JDM
Payment Solutions
a PHOENIX company

ASE_ST
Y7
Security Target for the Evaluation of the Product
JDM Y7
of
JDM Payment Solutions SAS
according to the Common Criteria 3.1
Level EAL3+
Certification Id:
BSI-DSZ-CC-1233

Table of Contents

Version History

Rev	Date	Author	Modifications
0.0.6	07/11/2023	J. Bain	See ST Changelog v0.0.6
0.0.7	07/12/2023	J. Bain	See ST Changelog v0.0.7
0.0.8	18/01/2024	J. Bain	Updates following Observation Report 0.5
0.0.9	01/02/2024	J. Bain	Updates following Observation Report 0.7
0.0.10	09/02/2024	J. Bain	Updates following Observation Report 0.9
0.0.11	19/02/2024	J. Bain	Updates to Fig 2 and 7.3
0.0.12	15/07/2024	J. Bain	Updates following Observation Report 0.12
0.0.13	06/12/2024	J. Bain	Update to 1.3.2 Hardware Scope and 7.7 TOE Access
0.0.14	19/12/2024	M. Quercia	Removed HMAC SHA256 for Secure Firmware Update Removed AES_CCM for FCS_COP.1.1/Con_Sym
0.0.15	06/02/2025	J. Bain	Update to key algorithm in FCS_COP.1/SIG_FW (1)
0.0.16	11/04/2025	J. Bain	Update to key algorithm in FCS_COP.1/SIG_FW (1) & update to TOE version.
0.0.17	31/10/2025	J. Bain	Update to FW & eHealth application version numbers
0.0.18	30/01/2026	J. Bain	Update to FW & eHealth application version numbers

1. ST Introduction

1.1. ST Reference

Certification ID	BSI-DSZ-CC-1233
CC Version	3.1
Assurance Level	The assurance level for this ST is EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA_VAN.4.
Document Version	0.0.18
Date	30/01/2026

1.2. TOE Reference

Target of Evaluation	Y7
TOE Version	4.3.1:1.3.2 with eHealth Application 1.1.24
Developer	JDM Payment Solutions SAS

1.3. TOE Overview

This Security Target defines the security objectives and requirements for the **Y7 Electronic Health Card Terminal** based on the regulations for the German healthcare system.

1.3.1 TOE description and operational usage

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 [14] for further information about card compatibility. The TOE fulfils the requirements to be used as a secure PIN pad entry device for applications according to [14], which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.

The Terminal operates in 4 modes – secure mode (eHealth), payment mode, application mode and tamper mode.

- Secure Mode (eHealth)
  This mode is a security enforcing part of the TOE.
  A header is displayed informing users that eHealth mode is active.
  When a card entry request has been made and a valid eHealth card has been inserted, the PIN entry screen will be displayed with banners and pop ups notifying users that it is safe to enter their PIN.

- Tamper Mode
  This mode is a security enforcing part of the TOE.

  In the event of Tamper the master key is deleted preventing any access to sensitive data. This renders the terminal inoperable and is immediately made evident to the user on the secure display.
  Tamper mode is always active and can be entered from any of the other modes.

- Payment Mode
  This mode is a security non-interfering part of the TOE.
  It is used to handle secure payment transactions including PIN entry.
  A notification is displayed that users should not enter their eHealth PIN.

- Application Mode
  This mode is not part of the TOE.
  It is used for non-security related operations including Android applications.
  A notification is displayed that users should not enter their eHealth PIN.

The TOE for use in the German health care is based on the specification SICCT, which is adapted for operation by profiling as eHealth card terminal (see [15]).

1.3.2 Hardware Scope

The terminal is based on a two-chip architecture which combines the NXP/Freescale MK81FN256VDC15 (K81) security processor and the application processor NXP/Freescale MCIMX6QP5EYM1AA (iMX6Q).

Security Modules (SM): devices for management of cryptographic keys and cryptographic functions.

- NXP/Freescale MK81FN256VDC15 (K81) security processor –The eHealth Application and terminal OS run on this.

- Secure FPGA – The Secure FPGA is used to handle the security of display prompts (PIN Entry). It also provides APIs for handling EC point addition and EC point multiplication operations as part of EC cryptography operations.

- Atmel Touchscreen controller – controls the input of prompts

- QSPI Boot – stores initial yOS firmware for Secure Initialization

- SDRAM – overflow memory storage for secure applications

The TOE is a standalone terminal with all eHealth, security components and card readers contained within the Core TSF. The TOE has active physical anti-tamper mechanisms to protect sensitive components including card readers and processors.

The TOE has 2 ID-1 smart card readers, 2 ID-000 readers and an NFC contactless reader. These are all controlled through the secure processor to enable the eHealth application to have sole control.

User I/Os:

- Display
- Touch Panel
- Front and back cameras
- Security LEDS
- LED Ring
- USB x 2
- Power Button
- Speaker
- Buzzer
- Up / Down Buttons

The Operations Manual provides guidance to administrators and users.

Display

The TOE has an integrated display – 7 inch colour with 1280 by 800 pixels resolution. In Secure (eHealth) mode, all Display outputs are controlled by SICCT running on the secure processor.

1.3.3 Logical Scope

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, and
- Active physical protection

And is limited by the functionality for which the TOE relies on the services of the SM-KT, which is not part of the TOE.

The NFC functionality is not modelled to the SFRs.

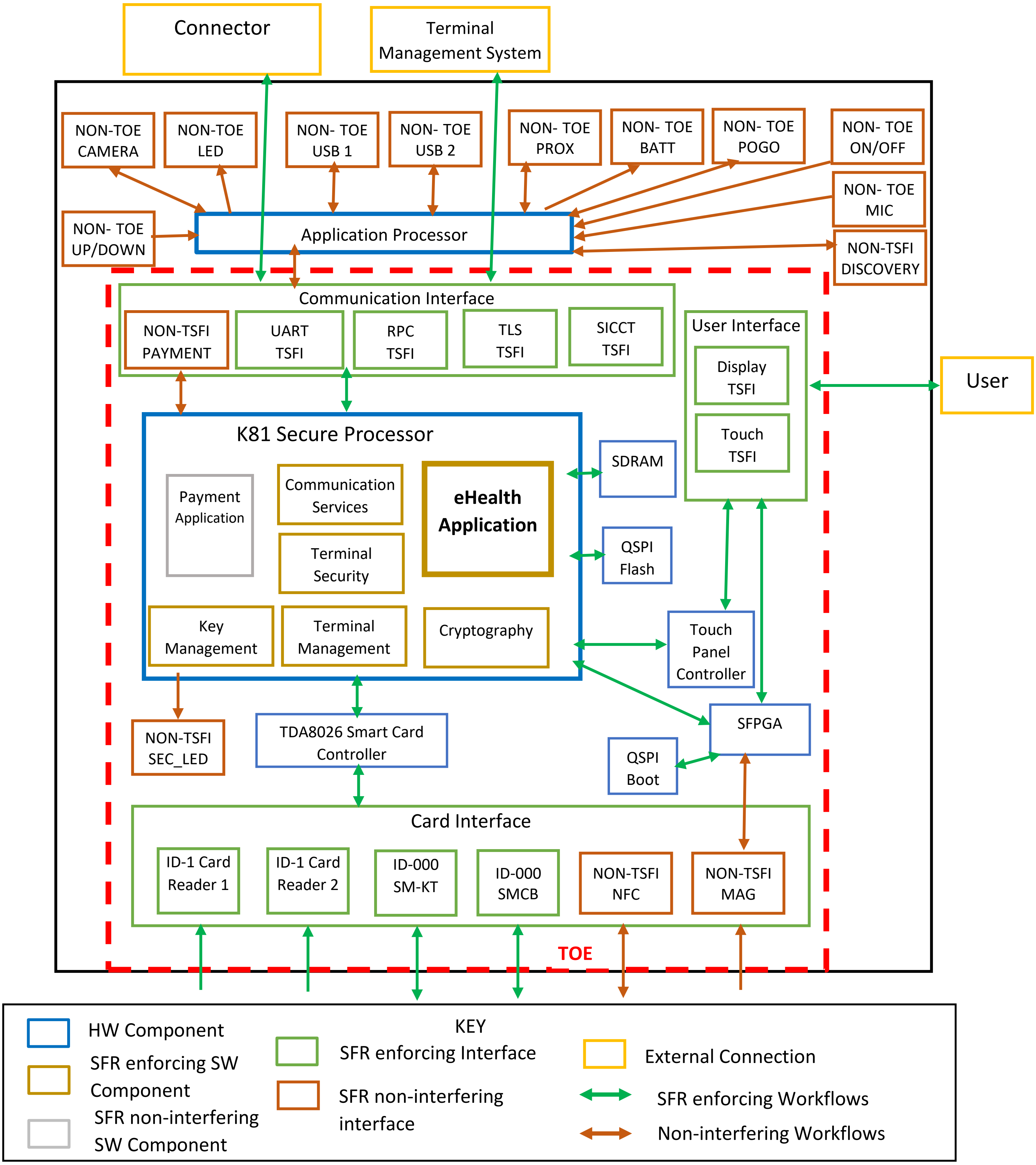

Fig 2 TOE Hardware and Software Architecture

The TOE works with a cryptographic key for authentication, integrity assurance and to ensure the confidentiality of data transmitted. Due to the very high protection requirements of the information objects transmitted, 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[1].

