator PIN before any other action can be performed by the TOE. After setting the administrator PIN the validity is set to *valid*.

After 5 unsuccessful response entries for a challenge the TOE will block further response data entries unless a new challenge has been generated.

(FDP_ACC.1/Terminal, FDP_ACF.1/Terminal, FDP_ACC.1/Management, FDP_ACF.1/Management, FIA_AFL.1/PIN, FIA_AFL.1/C&R, FIA_ATD.1, FIA_UAU.5, FMT_MSA.1/Management, FMT_MSA.3/Terminal)

7.1.3 SF_3: Network Connections

The TOE will accept any information arriving at the network interface from the connector/SAC only if the communication path is encrypted and the connector/SAC has been successfully authenticated. A connector/SAC authentication is not required for SICCT commands by unauthorized users as listed in the following paragraph.

The TOE accepts the following SICCT commands arriving at the network interface even if no pairing process is established, no valid connector/SAC certificate is required for unauthorized users (**FDP_IFF.1.4/NET)**:

- SICCT CT INIT CT SESSION
- SICCT CT CLOSE CT SESSION
- SICCT GET STATUS

The TOE accepts the following SICCT commands arriving at the network interface even if no pairing process is established, no valid connector/SAC certificate is presented for administrator (**FDP_IFF.1.4/NET)**:

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

The TOE additionally accepts the following EHEALTH commands arriving at the network interface if no pairing process is established but a valid connector/ SAC certificate is presented:

- EHEALTH TERMINAL AUTHENTICATE.

The information flow is based on the following rules:

- never lets Passwords for management interfaces leave the TOE
- never lets the shared secret leave the TOE in clear text (even over trusted channel)
- never transfers patient data via the management interfaces**.**

(FDP_IFC.1/NET, FDP_IFF.1/NET)

7.1.4 SF_4: 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.

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

- 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 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. For the use in the German Healthcare System the named versions are also approved by the gematik.
- In case of a common update the TOE installs the new firmware list at first. The new list is used to decide whether an update to the accompanying firmware core is allowed.
- Downgrades of the firmware list are not allowed.
- No subject can modify the public key for the signature verification for firmware updates

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.

Updates of the TSP CA list are performed only as part of a firmware update with signature verification.

(FDP_ACC.1/Terminal, FDP_ACF.1.2/Terminal, FCS_COP.1/SIG_TSP, FCS_COP.1/SIG_FW)

7.1.5 SF_5: Secure PIN-entry

No subject shall read out the PIN or management credentials while they are temporarily stored in the TOE. All PINs are stored in volatile memory only.

PINs for a card in a slot of the TOE or a remote card terminal will never be stored in a non-volatile memory of the TOE when the PIN is entered.

The PIN entered by the user will only be sent to the addressed card in the card slot of the TOE or via a TLS secured connection to the connector/SAC to a remote card terminal for remote-PIN verification.

For PIN entry the TOE supports a secure PIN-entry mode. This mode can only be activated by the TOE and is indicated by a padlock symbol for every PIN digit that has to be entered. For every entered PIN digit the padlock symbol is replaced by an asterisk symbol. PINs and PIN digits will never be displayed. The administrator-PIN will never leave the TOE.

PIN entry will be checked for PIN length of 8 digits for the management interface . A PIN must be composed of at least the following characters: "0"-"9". PINs for management cannot be saved on programmable function keys.

(FDP_ACC.1/Terminal, FDP_ACF.1.4/Terminal, FDP_IFC.1/PIN, FDP_IFF.1/PIN, FIA_SOS.1, FIA_UAU.7, FTA_TAB.1/SEC_STATE)

7.1.6 SF_6: Secure Data Deletion

Memory no longer used for storage of PIN, cryptographic keys, all information that is by a card in a slot of the TOE or by the connector/SAC (except the shared secret), will be erased by overwriting with 0x00 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. 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) will securely deleted and written with 0x00.

