KoCoBox MED+ Netzkonnektor
Common Criteria Certification

Security Target

Autor: KoCo Konnektor GmbH

Version: 1.8.5
Datum: 18.10.2017

Abstract

This document contains the Security Target for the Common Criteria Evaluation of KoCoBox MED+ Netzkonnektor.

Schlagwort

CC, ST, Common Criteria

Inhaltsverzeichnis

1 ST Introduction

The target of evaluation (TOE) described in this security target is the KoCoBox MED+ Netzkonnektor. The TOE is part of a secure platform called KoCoBox MED+ which is used as an “e-Health Konnektor” in the context of the German health care telematics infrastructure.

The e-Health connector platform as a “Gesamtkonnektor” includes several other components that are not part of the TOE. Those are the greater part of the application connector (AK), the signature application component (SAK) and the cryptographic identities.

The cryptographic identities of the connector are set up by three smart-card-based secure modules for the connector (gSMC-Ks) which are put into the connector’s internal smart-card slots. Each gSMC-K is dedicated to either NK, AK, or SAK. The gSMC-Ks are Common-Criteria-certified in compliance with the protection profile BSI-CC-PP-0082-V2.

This document is the security target (ST) which describes the functional and assurance security requirements for the TOE and its operational environment.

A list of the referenced documents, the conventions for this ST and the used terminology and abbreviations can be found in section 8, the appendix.

1.1 ST Reference

Title of the Security Target:	Security Target for the KoCoBox MED+ Netzkonnektor
ST version:	1.8.5
Issue date:	18.10.2017
Status:	Final
Author:	KoCo Connector GmbH

1.2 TOE reference

Target of evaluation (TOE):	KoCoBox MED+ Netzkonnektor, Short: KoCoBox NK
TOE version:	1.3.4
Product Owner:	KoCo Connector GmbH
Assurance level:	EAL3 with augmentation of AVA_VAN.5, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 (hereafter called „EAL3+“)
Compliant with Common Criteria version:	3.1 Release 4

1.3 TOE Overview

The TOE is the network connector (German: “Netzkonnektor”) and a small part of the application connector (German “Anwendungskonnektor”) of the so-called “KoCoBox MED+” connector (German: “Konnektor”). As described in [BSI-CC-PP-0047, 1.2. PP-Übersicht], the network connector is only one part of the entire connector (German: “Gesamtkonnektor”).

The KoCoBox MED+ Netzkonnektor – short KoCoBox NK – is a secure platform used as “e-Health Konnektor” in the context of the German “Gesundheitstelematikinfrastruktur” (health care telematics infrastructure) as specified by the Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) [gemSpecKonnektor].

The network connector provides a secure environment for security-related services and a secure interconnection between the decentralized components and the central telematics infrastructure which is established over an IPSec-based VPN. The connector protects itself and the telematics infrastructure from attacks originating from workstations over the LAN and itself and the components in the LAN from attacks over the WAN. Furthermore, the network connector implements certain security sensitive (i.e. SFR-enforcing and SFR-supporting) functions and services that are invoked by connector components outside of the TOE.

The KoCoBox MED+ is designed as a single-component solution according to the terminology of the connector specification and includes the network connector, the application connector, and provides secure access to the internet via SIS. These components make use of smart-card based secure modules for the connector (gSMC-Ks) which are put into designated smart-card slots of the device. The gSMC-Ks include several cryptographic identities for identification and authentication towards various infrastructure components (e.g. VPN concentrator, eHealth card terminals, smart cards, extended trusted viewer) and encryption of assets.

The KoCoBox is especially designed for the use cases required by resident doctors and pharmacies—it is intended for an IT environment that is only lightly managed and where a systems administrator may not always be available to monitor its operation.

The connector is intended to be deployed in the so-called “zutrittsgeschützter Bereich” (access protected area) within the premises of a medical care provider. This implies the following security requirements for the environment:

- Identification of a breach: The environment has to identify the entry of an attacker and the manipulation of the device hardware.
- If the connector is booted up, the environment has to prevent access to the area by utilizing organizational (e.g. checking for indications of breaches in irregular intervals) and/or technical (e.g. alarm system) measures.
- Requirements according to “IT-Grundschutz” or “Richtlinien der BÄK”

The connector can be administered through a HTTPS-based web interface. This interface allows authenticated users to perform various management tasks, including secure firmware updates, modification of configuration parameters and querying diagnostic information.