In its environment, the TOE communicates with a so called connector. This 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.

1.3.4 TOE major security features for operational use

To protect the communication between the connector and the TOE the TOE possesses a cryptographic identity (in form of a X.509 certificate) and functionality for encryption/decryption as well as signature creation (see also [14]).

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 based on RSA (and for card generation G2.1 also ECC) for encryption/decryption and signature creation
- A random number generator
- A function to read out the public key

Even though this SM-KT is physically within the cage of the TOE it does not belong to the logical and physical scope of the TOE as seen in Figure 2. More information about the SM-KT can be found in the Protection Profile Card Operating System 2 (PP COS G2) [11] and the gematik specification on the gSMC-KT object system [16].
The TOE uses a DF.KT of a gSMC-KT as SM-KT, which is addressable via the Connector. The TOE accesses this DF.KT via the base-channel 0. During use of the SM-KT by the TOE the terminal card commands of the TOE are priorized and the processing of possibly existing client SICCT commands interrupted and continued only after completion of the internal command sequence. The connector makes sure that a DF.KT of a gSMC-KT as SM-KT which is

[1] Please note that firmware update could also mean a firmware downgrade. Both actions are possible. The developer of the TOE ensures that in case of a downgrade of the firmware the TOE warns the Administrator before the installation that the action to be performed is not an upgrade. The TOE offers a chance to cancel the installation.

[2] Please note that the SM-KT is only responsible for the core functions of the asymmetric cryptography (RSA & ECDSA) and for random number generation. The TOE will be responsible for negotiating the session with the connector and for encryption/decryption using a symmetric AES key. More details can be found in [10] and the following chapters.

addressable via the connector is only be accessed by the TOE and not be used by any other system than the TOE.

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 is preserved and indicated after a firmware update or a downgrade (see [14] for further information). The developer of the TOE has ensured that in case of a downgrade of the firmware of the TOE the Administrator is warned by a display notification before the installation that the action to be performed is not an upgrade. The TOE offers a chance to cancel the installation. The developer-specific update component warns the administrator about taking the responsibility in case of performing a downgrade.

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

- Initial pairing:

This provides a logical connection from the perspective of the connector by using shared secret between card terminal and SM-KT

- Review of pairing- information:

The connector checks as a second step of authentication, if the card terminal is in the possession of the shared secret after establishing the TLS connection.

- Maintenance-pairing:

Announcement of a new connector certificate on the card terminal by using a known shared secret. Please see [14] for further information on the pairing process.

The TOE is also able to send/receive a PIN to/from a remote card terminal. This communication is routed via the connector. The connector never 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.

1.3.5 TOE Type

The TOE is an Electronic Health Card Terminal based on the regulations for the German healthcare system. It is a smart card terminal with secure PIN entry functionality and fulfils the requirements for the use within the German telematic infrastructure. The physical scope of the TOE comprises

- The hardware and sealed cage of the smart card terminal,
- The firmware of the smart card terminal and
- The related guidance documents

Please note that even though the SM-KT is physically within the cage of the terminal this module does not belong into the scope of the TOE as described in this ST.

The TOE features active detection of physical attacks.

Further 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 is installed into the card terminal. Functionality that is relying on the SM-KT for secure operation will not work as intended before the SM-KT is installed. Therefore, the developer has described – as part of the evidence for assurance requirements in ALC_DEL – how such functionality can be securely used.

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

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

And is limited by the functionality for which the TOE relies on the services of the SM-KT, which is not part of the TOE.

1.3.6 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 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 is a DF.KT of a gSMC-KT as SM-KT.

Although this secure module is physically placed within the cage of the TOE it does not belong to the logical and physical scope of the TOE.

- A 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 which can interact with a DF.KT of a gSMC-KT as SM-KT as mentioned above.

2. Conformance Claim

2.1. Common Criteria conformance

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, 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; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

has to be taken into account.

2.2. PP conformance

This security target claims strict conformance to

- Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, Version 3.8, 15.12.2022

2.3. Package conformance

This security target claims conformance 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 rationale

This security target is strictly conformant to Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, Version 3.8, 15.12.2022:

- Threats in this security target are identical to the threats in the Protection Profile.
- Organisational Security Policies in this security target are identical to the OSPs in the Protection Profile.
- Assumptions in this security target are identical to the Assumptions in the Protection Profile.

3. Security Problem Definition

This chapter describes

- the assets that need to be protected by the TOE,
- the subjects that are interacting with the TOE,
- the threats that have to be countered by the TOE,
- the organizational security policy that TOE complies with, and
- the assumptions that need to be ensured for the environment of the TOE.

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. This asset is user data.
Management credentials	The TOE stores credentials (e.g. passwords) to authenticate TOE administrators for management activities. The TOE has to ensure the confidentiality and integrity of these credentials. This asset is user data.
Shared secret	The TOE stores a shared secret which is generated by the connector during the initial pairing process. The shared secret and the SM-KT represent the identity of the card terminal. This identity is used for secure identification and authentication of the card terminal by the connector. The TOE has to ensure the confidentiality and integrity of the shared secret. This asset is TSF data.
Patient Data	This data comprises health information and billing data that is related to patients. The TOE gets patient data from the cards in its slots, encrypts this data and sends it to the connector. Further the TOE accepts patient data from the connector, decrypts it, and sends it to the corresponding eHC in its slot. The TOE has to ensure the confidentiality and authenticity of this data. This asset is user data.
Communication data	Confidential data that is transmitted between the TOE and the connector. This data comprises at least patient data and PINs for remote-PIN verification. The TOE has to ensure the confidentiality and authenticity of this data. This asset is user data.

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 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.

Table 1: Assets

3.2. Subjects

The following subjects are interacting with the TOE:

Subject	**Description**
TOE Administrator	The TOE administrator is in charge of managing the security functions of the TOE.
Attacker	A human, or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify application sensitive information. The attacker has a moderate level attack potential.
Authorized card	Authorized cards (HPC, SMC-B) are able to perform card-to-card authentication which is used for remote-PIN verification.
Card	The TOE is handling the communication for one or more smart cards in its card slots.
Connector	The connector is the only entity in the environment of the TOE (except for users of the management interface) which is foreseen to communicate with the TOE. It is the interface for the TOE to securely communicate with the telematic infrastructure of the German healthcare system.
Medical supplier	The medical supplier (e.g. a physician) uses the TOE together with his HPC (or SMC-B). With the HPC it is also possible for medical suppliers to generate qualified digital signatures. Other than the patient the medical supplier can be held responsible for the secure operation of the TOE.

Subject	Description
Patient	The patient uses the TOE together with his eHC. The patient uses the TOE for other services of the eHC. A patient will never use the services of the TOE alone but will always be guided by the medical supplier.
Push Server	The Push Server is a trusted entity in the internal network of the medical supplier which updates firmware on card terminals that are connected to that network. The Push Server uses the SICCT interface or another network interface of the card terminal for remote update. See A.PUSH_SERVER for assumptions on the Push Server.
Terminal Management System	The Terminal Management System (TMS) connects to the TOE to enable secure firmware updates.
HSM	The HSM connects to the TOE in the Secure Room of the Manufacturing Facility to enable initial key and firmware loading.
SM-KT	The SM-KT represents the cryptographic identity of the TOE. It is a secure module that carries a X509 certificate and provides : • Protection of the private key • Cryptographic functions for encryption/decryption and signature creation • A random number generator • A function to read out the public key
TOE Reset Administrator	The TOE Reset Administrator is the only user role that is able to perform a reset of the TOE settings when management credentials are lost. The type of authentication for this role depends on the particular implementation. The TOE Reset Administrator could be the developer himself.
User	A user is communicating with the TOE in order to use its primary services, i.e. to access a smart card which has been put into one of the slots of the TOE before. The TOE is used by different kinds of users including medical suppliers, patients and administrators.