(FCS_CKM.4, FDP_RIP.1, FDP_ACC.1/Management, FDP_ACF.1/ Management)

7.1.7 SF_7: Secure Management-Functions

The TOE is aware of three roles: administrator, reset administrator and user. To identify and authenticate the roles administrator and reset administrator 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:

Only if the TOE administrator's local management PIN has been set, which also changes the PIN validity attribute from *not valid* to *valid,* a subject can access objects under TOE control.

The TOE allows the TOE administrator in addition to functions executable by all roles to perform the following management functions:

- Manage local management login credentials
- Perform the pairing process (initial pairing, review of pairing- information and maintenance-pairing) with the connector/SAC
- Secure deletion of pairing information from all three possible pairing processes
- View/set card terminal name for card terminal
- Perform a firmware update
- Reset the TOE settings to factory defaults
- Perform self-test by verifying the integrity of the TSF data and the TSF and receive results
- Managing network configuration
- Enable/Disable remote update functionality for firmware update

The following management functions are executable by all roles:

- Display the product version information of the TOE
- Manage login credentials if unset in factory delivery state
- View card terminal name for card terminal
- View the available network configuration
- Display the MAC-address of the TOEs network interface
- generate challenge data for a C&R operation
- enter response data for a C&R operation

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:

- Perform the initial pairing possible pairing processes with the connector/SAC.

The TOE Reset Administrator only is able to execute the Reset the TOE settings to factory defaults (fallback).

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

After a successful performance of a Challenge & Response operation the management credentials attribute *validity* is set to *not valid*.

According to Application Note 8 in [19], an unauthorized reset mechanism is optional, and the management function to enable/disable the mechanism is only required if it is implemented (which is not the case for the current TOE). Therefore FMT_MSA.1/Terminal is trivially fulfilled.

The TOE restricts the ability to query, modify, delete the security attributes of all management functions to the TOE administrator.

(FMT_SMR.1, FDP_ACC.1/Terminal, FDP_ACF.1/Terminal, FMT_SMF.1, FPT_TST.1, FDP_ACC.1/Management, FDP_ACF.1/Management, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Terminal, FMT_MSA.1/Management, FMT_MSA.2, FMT_MSA.3/Terminal, FMT_MSA.3/Management)

7.1.8 SF_8: Self-Test

The TOE can perform self-test on power-on and after activation by an authorised user.

The following tests are performed at after activation by an authorized user:

1. Integrity tests of parts of the TSF (all applications, scripts and shared libraries in the root file system are verified),
1. Known-answer test for the cryptographic algorithms that are used for TLS (i.e. AES128, AES256, MD5, SHA1, and SHA256), and
2. Integrity tests of parts of the TSF data (TSP CA certificates).

During start-up and after activation by an authorized user the following tests are performed by the TOE:

3. Integrity tests of parts of the TSF (all applications, scripts and shared libraries in the root file system are verified),
4. Known-answer test for the cryptographic algorithms that used for firmware update (i.e. RSA4096 and SHA256), and
5. Status check of the tamper detection realizing FPT_PHP.3.

By performing these integrity tests and the hardware test the correct operation of the TSF is ensured at every start-up.

For integrity-verification, a SHA256 hash calculation is used.

(FPT_TST.1, FPT_PHP.3)

7.1.9 SF_9: Secure Fail-State

In case of

- an alarm condition indicates possible tampering or if a
- self-test detects an error or
- failure during firmware update

the TOE will be put into a secure fail state.

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

(FPT_FLS.1)

7.1.10 SF_10: Physical Protection of the TOE

The TOE is protected against unnoticed tampering by security seals which will be visibly destroyed on attempts to tamper with the TOE body. The TOE has an alarm function constantly checking switches triggering an alarm on opening the TOE housing and a drill and probing protection foil for alarm conditions which are drilling and probing attacks to the bottom side, the left and right side and the rear side of the TOE causing short-cuts or interruption of the circuit paths on the foil. On alarm (indicating possible tampering) the alarm function will put the TOE in a defined non-functioning state (see SF_9) and will display a message on the TOE display. The alarm condition remains even after a TOE reset.

(FPT_FLS.1, FPT_ITT.1, FPT_PHP.1, FPT_PHP.3)

7.2 Security Measures

7.2.1 SM_1: Sealing

The TOE is protected against unnoticed manipulations by security seals.