The KoCoBox consists of a network connector (NK), an application connector (AK), and a custom design hardware platform. It is designed to work and be operated “out-of-the-box” without the need of any additional hardware, software, or firmware, after it has been configured via the HTTPS-based management interface. The gSMC-Ks are put into the device at the manufacturing site during the personalization process and, therefore, do not have to be added manually by the end-user.

The distinction between and functionality of the NK, AK, and gSMC-K is described in detail in [BSI-CC-PP-0047, 1.3.1].

The TOE is firmware-only. It requires the following non-TOE parts for its operation (see also chapter 1.4.3):

- The KoCoBox MED+ hardware
- Three built-in gSMC-Ks

1.4 TOE Description

The main purpose of the TOE is to provide a dynamic packet filter and VPN functionality to the other components. The TOE presented in this security target is part of a single-component solution; i.e. the TOE and the other connector components are embodied in a single device. Therefore, the device consists of hardware and software components. The casing of the KoCoBox MED+ hardware is depicted in Figure 1.

Figure 1: Casing of KoCoBox MED+ hardware (front and back)

However, the TOE is software only and constitutes a part of the device firmware. It uses the hardware platform as a run-time environment. The TOE provides functionality to other software components (e.g. network functionality) and utilizes functions of other trusted IT products (e.g. gSMC-K).

The TOE runs on an Arch Linux based embedded Linux system. Parts of the OS belong to the SFR-enforcing functionality of the TOE (TCP/IP stack, netfilter, IPsec). The TOE is implemented in C/C++, Java and shell scripts.

The TOE includes guidance documentation.

1.4.1 Overview

The connector is designed for use in the telematics infrastructure and for secure communication with the internet via a Secure Internet Service (SIS), as described in [BSI-CC-PP-0047, 1.3. EVG-Beschreibung].

1.4.2 Function Blocks

The different function blocks of the connector are described in [BSI-CC-PP-0047, 1.3.1, Abbildung 1].

The greater part of the application connector and the secure module for the connector (gSMC-K) are not part of this TOE.

The TOE mainly consists of the network connector but also contains the parts of the application connector that provide security functionality for:

- TLS channels for local and remote management interfaces,
- a certificate validation service (“Zertifikatsdienst”) for handling VPN certificates.

In addition, the boot loader, which starts the firmware during boot-up, is part of the TOE.

1.4.3 Environment

Operational Environment

The TOE depends on certain environment components for execution and maintaining a secure state. This set of components consists of runtime environment components, hardware, software, and other trusted IT-products.

The required components for the operational environment of the TOE are listed in Table 1.

Component	Description	Version
KoCoBox MED+ hardware	Hardware-based runtime environment for the TOE (see section 1.4.6).	2.0.0
KoCoBox non-TOE parts	The non-TOE parts of KoCoBox MED+. It provides the main services of the application connector to client systems, card services, card terminal services and management interfaces. The TOE communicates with the non-TOE parts via a set of Java interfaces (see LS.AK in chapter 1.4.5).	1.3.0

Component	Description	Version
3x STARCOS 3.6 Health SMCK R1	Trusted, certified smart-card-based (ID-000 card size) gSMC-Ks. CC-Certification-ID: BSI-DSZ-CC-0916-2015 [BSI-DSZ-CC-0916-2015] KoCoBox NK supports three gSMC-Ks to increase performance for cryptographic operations. However, only two are used in the current TOE. The gSMC-Ks are plugged into the TOE during production of the KoCoBox. Afterwards, the casing of the KoCoBox is sealed. To access the cryptographic objects of the network connector on the first gSMC-K (gSMC-K#1) the TOE uses a specific PIN (PIN.NK) which is not known by other parts of the connector. The AK parts of the TOE use the second gSMC-K (gSMC-K#2) with the PIN.AK which is only known to the AK-part of the TOE. The third gSMC-K (gSMC-K#3) is not relevant for the TOE.	certified against [BSI-CC-PP-0082]
Telematics infrastructure	German e-health telematics infrastructure provided by gematik accessible over the WAN interface (see sections 1.4.4 and 1.4.5).	according to gematik specification release OPB1
SIS	A dedicated VPN concentrator for SIS provides secure access to the internet accessible over the WAN interface.	according to gematik specification release OPB1

Table 1: Required operational environment

1.4.4 Physical Interface

All interfaces are physically located on the connector. The following list refers to [BSI-CC-PP-0047, 1.3.3.1. Physische Schnittstellen des TOE]. PS.DISPLAY has been added.