Table 2: Subjects

3.3. Threats

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

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

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

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

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

The assets that are threatened and the paths for each threat are defined in the following table:

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

T.F-CONNECTOR	Unauthorized personnel may try to initiate a pairing process with a fake connector after an unauthorized reset to factory defaults, e.g. to initiate an unauthorized firmware update or to receive confidential (patient) data.

Table 3: Threats

3.4. Organizational Security Policies

The TOE is implemented according to the following specifications:

Policy	Description
OSP.PIN_ENTRY	The TOE shall fulfil the requirements to be used as a secure PIN pad entry device for applications according to [14]. This specifically means that a PIN, which has been entered by a user at the TOE, must never leave the TOE in clear text, except to smart cards in local card slots. For the case that a terminal implements an insecure mode (e.g. a mode, in which it cannot be guaranteed that the PIN will not leave the TOE or a mode in which not trustworthy entities are allowed to communicate with the TOE) the TOE has to be able to inform the medical supplier whether it is currently in a secure state or not.

Table 4: Organisational Security Policies

3.5. Assumptions

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

Assumption	Description
A.ENV	It is assumed that the TOE is used in a controlled environment. Specifically it is assumed: • The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible, • That the user handles his PIN with care; specifically that the user will keep their PIN secret, • That the user can enter the PIN in a way that nobody else can read it, • That the user only enters the card PIN when the TOE indicates a secure state, • That the medical supplier checks the sealing (if applicable) and the physical integrity of the TOE regularly before it is used, • That the network of the medical supplier is appropriately secured so that authorized entities are trustworthy, see also [12].

A.ADMIN	The administrator of the TOE and the medical supplier shall be nonhostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier shall be responsible for the secure operation of the TOE. Specifically it shall be ensured: • That they enforce the requirements on the environment (see A.ENV), • That the administrator ensures that the medical supplier received the necessary guidance documents (especially for firmware updates), • That the physical examination of the TOE is performed according to the process described by the manufacturer in the evaluation process (e.g. seal checking if applicable), • That the administrator checks the integrity of the terminal before the initial start-up procedure (every new pairing process) and the medical supplier checks the integrity of the terminal before every start-up procedure, • That they react to breaches of environmental requirements according to the process described by the manufacturer in the evaluation process (e.g. reshipment to the • manufacturer).
A.CONNECTOR	The connector in the environment is assumed to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for a mutual authentication. It is assumed that the connector has undergone an evaluation and certification process in compliance with the corresponding Protection Profiles [12]. Further it is assumed that for the case the TOE uses a DF.KT of a gSMC-KT as SM-KT which are addressable via the connector, the TOE accesses this DF.KT via the base-channel 0. During the use of the SM-KT by the TOE the terminal card commands of the TOE have to be given precedence and the processing of possibly existing client SICCT commands has to be interrupted and continued only after completion of the internal command sequence. The developer may queue the interrupts internally or implement error messages as answers to the commands. It is also assumed that the connector makes sure that a DF.KT of a gSMC-KT as SM-KT which is addressable via the connector can only be accessed by the TOE and cannot be used by any other system than the TOE. Further, it is assumed that the connector periodically monitors the pairing state with the TOE and provides warning mechanisms to

	indicate unexpected results like paired terminals which lack the shared secret.
A.SM	The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate. It is assumed that the cryptographic keys in this module are of sufficient quality and the process of key generation and certificate generation is appropriately secured to ensure the confidentiality, authenticity and integrity of the private key and the authenticity and integrity of the public key/certificate. The random number generator of the SM-KT is assumed to provide entropy of at least 100 bit for key generation. It is further assumed that the secure module is secured in a way that protects the communication between the TOE and the module from eavesdropping and manipulation and that the SM-KT is securely connected with the TOE (according to TR-03120 [7] and its appendix [8]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [11] and complies with the specification [16].
A.PUSH_SERVER	It is assumed that the internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [14]. The TOE administrator is assumed to be responsible for the operation of the Push Server and able to select the particular firmware version that the server is allowed to install on the card terminals. It is further assumed that every time an update process is performed for a card terminal the Push Server logs the following information: identifier of involved card terminal, version of firmware to install, result of the update process.

A.ID000_CARDS	It is assumed that all smartcards of form factor ID000 are properly sealed after they are brought into the TOE. Further, the developer is assumed to provide guidance documentation on how a TOE administrator could renew a sealing after an ID000 card is replaced by another one.

Table 5: Assumptions

4. 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 are met by the TOE:

Objective	Description
O.ACCESS_CONTROL	To protect the configuration of the TOE against unauthorized modifications only an authorized user shall be able to read out information about the current configuration of the TOE and only the administrator shall be able to modify the settings of the TOE. Therefore the TOE shall provide an access control function based on the identity of the current user. Further the access control mechanism of the TOE has to ensure that the PIN cannot be read from the TOE. The TOE shall also ensure that the TOE administrator's credentials for local management are set before access to other TOE functionality is possible.
O.PIN_ENTRY	The TOE shall serve as a secure pin entry device for the user and the administrator. Thus the TOE has to provide the user and administrator with the functionality to enter a PIN and ensure that the PIN is never released from the TOE in clear text, except to smart cards in each addressed local card slot. For remote-PIN verification the PIN shall be encrypted, by a local gSMC-KT, controlled by the Connector, so that it can only be decrypted by the receiving smart card (HPC or SMCB).
O.I&A	For its access control policy and for parts of the management functionality the TOE has to be aware of the identity of the current user. Thus the TOE has to provide a mean to identify and authenticate the current user. The TOE shall maintain at least three distinct roles: administrators, the TOE Reset Administrator, and users[3].

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

Objective	Description
O.MANAGEMENT	In order to protect its configuration the TOE shall provide only an authenticated and authorized administrator with the necessary management functions. The TOE shall enforce an access control policy for management functions, as some functions shall only be accessible by administrators authenticated by the local management interface. Further, the following management functions can be used by unauthenticated users • Display the product version number of the TOE • View card terminal name for card terminal The TOE shall provide a local management interface, and management over SICCT interface. A firmware consists of two parts: (1) the so-called “firmware list” and (2) the “firmware core” which includes the whole firmware except the firmware list. Firmware lists and cores have to versioned independently. The firmware list states all firmware core versions to which a change is allowed: An update of the firmware core is only allowed if the core version is included in the firmware list. A firmware update of the TOE shall only be possible after the integrity and authenticity of the firmware has been verified and the following holds: • The TOE provides functionality to update and downgrade its firmware. This includes both the change to a newer firmware as a downgrade to a firmware which is approved with the concept of firmware-group. • The configuration, such as terminal type, IP address or pairing-information shall be preserved and indicated after a firmware update or a downgrade (see [14] for further information). • The developer of the TOE shall ensure that in case of a downgrade of the firmware the TOE must warn the Administrator (e.g. within the Guidance) before the installation that the action to be performed is not an upgrade. The TOE must offer a chance to cancel the installation. The developer- specific update component shall warn the administrator about taking the responsibility in case of performing a downgrade. The administrator shall be able to manage the list of TSP CAs which is used to verify the authenticity of connectors. An update of the TSP CA list shall only be possible after the integrity and authenticity of the list has been verified. The TOE shall ensure that for all security attributes, which can be

Objective	Description
	changed by an administrator or the user, only secure values are accepted. This includes the enforcement of a password policy for the management interfaces. In addition to the developer-specific update component the TOE supports update features of the SICCT specification, whereby a trigger component is able to update the TOE (e.g. the Configuration and Software Repository-Service (KSR) of the telematic infrastructure).
O.SECURE_CHANNEL	When establishing a connection between the TOE and the connector both parties shall be aware of the identity of their communication partner. Thus the TOE has to provide a mean to authenticate the connector and to authenticate itself against the connector in accordance with [14]. The TOE in each security context shall only have one connection to one connector at a time. For all communications which fall into the context of the electronic health card application the TOE shall only accept communication via this secure channel to ensure the integrity, authenticity and confidentiality of the transmitted data. Only functions to identify the TOE in the network (service discovery) may be available without a secure channel.
O.STATE	In principle it would be possible that a card terminal compliant to the Protection Profile realises more than just the necessary set of functionality as required by the PP. However, additional functionality that is not security functionality (e.g. value-added modules) may lead to an insecure state of the TOE as the user may be not aware of the fact that they are using a functionality, which doesn’t fall into the scope of the certified TOE or because a part of the security functionality as required by this ST is not working during its use. Thus the TOE shall be able to indicate whether it is currently in a secure state, i.e. whether all TSF as required by this ST are actually enforced.