The seals are sticky seals, carry authenticity attributes and fulfil the requirements of security level 2 according to BSI 7500.

The seals are placed over the jointing of the body parts.

Seal positions, their look and how to identify broken security seals with be described in the guidance documents.

7.3 Mapping of the Security functions

	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7	SF_8	SF_9	SF_10
FCS_CKM.1/Connector	X									
FCS_CKM.1/Management	X									
FCS_CKM.4	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		X			
FDP_ACC.1/Management		X				X	X			
FDP_ACF.1/Terminal		X		X	X		X			
FDP_ACF.1/Management		X				X	X			
FDP_IFC.1/PIN					X					
FDP_IFF.1/PIN					X					
FDP_IFC.1/NET	X		X							
FDP_IFF.1/NET	X		X							
FDP_RIP.1						X				
FIA_AFL.1/PIN		X								
FIA_AFL.1/C&R		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			

	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7	SF_8	SF_9	SF_10
FMT_MSA.1/Terminal							X			
FMT_MSA.1/Management		X					X			
FMT_MSA.2							X			
FMT_MSA.3/Terminal		X					X			
FMT_MSA.3/Management							X			
FMT_SMF.1							X			
FMT_SMR.1							X			
FPT_TST.1							X	X		
FPT_FLS.1									X	X
FPT_ITT.1										X
FPT_PHP.1										X
FPT_PHP.3								X		X
FTA_TAB.1/SEC_STATE					X					
FTP_ITC.1/Connector	X									
FTP_TRP.1/Management	X									

Table 15: Mapping Security Function to SFRs

8 Glossar

AES	Advanced Encryption Standard
BCS	Basic Command Set
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CT	Card Terminal
DF.KT	Dedicated File Kartenterminal
DMS	Dokumentenmanagementsystem
eGK	elektronische Gesundheitskarte
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptograhie
ECDSA	Elliptic Curve Digital Signature Algorithm (DSA)
HPC	Health Professional Card
ID	Identity
KSR	Configuration and Software Repository- Service of the telematics infrastructure
KT	Kartenterminal
KVK	Krankenversichertenkarte
LAN	Local Area Network
LED	Light Emitting Diode
MAC-Address	Media Access Control-Address
PIN	Personal Identification Number
RFID	Radio-Frequency Identification
RSA	Asymmetrical Cryptographie (Rivest, Shamir und Adleman)
SAC	Signature Application Component
SFP	Security Function Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable Chip Card Terminal
SMC	Security Module Card
SM-KT	Security Module Kartenterminal
SM-K	Security Module Konnektor
ST	Security Target
TBD	to be defined
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	Trust-Service Provider that issues connector/SAC certificates

USB	Universal Serial Bus

9 References

Common Criteria

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

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

Specifications

[6] TeleTrusT SICCT-Spezifikation as referenced by [7]

[7] gematik: Spezifikation eHealth-Kartenterminal, Version 3.12.0 , Stand 02.03.2020

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

[15] RFC5246 The TLS Protocol, Version 1.2

[17] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002

[21] gematik:Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.15.0, 02.10.2019

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

[24] gematik: Spezifikation der gSMC-KT Objektsystem, Version 3.9.0, Stand 24.08.2016, gemSpec_gSMC-KT_ObjSys, Generation G2

[25] gematik: Spezifikation der gSMC-KT Objektsystem, Version 4.2.0, Stand 14.05.2018, gemSpec_gSMC-KT_ObjSys_G2.1, Generation G2.1

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

[TR-03120-A] BSI TR-03120 Appendix, „Anhang: Kartenterminalsschutz" zur Technischen Richtlinie BSI TR-03120, Version 1.1

[ST33TPHF20] Datasheet ST33TPHF20SPI, ST | Trusted Platform Module 2.0 with TCG SPI interface , März 2016

Protection Profiles

[19] / [PP] Common Criteria Protection Profile *Electronic Health Terminal (eHCT)*, BSI-CC-PP-0032-V2-2015-MA-01, Version 3.7, 21.09.2016.

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

Analysis

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