PS.Mehrbox (PS1 accoring to PP)
: is an interface to the application connector (AK). Since a single box solution is deployed, this physical interface does not exist here.

PS.LAN (PS2 according to PP)
: is an interface to the LAN and the client systems respectively. Although the

network connector does not communicate with the client systems by itself, it provides a physical interface to the LAN which is used by the application connector to communicate with infrastructure components in the LAN. This interface is also used for a remote administration (not part of the TOE). It is protected by the network connector's packet filter.

PS.WAN (PS3 according to PP)
: is an interface to the WAN. This interface's purpose is to supply connectivity for the VPN connections to the telematics infrastructure and to the SIS. This interface is protected by the network connector's packet filter.

PS.SMC (PS4 according to PP)
: is an interface to a certified secure module of the network connector (SM-NK) which is a part of the gSMC-K. For the KoCoBox tree smart-card based gSMC-Ks will be used. The first gSMC-K will be used by the NK-part of the TOE only. The second one will be used by the AK-part. The third will be used by the SAK which is not part of the TOE.

PS.DISPLAY
: represents the display and the buttons. The display is used to inform the administrator about critical states. The buttons allow the administrator to navigate through the menu, perform a reset and reset the IP address of the LAN to a default value.

Please note that the TOE is software-only, though according to the PP the physical interfaces to the connector should be identified.

1.4.5 Logical Interfaces of the TOE

The TOE possesses the logical interfaces described in [BSI-CC-PP-0047, 1.3.3.2. Logische Schnittstellen des TOE] which are listed in this ST for better readability.

LS.AK (LS1 according to PP)
: is a Java interface to the application connector. It is used to manage the TOE.

LS.JRE
: is the interface between the Java Virtual Machine (JVM) of the TOE and Java programs (TOE and non-TOE parts of the connector).

LS.LAN (LS2 according to PP)
: is an interface to the infrastructure components in the LAN (client systems and eHealth card terminals), which are accessible via the LAN interface PS.LAN.

LS.VPN_TI (LS3 according to PP)
: is an interface to the centralized telematics infrastructure. Communication to the infrastructure occurs over a VPN channel via the WAN interface PS.WAN (or via PS.LAN when WAN and LAN are not separated).

LS.VPN_SIS (LS4 according to PP)

is an interface to the SIS for secure internet access. Communication to the internet occurs over a VPN channel via the WAN interface PS.WAN (or via PS.LAN when WAN and LAN are not separated).

LS.WAN (LS5 according to PP)

is an interface to the unprotected transport network (via PS.WAN), which is used for the establishing of VPN channels when WAN and LAN are separated.

LS.SMC (LS6 according to PP)

represents the interface to the secure module of the connector (gSMC-Ks) via PS.SMC.

LS.DISPLAY

represents the logical interface to display and buttons via PS.DISPLAY.

1.4.6 Assembly and Physical Differentiation of the Network Connector

Covering the requirements in [BSI-CC-PP-0047, 1.3.3. Aufbau und physische Abgrenzung des Netzkonnektors], the assembly and physical differentiation are described as follows.