Objective	**Description**
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 TOE Security Policy within 10 minutes can be afterwards detected by the medical supplier. To avoid interference the TOE has to ensure that each connection is held in its own security context where more than one connection of a TOE to a connector is established. Also if more than one smart card in the slots of the TOE is in use the TOE has to ensure that each connection is held in its own security context. The TOE shall delete • PINs, • cryptographic keys, and • all information that is received by a card in a slot of the TOE or by the connector (except the shared secret) in a secure way when it is no longer used. In case a TOE comprises physically separated parts, the TOE shall prevent the disclosure and modification of data when it is transmitted between physically separated parts of the TOE.

Table 6: Security Objectives for the TOE

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

4.2. Security Objectives for the Operational Environment

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

Objective	Description
OE.ENV	It is assumed that the TOE is used in a controlled environment. Specifically it is assumed: • The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible, • That the user handles his PIN with care; specifically that the user will keep their PIN secret, • That the user can enter the PIN in a way that nobody else can read it, • That the user only enters the card PIN when the TOE indicates a secure state, • That the medical supplier checks the sealing if applicable and the physical integrity of the TOE regularly before it is used, • The medical supplier sends the TOE back to the manufacturer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel, and • That the network of the medical supplier is appropriately secured so authorized entities are trustworthy, see also [12].

Objective	Description
OE.ADMIN	The administrator of the TOE and the medical supplier shall be nonhostile, well trained and have to know the existing guidance documentation of the TOE. The administrator and the medical supplier shall be responsible for the secure operation of the TOE. Specifically it shall be ensured: • That they enforce the requirements on the environment (see A.ENV), • That the administrator ensures that the medical supplier received the necessary guidance documents (especially for firmware updates), • That the physical examination of the TOE is performed according to the process described by the manufacturer in the evaluation process (e.g. seal checking if applicable), • That the administrator checks the integrity of the terminal before the initial start-up procedure (every new pairing process) and the medical supplier checks the integrity of the terminal before every start-up procedure, • That they react to breaches of environmental requirements according to the process described by the manufacturer (e.g. reshipment to the manufacturer), and • That the administrator checks the secure state of the TOE regularly[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 [12]. Further the connector has to periodically check the pairing state with the TOE and warn the administrator accordingly.

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

Objective	Description
OE.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 [7] and its appendix [8]). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile [11] and complies with the specification [16].
OE.PUSH_SERVER	The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism described in [14]. The TOE administrator is responsible for the operation of the Push Server and able to select the particular firmware version that the server is allowed to install on the card terminals. Every time an update process is performed for a card terminal the push server logs the following information: identifier of involved card terminal, version of firmware to install, result of the update process.
OE.ID000_CARDS	All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE.[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.

[6] Please see TIP1-A_3192 in [14].

4.3. Security Objectives Rationale

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

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

Table 8: Security Objective Rationale

4.3.1. Countering the Threats

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

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

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

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

4.3.2. Covering the OSPs

The organizational security policy **OSP.PIN_ENTRY** requires that the TOE has to serve as a secure PIN entry device [14] (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. *O.STATE* ensures that the TOE is able to indicate to the medical supplier, whether it is currently working in a secure state as required by OSP.PIN_ENTRY. Such a secure state includes (but is not limited to) that the secure PIN entry can be guaranteed. Finally *O.PROTECTION* ensures that the TOE is able to verify the correct operation of the TSF and that an adequate level of physical protection is provided.

4.3.3. Covering the Assumptions

The assumption **A.ENV** is covered by *OE.ENV* as directly follows.

The assumption **A.ADMIN** is covered by *OE.ADMIN* as directly follows.

The assumption **A.CONNECTOR** is covered by *OE.CONNECTOR* as directly follows.

The assumption **A.SM** is covered by *OE.SM* as directly follows.

The assumption **A.PUSH_SERVER** is covered by *OE.PUSH_SERVER* as directly follows.

The assumption **A.ID000_CARDS** is covered by *OE.ID000_CARDS* as directly follows.

5. Extended Components Definition

This security target uses no components which are not defined in CC part 2.

6. Security Requirements

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

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

All operations which have been performed from the original text of [2] are written in italics for assignments, underlined for selections and bold text for refinements. Selectable assignments are written in italics and underlined. Furthermore the [brackets] from [2] are kept in the text.

SFRs coloured grey are not implemented.

6.1. Security Functional Requirements for the TOE

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

Cryptographic Support (FCS)	
FCS_CKM.1/Connector	Cryptographic key generation for connector communication
FCS_CKM.1/Management	Cryptographic key generation for remote management
FCS_CKM.4	Cryptographic key destruction for communication
FCS_COP.1/Con_Sym	Cryptographic operation for connector communication (symmetric algorithm)
FCS_COP.1/SIG	Cryptographic operation for signature generation/verification
FCS_COP.1/Management	Cryptographic operation for remote management
FCS_COP.1/SIG_FW (1)	Cryptographic operation for firmware signature verification
FCS_COP.1/SIG_FW (2)	Cryptographic operation for firmware signature verification
FCS_COP.1/SIG_TSP	Cryptographic operation for signature verification of TSP CA lists

User data protection (FDP)	
FDP_ACC.1/Terminal	Subset access control for terminal functions
FDP_ACC.1/Management	Subset access control for management
FDP_ACF.1/Terminal	Security attribute based access control for terminal functions
FDP_ACF.1/Management	Security attribute based access control for management
FDP_IFC.1/PIN	Subset information flow control for PIN
FDP_IFF.1/PIN	Simple security attributes for PIN
FDP_IFC.1/NET	Subset information flow control for network connections
FDP_IFF.1/NET	Simple security attributes for network connections
FDP_RIP.1	Subset residual information protection
Identification and Authentication (FIA)	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
Security Management (FMT)	
FMT_MSA.1/Terminal	Management of security attributes for Terminal SFP
FMT_MSA.1/Management	Management of security attributes for management SFP
FMT_MSA.2	Secure security attributes
FMT_MSA.3/Terminal	Static attribute initialisation for Terminal SFP
FMT_MSA.3/Management	Static attribute initialisation for management SFP
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Protection of the TSF (FPT)	
FPT_FLS.1	Failure with preservation of secure state

FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
TOE Access (FTA)	
FTA_TAB.1/SEC_STATE	Default TOE access banners for secure state
Trusted path/channels (FTP)	
FTP_ITC.1/Connector	Inter-TSF trusted channel for connector communication
FTP_TRP.1/Management	Trusted path for remote management

Table 9: Security Functional Requirements for the TOE

6.1.1. Cryptographic Support (FCS)

6.1.1.1 FCS_CKM.1/Connector Cryptographic key generation for connector communication

FCS_CKM.1.1/Connector The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ephemeral Diffie–Hellman key exchange (*
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C)
using DHE group 14 for RSA
and curves:
P-256 and P-384]
and specified cryptographic key sizes [*128bit and 256bit for AES, 160bit, 256bit and 384bit for SHA*] that meet the following: [*[14]*].

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 (for further information see *[14]* and also chapter 6.1.1.4). The generation (actually negotiation) of this key is done in accordance with the TLS handshake protocol (see [16]).

It should be noted that this negotiation includes a mutual authentication of the TOE and the connector based on certificate validation (see [14]) and validation of a shared secret. The TOE determines the role from the connector certificate presented during the buildup of the TLS connection. The TOE checks that the determined role corresponds with the role "Signature Application Component (SAC)" (see [14]).

The TOE uses the SM-KT for Random Number generation, Signature generation and Signature Verification (see also A.SM) or its own functionality required by FCS_COP.1/SIG.

The connection to network based management interfaces is always secured with TLS according to [17].

6.1.1.2 FCS_CKM.1/Management Cryptographic key generation for remote Management

FCS_CKM.1.1/Management

This SFR is not implemented in the TOE. See Application Note 2.

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ephemeral Diffie–Hellman key exchange (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 using DHE group 14 for RSA and curves brainpoolP256r1 and brainpoolP384r1 for ECDSA*] and specified cryptographic key sizes [*128bit and 256bit for AES, 160bit, 256bit and 384bit for SHA*] that meet the following: [*[14]*].

Hierarchical to: No other components.

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

Application Note 2: **According to [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 [*zeroizing*] that meets the following: [*no standard*].

Hierarchical to: No other components.

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

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

FCS_COP.1.1/Con_Sym The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES_GCM*] and cryptographic key sizes [*256bit*] that meet the following: [*[14]*].

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 (see also chapter 6.1.7.1 for the definition of the trusted channel itself).

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

FCS_COP.1.1/SIG The TSF shall perform [*signature generation/verification*] in accordance with a specified cryptographic algorithm [*RSASSA-PSS (PKCS#1) and ECDSA*] and cryptographic key sizes [[*2048bit for RSA and 256 bit and 384 bit for EDCSA*] that meet the following: [*[14]*].

Hierarchical to: No other components.

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

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

6.1.1.6 FCS_COP.1/Management Cryptographic operation for remote management

FCS_COP.1.1/Management **This SFR is not implemented in the TOE. See Application Note 5.**
The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-GCM*] and cryptographic key sizes [*128bit and 256bit*] that meet the following: [[14]].

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: **According to [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 (1) Cryptographic operation for firmware signature verification

FCS_COP.1.1/SIG_FW (1) The TSF shall perform [*signature verification for **eHealth** firmware updates*] in accordance with a specified cryptographic algorithm [*ECDSA with NIST curves secp384r1*] and cryptographic key sizes [*384bit*] that meet the following: [[14]] and [**13**].

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 cryptographic functionality complies with the requirements described in [17][7].

6.1.1.8 FCS_COP.1/SIG_FW (2) Cryptographic operation for firmware signature verification

FCS_COP.1.1/SIG_FW (2) The TSF shall perform [*signature verification for **Secure Processor** firmware updates*] in accordance with a specified cryptographic algorithm [ECDSA with NIST curves secp384r1] and cryptographic key sizes [*384bit*]] that meet the following: [13].

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

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

FCS_COP.1.1/SIG_TSP The TSF shall perform [*signature verification*] in accordance with a specified cryptographic algorithm [*ECDSA with NIST curves secp384r1, secp256r1, secp224r1]* and cryptographic key sizes [*256bit*] that meet the following: [[14]].

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

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

Application Note 7: The TSP CA list updates are provided via the firmware update mechanism, therefor this SFR is considered to 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 list, shared secret, management credentials, firmware, cryptographic keys, Communication data [*and no other objects*]

Operations: Read, modify, [*and no other operations*]].

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[9] [*no other objects*]].

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 (1) 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 readonly area of the device and shall only 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 warns the administrator before the installation that he is*

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

[9] i.e. its configuration status

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 installs the new firmware list at first. The new list is used to decide whether an update to the accompanying firmware core is allowed.*
- ○ *Updates of the firmware list are only allowed to newer versions. Use higher version numbers to distinguish newer versions.*
- ○ *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 (1).*

If a TSP CA list update is initiated, a modification of the list shall only allowed after the integrity and authenticity of the new TSP CA list has been verified according to FCS_COP.1/SIG_TSP.

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

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

- [*<u>none</u>*]

[*no other rules*]

].

FDP_ACF.1.3/Terminal The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4/Terminal

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

- *No subject shall access any object but the TOE administrator's local management credentials before the TOE administrator's credentials are initially set.*
- *No subject shall read out the PIN, shared secret, management credentials or secret cryptographic keys while they are temporarily stored in the TOE*
- *No subject shall modify the public key for the signature verification of firmware updates unless a new public key is part of a firmware update.*

].

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

Application Note 8: No additional Access Control Policies are required.
No unauthorized reset to factory defaults is implemented.

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

FDP_ACF.1.1/Management

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

Subjects: users, [*none*]

Subject attributes: role(s), ***local and SICCT*** *management interfaces, [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 for SICCT interface.*
- *View card terminal name for card terminal*
- [*View the available network configuration*]
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [*none*]
- [*no further management functions*]

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

- [*Manage the available network configuration*]
- [*None*]
- [*None*]
- *Manage local* ~~***and remote***~~ *login credentials*
- *Secure deletion of pairing information from all three possible pairing processes (initial pairing, review of pairing-information and maintenance-pairing)*
- *Manage the list of TSP CAs*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*
- [*None*]
- [*no further management functions*]

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

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

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

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

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

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

[*no further rules*].

FDP_ACF.1.3/Management The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4/Management The TSF shall explicitly deny access of subjects to objects based on the following additional rules [*no additional rules*]

Hierarchical to: No other components.

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

Application Note 9: FDP_ACF.1/Management was used to define the access control for management functionality of the TOE. It applies to all local or SICCT interfaces, which are capable of management functionality[10].

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

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

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

Subjects: user, card, connector, remote card terminal[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] *,* [*no other attributes*]].

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

PINs shall never be stored in the non-volatile memory of the TOE. The PIN entered by the user shall only be sent via the secure channel targeting the card in the card slot of the TOE or a remote card terminal for remote-PIN verification.

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

].

FDP_IFF.1.3/PIN The TSF shall enforce the [*PIN digits shall never be displayed on the display during entry of the PIN. The TOE rather shall 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 the 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

[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

Application Note 10: For information about the specific realization of the display for the TOE see Chapter 1.3 "TOE Overview[13].

For remote-PIN verification the TOE may send the PIN to another card terminal via the connector. The PIN is then encrypted and transferred using card-to-card authentication of the smart cards in both card terminals.

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

Communication between TOE and connector is additionally secured using FCS_COP.1/Con_Sym.

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

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

Subjects: Connector, the TOE,

Information: all information arriving at the network interface Operation: accept the communication].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

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

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

Subject: Connector

Information: Passwords, patient data, shared secret, any other information

Information attribute: sent via the trusted channel, [*no other attributes*]].

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

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

Any information arriving at the network interface from the connector must only be accepted if the communication path is encrypted and the connector has been successfully authenticated[14]

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

].

FDP_IFF.1.3/NET The TSF shall enforce [*no additional rules*].

FDP_IFF.1.4/NET The TSF shall explicitly authorise an information flow based on the following rules: [

The TOE should accept the following SICCT commands arriving at the network interface even if no pairing process is established and no valid connector certificate is presented:

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

The TOE shall additionally accept the following EHEALTH commands (please refer to [14]) arriving at the network interface if no pairing process is established but a valid connector certificate[15] is presented:

- *EHEALTH TERMINAL AUTHENTICATE*

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

].

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

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

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

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

].

Hierarchical to: No other components.

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

Application Note 11: Please note that the information flow policy defined in FDP_IFC.1/NET and FDP_IFF.1/NET is focused on the communications, which fall into the scope of the application for the electronic health card and which happen between the connector and the TOE.

Connections for administration of the TOE may not be initiated by a connector. Therefore such a connection may not be covered by this policy.

Further, according to [14] the terminal is free to accept unencrypted communications for other applications, which may be additionally realized by the terminal (or during the migration phase). In these cases the terminal indicates to the user that it is working in an insecure state.

Please note that as a limitation to [15] the control byte for the bits b2..b1 of the Command-To-Perform Data Object CMD DO does not contain other values than {b 2 = 1, b1 = 0} or {b 2 = 1, b1 = 1}.

6.1.2.9 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*PIN, cryptographic keys, all information that is received by a card in a slot of the TOE or by the connector (except the shared secret),* [*no other objects*]].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 12: The functionality, defined in FPD_RIP.1 defines that the TOE is not allowed to save any information that was received by the connector or a card in a slot of the TOE permanently. This is necessary as the TOE relies on a controlled environment (A.ENV) to provide an adequate level of protection for the assets. If a TOE was e.g. stolen an attacker must not be able to read any of the information that was received from the connector or a card in a slot of the TOE.

Only information that is absolutely indispensable for the operation of the TOE (e.g. a secret that may be used for an initial review or the review of pairing information as part of the authentication with the connector) may be stored permanently within the TOE.

The TOE performs Batch Signatures using the functionality of the authorized card. The PIN is not stored temporarily to trigger single signature processes using the stored PIN. The PIN is sent to the card once only and is made unavailable immediately after the batch signing process is initiated.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [[*at least 3*]] unsuccessful authentication attempts occur related to [*management authentication excluding authentication for the TOE Reset Administrator*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met, surpassed], the TSF shall [*lock the particular management interface for that account for a time period according to Table 10 depending on the number of consecutive unsuccessful authentication attempts*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

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

Table 10: Lockout times

6.1.3.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Role*[16], [*no other attributes*]].

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 14: No further user attributes are needed for any policy of a TOE, therefor "no other attributes" is used as assignment in FIA_ATD.1.1

6.1.3.3 FIA_SOS.1 Verification of secrets

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

[

Passwords for management shall:

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

].

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

6.1.3.4 FIA_UAU.1 Timing of authentication for management

FIA_UAU.1.1 The TSF shall allow [

- *Display the product version number of the TOE*
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [none]
- [*no other actions*]

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

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

6.1.3.5 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

- *A password based authentication mechanism,*
- *A remote authentication mechanism using the SICCT interface*
- *An authentication mechanism for the TOE Reset Administrator*
- [*no additional authentication mechanism*]] *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*
- [*no additional rules*]

]

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 16:

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

The authentication mechanism for the TOE Reset Administrator requires authentication with a PUK. The Administrator must have physical access to the terminal to do this. There are no additional reset mechanisms in case of the loss of both the PUK and the Administrator PIN.

6.1.3.6 FIA_UAU.7 Protected authentication feedback

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

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

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

6.1.3.7 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [

- *Display the product version number of the TOE*
- *View card terminal name for card terminal*
- [*Display the MAC-address(es) of the TOEs network interface(s)*]
- [*none*]
- [*no other TSF mediated actions*]

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

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

Hierarchical to: No other components

Dependencies: No dependencies.

Application Note 18: The assignments in FIA_UAU.1.1/Management and FIA_UID.1.1/Management are performed in a way that none of the TSP of the TOE is violated.

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*[17]] to [*authenticated TOE administrators (excluding SICCT interface)*[18]].

Hierarchical to: No other components.

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

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

FMT_MSA.1.1/Management The TSF shall enforce the [*Management SFP*] to restrict the ability to [query, modify, delete, [*no other operations*]] the security attributes [*manageable objects, i.e. all management functions*] to [*TOE administrators*].

Hierarchical to: No other components.

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

6.1.4.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [*role(s)*[19]].

Hierarchical to: No other components.

[17] i.e its configuration status

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

[19] Role(s) as defined in 6.1.4.7

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

6.1.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management Functions **for Local and SICCT management interfaces**: [

- *Manage local ~~and remote~~ login credentials*[20]
- *Perform the pairing process (initial pairing, review of pairinginformation and maintenance-pairing) with the connector*

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

- *Secure deletion of pairing information from all three possible pairing processes*
- *Manage the list of TSP CAs*[22]
- *View/set card terminal name*[21] *for card terminal*
- *Perform a firmware update*
- *Reset the TOE settings to factory defaults*[22]
- *Reset the TOE settings to factory defaults (fallback)*[23]
- *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***~~
- [*none*]
- [*none*]
- [*none*]
- [*none*]
- *[Display the MAC-address(es) of the TOEs network interface(s)*][24]

[*no other relevant management functions*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 20: FDP_ACF.1/Management and FDP_ACC.1/Management further define which management functions are executable for the various user roles. Please note, that relevant data like failure counters for management interfaces and the shared secret are not reset when the firmware is updated.
As the reset to factory defaults (fallback) is only possible for authenticated TOE Reset administrators (see FDP_ACF.1/Management), if the administrator's management credentials are lost then a reset PUK is required to perform the reset (see 7.5 Security Management (FMT)).
Note that remote update functionality for firmware update may only be implemented as a PUSH service described in [13]. This requires an update component located in the local network of the medical supplier which is under the control of the TOE administrator (see

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

[22] 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.

[23] The fallback solution for reset of TOE settings is necessary in case the credentials for management are lost. [26] In case this functionality is implemented it must be disabled by default. Please also refer to Application Note 8 for further information

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

OE.PUSH_SERVER). The administrator approves and releases the firmware update that should be pushed by the update component. The update component logs card terminal identifier, the time of update, the version of the firmware to install, and the result of the update for each single update process.
The TOE administrators are able to Enable/Disable the functionality of an unauthorized reset to factory defaults in case this functionality is implemented by the TOE.
Further only authenticated TOE administrators are able to choose, which reset to factory defaults mechanism (reset the TOE settings to factory defaults or unauthorized reset to factory defaults) to perform when performing a reset.
Those SFRs refer to all Management interfaces and have to be refined accordingly. Those include mandatory local and SICCT as well as the optional remote management interface.

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* [*no other roles*]].

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*[25]*, failure during firmware update,* [*other types of failures in the TSF: failure of integrity and authenticity tests at start up and on performance of a self-test*]].

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

6.1.5.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 22: This SFR is fulfilled as the TOE does not comprise physically separated parts.

6.1.5.3 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [*physical tampering scenarios*] to [*all internal components including PCBs, touch screen controller & ID- 1 card readers*] by responding automatically such that the SFRs are always enforced.

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 23: *FPT_PHP.1 has been replaced by FPT_PHP.3 to require an active protection mechanism against physical manipulation*. The requirement of sealing of the cage of the TOE is obsolete as active detection of attacks and resistance towards attacks is implemented in such a way that the sealing of the cage of the TOE is not necessary.

6.1.5.4 FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self-tests [during initial start-up, at the conditions [*every 24 hours and on demand*]] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*]].

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

Hierarchical to: No other components.

Dependencies: No dependencies

Application Note 24: Please note that [14] does not define any concrete requirements for the minimum functionality that has to be covered by the self-test of the TOE. Test functionality were described for all important aspects of all Security Functions that the TOE provides.

6.1.6 TOE Access (FTA)

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

In operating modes outside of the secure state, banners and pop ups are displayed warning users not to enter their PIN.
In the Payment mode, if a payment transaction is implemented, the user will be prompted to enter a payment card. If a valid payment card is inserted then a PIN entry screen will be displayed with banners informing users that it is safe to enter their PIN. If an invalid (or eHealth card) PIN is entered then the transaction is aborted and PIN data immediately deleted. This screen and banners will not be displayed here if an eHealth card is inserted.

6.1.7 Trusted path/channels (FTP)

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

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

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

trusted channel.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 27: The SFR covers the authentication of the connector by the TOE using the connector certificate of an already paired connector. The TOE also verifies that the connector certificate is trusted by the TSP CA using signature verification of FCS_COP.1/SIG.
The trusted channel will only be active when the TOE is in "secure state". Otherwise it will be dropped.

There is only one connection to one connector at a time.

The TOE authenticates itself with the shared secret and the certificate of the SM-KT. If the SM-KT is unplugged then the service is stopped ensuring that no security threat arises.

6.1.7.2 FTP_TRP.1/Management Trusted path for remote management

These SFRs are not implemented in the TOE. See Application Note 28.

FTP_TRP.1.1/Management The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification or disclosure, [*no other types of integrity or confidentiality violation*]].

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

FTP_TRP.1.3/Management The TSF shall require the use of the trusted path for [[*authentication of TOE administrators, remote management*]].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 28: **According to [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 ST:

Assurance Class	**Assurance Components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security Measures
	ALC_LCD.1 Developer defined life-cycle Model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing

	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.4** 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					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 (1)				X			
FCS_COP.1/SIG_FW (2)				X			
FCS_COP.1/SIG_TSP				X			
FDP_ACC.1/Terminal	X	X		X			
FDP_ACC.1/Management				X			
FDP_ACF.1/Terminal	X	X		X			
FDP_ACF.1/Management				X			
FDP_IFC.1/PIN		X					
FDP_IFF.1/PIN		X					

FDP_IFC.1/NET					X		
	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION
FDP_IFF.1/NET					X		
FDP_RIP.1							X
FIA_AFL.1			X				
FIA_ATD.1			X				
FIA_SOS.1				X			
FIA_UAU.1			X				
FIA_UAU.5			X				
FIA_UAU.7		X					
FIA_UID.1			X				
FMT_MSA.1/Terminal	X			X			
FMT_MSA.1/Management				X			
FMT_MSA.2				X	X		
FMT_MSA.3/Terminal	X			X			
FMT_MSA.3/Management				X			
FMT_SMF.1				X			
FMT_SMR.1			X				
FPT_TST.1							X
FPT_FLS.1							X
FPT_ITT.1							X
FPT_PHP.3							X
FTA_TAB.1/SEC_STATE						X	
FTP_ITC.1/Connector					X		
FTP_TRP.1/Management				X			

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

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

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

The Security Objective **O.I&A** is met by a combination of FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1 and FMT_SMR.1. FIA_AFL.1 requires that the password policy is enforced. FIA_UID.1 and FIA_UAU.1 require each user to be authenticated and identified before allowing any relevant actions on behalf of that user. Further the objective requires that the TOE will at least maintain the roles, TOE administrator and TOE Reset Administrator. This is defined in FMT_SMR.1, which defines the roles and FIA_ATD.1, which defines the user attribute for the role. FIA_UAU.5 defines all the authentication mechanism that is implemented by the TOE, in particular for local management.

The Security Objective **O.MANAGEMENT** is met by a combination of FCS_CKM.1/Management, FCS_CKM.4, FCS_COP.1/Management, FCS_COP.1/SIG_FW (1), FCS_COP.1/SIG_FW (2), 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[26]. FCS_CKM.4 requires that keys are adequately destroyed. FCS_COP.1/Management requires that remote management shall enforce TLS[27]. FCS_COP.1/SIG_FW (1) and FCS_COP.1/SIG_FW (2) are used to define the mechanism to check the authenticity of a firmware update. FCS_COP.1/SIG_TSP is used to define the mechanism to check the authenticity of a TSP CA list update. The access control policy defined in FDP_ACC.1/Terminal and FDP_ACF.1/Terminal define the rules under which a firmware update is possible. FDP_ACC.1/Management and FDP_ACF.1/Management define the access control policy that determines under what circumstance a particular management function is accessible and by whom. FIA_SOS.1 defines the password policy for management credentials. FMT_MSA.1/Terminal and FMT_MSA.1/Management define, which roles are allowed to administer the attributes of the access control and the information flow control policies. FMT_MSA.2 requires that only secure values are accepted for security attributes. FMT_MSA.3/Terminal defines that the terminal has to provide restrictive default values for the terminal access control policy attributes. FMT_MSA.3/Management defines that the terminal has to provide restrictive default values for the management access control policy attributes. FMT_SMF.1 describes the minimum set of management functionality, which has to be available according to the Security Objective. Finally, FTP_TRP.1/Management defines the trusted path between the TOE and the management client.

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

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

The Security Objective **O.PROTECTION** is met by a combination of the SFR FCS_CKM.4, FDP_RIP.1, FPT_ITT.1, FPT_PHP.3, FPT_FLS.1 and FPT_TST.1.

[26] Remote Management is optional and not implemented in the TOE. This SFR is therefore not implemented. See FCS_CKM.1/Management for more detail.

[27] Remote Management is optional and not implemented in the TOE. This SFR is therefore not implemented. See FCS_COP.1/Management for more detail.

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.3 builds the physical protection for the stored assets. FPT_TST.1 defines the necessary test functionality for the underlying abstract machine. FPT_FLS.1 defines a list of failures in the TSF for which the TOE has to preserve a secure state. Finally FPT_TST.1 defines that the TSF have to run a suite of self-tests to demonstrate the correct operation of the TSF at start-up and during the normal operation of the TOE.

6.3.2. 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
FCS_COP.1/SIG_FW (1)	[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_FW (2)	[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

SFR	Dependencies	Support of the Dependencies
FDP_IFC.1/PIN	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/PIN
FDP_IFF.1/PIN	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/PIN See chapter 6.3.2.1 for FMT_MSA.3
FDP_IFC.1/NET	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1/NET
FDP_IFF.1/NET	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1/NET See chapter 6.3.2.1 for FMT_MSA.3
FDP_RIP.1	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	Fulfilled by FIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UAU.5	No dependencies	-
FIA_UAU.7	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1
FIA_UID.1	No dependencies	-
FMT_MSA.1/Terminal	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FDP_ACC.1/Terminal, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1/Management	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FDP_ACC.1/Management, FMT_SMR.1 and FMT_SMF.1

SFR	Dependencies	Support of the Dependencies
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 FIA_UID.1
FPT_TST.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_ITT.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FTA_TAB.1/SEC_STATE	No dependencies	-
FTP_ITC.1/Connector	No dependencies	-
FTP_TRP.1/Management	No dependencies	-

Table 13: Dependencies of the SFR for the TOE

6.3.2.1 Justification for missing dependencies

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

The ST author has not extended these information flow policies in a way that they require security attributes.

The dependencies FDP_ITC.1 and FCS_CKM.4 of FCS_COP.1/SIG_FW (1) 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, in the context of this ST FCS_COP.1/SIG_FW (1) and FCS_COP.1/SIG_TSP are used for a requirement on signature verification for which no secret key is necessary. The key for signature verification is part of the TOE and is not imported. Therefor these dependencies do not need to be considered.

6.3.3. Security Assurance Requirements Rationale

The Evaluation Assurance Level for this Security Target is EAL 3 augmented by 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)

6.3.4. Security Requirements – Mutual Support and Internal Consistency

The core TOE functionality in this ST 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 ST 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.3, FPT_TST.1). By this way the SFRs in this ST 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.

6.4. Extended Functionality

The card terminal provides additional functionality in value-added modules. These modules are included in a separate firmware to that used for TOE functionality.

Value added modules are logically separated and guarantee that the TOE has exclusive access to terminal functionality when in use.

Logical value-added modules include:

- Payment Application

7. TOE Summary Specification

7.1. Overview

The TOE is part of an Electronic Health Card Terminal (The terminal") based on the regulations for the German healthcare system. It is a smart card terminal with secure PIN entry functionality and fulfils the requirements for the use within the German telematic infrastructure (See 1.3 TOE Overview).

The TOE for use in the German health care is based on the specification SICCT, which is adapted for operation by profiling as eHealth card terminal (see [15]).

Terminal secure functions are managed by the OS and eHealth application running on the NXP/Freescale MK81FN256VDC15 (K81) security processor.

When the eHealth application is active, it has control of all terminal functions.

Access to services and TSFIs is through APIs provided by the secure processor firmware.

Non-security-based components including the iMX6 processor are physically separate from secure components. VAM (Value added modules) such as secure payment are also logically and physically separated from the eHealth functionality.

The eHealth application has sole control over the display when running. This is enabled by the secure processor using the SFPGA processor and ensures that only prompts from the eHealth application can be displayed.

The TOE supports PIN on glass. This means that a virtual PIN pad is displayed, controlled by the secure processor. The location of the PIN pad is randomised on the display.

7.2. Cryptographic Support

TLS 1.2 is used to authenticate the connection between TOE and all external systems (Connector, Terminal Management System ("TMS"), Factory Key Loading (HSM)). The following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

For the EC cipher suites, the following curves are supported:

- P-256
- P-384

For key generation, DHE Group 14 is used.

Cryptographic functionality complies with PKCS#1.

For signature verification for the connection between the TOE and the Connector, the TOE stores a list of trusted CAs (TSP CA List). This list can be managed by the TOE administrator.

Firmware, Key and Configuration updates are encrypted using AES-GCM 256.

The SM-KT (Secure Module Kartenterminal) is used for the following functions:
- Key generation and protection
- Cryptographic functions based on RSA and ECSA for encryption/decryption and signature creation.
- Random number generation
- A function to read out the public key

For SM-KT with RSA-based identity, the following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

For SM-KT with ECDSA-based identity, the following cipher suites are supported:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C)

Zeroisation is used to destroy keys.

A logically distinct communication path is used to connect the TOE to the TMS. The connection has sole use of its TLS interface.
Firmware is encrypted by AES256 GCM.

The Cryptographic Support functions are designed to satisfy the following security functional requirements:
FCS_CKM.1/Connector Cryptographic key generation for connector communication
FCS_COP.1/Con_Sym Cryptographic operation for connector communication (symmetric algorithm)
FCS_CKM.4 Cryptographic key destruction for communication
FCS_COP.1/SIG Cryptographic operation for signature generation/verification
FCS_COP.1/SIG_FW (1) Cryptographic operation for firmware signature verification
FCS_COP.1/SIG_FW (2) Cryptographic operation for firmware signature verification
FCS_COP.1/SIG_TSP Cryptographic operation for verification of TSP CA lists

7.3. User data protection (FDP)

Administrative access to the TOE is controlled by roles for Direct Access. Roles are Administrator, Reset Administrator & User. Access is password controlled with a numeric password that must be a minimum of 8 characters in length and may be up to 12 characters.

Using the Direct Management module, the administrator can perform the initial pairing process with the connector.

Access to firmware, cryptographic key and CA list management is controlled through the Direct Management module. The Administrator Role is required. The TOE informs the administrator that an update is available and provides the version number. This enables the Administrator to verify the version number and trigger the secure update process on terminals for firmware and keys. This does not allow them any access to secure data.

The TOE checks the authenticity and integrity of all updates. If a firmware, key or CA list update fails then the update is discarded and the previous state restored.

There is no read access to PIN, shared secret, management credentials or secret cryptographic keys via any of the Management Roles including password and keys.

There is no unauthorized reset to factory defaults implemented by the TOE.

On first start-up and after reset to factory settings the TOE forces the administrator to specify a password for direct management.

The TOE also ensures that the TOE administrator’s credentials for local management are set before access to other TOE functionality is possible.

The PIN is stored in the non-volatile memory of the secure processor and never leaves the TOE in clear text except to smart cards in local card slots. The Memory Protection Unit access control permission ensures that no other applications including the payment application can access the PIN.

The PIN digits are never displayed and are replaced by asterisks.

When the application processor is using the display, blue banners are displayed indicating that it is not safe to enter PIN. When the eHealth application is running and PIN entry is requested, green banners are displayed indicating that it is safe to enter PIN.

Connections for the flow of information between the Connector and the TOE as well as TMS and the TOE are controlled through TLS 1.2.

Exceptionally, the TOE accepts the following SICCT commands at the network interface even if the pairing process has not been established and no valid connector certificate is presented:

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

All sensitive data (keys, PIN) received from cards or the connector are deleted immediately after use.

The User data protection (FDP) functions are designed to satisfy the following security functional requirements:

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

7.4. Identification and Authentication (FIA)

Administrator access to the Direct Management module is controlled by an error counter of incorrect password entries. The TOE blocks Administrator access from the third consecutive invalid password entry. This functionality is an authentication mechanism provided by the eHealth application subsystem.

User access is defined by role: User, Administrator, Reset Administrator.

Passwords are numeric with a length of at least 8 characters.

The following can be displayed to non-authenticated users:

- Product version number
- Card Terminal Name
- MAC address of the network interface

There are separate authentication mechanisms for the Direct Management and SICCT modules. Each have their own error counter. PIN is displayed by asterisks only. SICCT module access requires TLS mutual authentication.

The Administrator can reset or change a password.

The Identification and Authentication (FIA) functions are designed to satisfy the following security functional requirements:

FIA_AFL.1 Authentication failure handling
FIA_ATD.1 User attribute definition
FIA_SOS.1 Verification of secrets
FIA_UAU.1 Timing of authentication for management
FIA_UAU.5 Multiple authentication mechanisms
FIA_UAU.7 Protected authentication feedback
FIA_UID.1 Timing of identification

7.5. Security Management (FMT)

Factory reset and the management of security attributes can only be handled by authorised administrators via the Direct Management module.

The Direct & User Management modules have three roles – User, Administrator & Reset Administrator.
The Administrator role may perform the following management functions:

- Manage Management login credentials including the credentials of the Reset Administrator.
- Perform the pairing process (initial pairing, review of pairing information and maintenance-pairing) with the connector.
- Secure deletion of pairing information from all three possible pairing processes.
- Perform firmware and key & TSP CA List update.
- Manage the list of TSP CAs – the Administrator can view the details of each certificate. Direct changes to the TSP CA List are not permitted and will only be possible via Firmware update.

Unauthenticated users may perform the following management functions:

- View card terminal name.
- Display the product version number of the TOE.

The Reset Administrator role may perform the following management functions:
These roles may perform the following management functions:

- Manage their own login credentials.
- Reset the TOE settings to factory defaults.
  The factory reset is done using the Reset Administrator's password (PIN). If the PIN is lost, it is possible to reset using a reset PUK. If the PUK is also lost then it is not possible to perform a factory reset anymore and the terminal will need to be replaced.

The Security Management (FMT) functions are designed to satisfy the following security functional requirements:

FMT_MSA.1/Terminal Management of security attributes for Terminal SFP[28]
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

[28] FMT_MSA.1.1/Terminal is trivially fulfilled by the TOE, as no functionality of an unauthorized reset to factory defaults is implemented by the TOE.

7.6. Protection of the TSF (FPT)

If a firmware, key, TSP CA List or configuration update fails then the update is discarded and the previous state restored.

All parts of the TOE lie within the same device and do not comprise physically separated parts.

The TSF uses active detection to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. For this purpose, opening switches, pogo pins and wire mesh layers are used. Drilling through the casing, opening the casing and removing the display will all trigger a tamper event. All card readers are also covered by wire mesh and is enclosed in the physical security zone.

In the event of physical or logical tampering, the TOE is set into tamper mode. This renders the terminal inoperable and is immediately made evident to the user on the secure display. Tampered terminals are returned to the manufacturing facility where they are taken out of service and the security processor destroyed.

In Tamper Mode the following steps take place:

- The Secure FPGA is instructed by the Self Protection Module to takeover the Display indicating that the device is in lock-down.
- The Secure FPGA is instructed by the Self Protection Module to disable touch events, preventing user interaction.
- The terminal performs a reset. The contents of the RAM are deleted – this included TLS session keys and shared secrets between the Terminal and Connector.
- The Secure Boot Module to update the execution life-cycle of the secure firmware to End-Of-Life.
- The KEK_MK master key is deleted preventing the use of any other keys.

The TSF runs a suite of self-tests during initial start-up, every 24 hours and on user request. The integrity of the Firmware is checked and if it does not pass then the TOE will go into Tamper mode and become inoperable.

The Protection of the TSF (FPT) functions are designed to satisfy the following security functional requirements:

FPT_FLS.1 Failure with preservation of secure state

FPT_ITT.1 Basic internal TSF data transfer protection
FPT_PHP.3 Resistance to physical attack
FPT_TST.1 TSF testing

7.7. TOE Access (FTA)

The secure state of the TOE is indicated by the use of banners on the display.

When the eHealth mode is active, the device is in a trusted state for eHealth functions including secure PIN entry. This is indicated by a banner that displays “eGK Anwendung aktiv.”

When a card entry request has been made and a valid eHealth card has been inserted, the PIN entry screen has a banner which displays “Jetzt ist es sicher ihre eGK PIN einzugeben”

When not in a secure state, blue banners and pop ups display the message “Do not enter your bank/eHealth PIN”.

The TOE Access (FTA) functions are designed to satisfy the following security functional requirements:
FTA_TAB.1/SEC_STATE Default TOE access banners for secure state

7.8. Trusted path/channels (FTP)

The TOE follows the specification detailed in **PP-0032-V3-2023, Version 3.8, 15.12.2022** for the authentication of the connector by the TOE. This includes certificate / signature verification and TLS authentication.

The TOE establishes a Trusted Channel from the secure processor to the connector. The SICCT protocol over TLS 1.2 with mutual authentication is used to secure the channel.

A logically distinct communication path is used to connect the TOE to the TMS for update management. The connection has sole use of its TLS interface.

The Trusted path/channels (FTP) functions are designed to satisfy the following security functional requirements:
FTP_ITC.1/Connector Inter-TSF trusted channel for connector communication

8. Bibliography

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5,April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

[5] AIS 27, Version 5, Transition from ITSEC to CC, Certification body of the BSI in the context of the certification scheme, August, 17th 2010

Cryptography

[6] BSI TR-03116-1, Technische Richtlinie TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20

[7] BSI TR-03120, Technische Richtlinie „Sichere Kartenterminalidentität (incl. Kartenterminalschutz)“, Version 1.1

[8] BSI TR-03120 Appendix, „Anhang: Kartenterminalschutz“ zur Technischen Richtlinie BSI TR-03120, Version 1.1

[9] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21.12.2016

[10] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

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

[12] Common Criteria Protection Profile - Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[13] BSI-TR-03111_V-2-1, Elliptic Curve Cryptography, Version 2.10, 01.06.2018

Specifications

[14] gematik: Spezifikation eHealth-Kartenterminal, Version 3.16.0, Stand 07.07.23

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

[16] gematik: Spezifikation der gSMC-KT – Objektsystem, Version 3.9.0, Stand 24.08.2016 (for card generation G2) and gematik: Spezifikation der gSMC-KT – Objektsystem, Version 4.3.0, Stand 12.05.2022 (for card generation G2.1)

[17] gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.28.0, Stand 09.06.2023