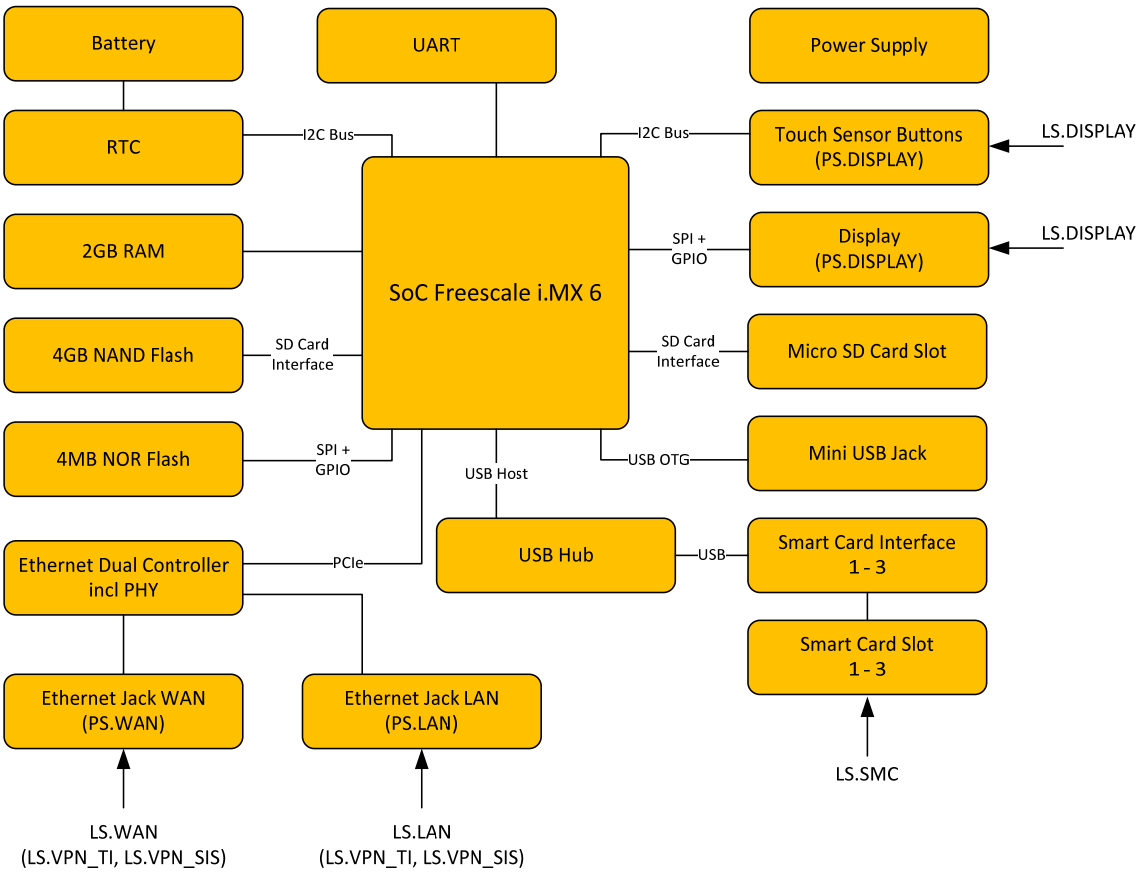


Figure 2: Hardware diagram of the KoCoBox

Figure 2 shows the hardware components belonging to the KoCoBox (the device) which serves as a run-time environment for the connector firmware and, thus, for the TOE and other software components. All parts of the compiled TOE are executed by the CPU on the SoC. No common-off-the-shelf hardware is used as part of the TOE.

The physical interfaces of the TOE are indicated in the diagram in the relevant outer components. The logical interfaces which are accessible from outside the KoCoBox hardware are indicated by arrows.

The Real-Time-Clock (RTC) is used by the TOE to provide reliable time stamps. It is powered by a battery to keep the time when there is no power supply.

The 2 GB RAM represents the volatile main memory. The persistent NAND-flash memory is located on a 4 GB embedded Multimedia Card (eMMC). The 4 MB NOR-Flash contains the boot loader.

The Ethernet dual controller separates between the two physical interfaces for LAN (PS.LAN) and WAN (PS.WAN) by providing a separate port per interface. Each of the ports provides their own MAC address. It maintains the Ethernet frames of its allocated interface jack and ensures that frames are not exchanged between the ports. Based on the port and MAC allocation, the TOE provides different interfaces for each port.

The buttons and the display are used to get status information from the connector and to reset the IP address on the LAN.

The gSMC-Ks have to be plugged into the three internal smart card slots which are connected to the smart card interfaces 1 through 3. The gSMC-K also provides a PRNG. The first gSMC-K is used by the NK parts of the TOE, the second is used by the AK part of the TOE and the third is used by the SAK (none-TOE part).

The mini-USB jack (USB On-the-Go (OTG)) is used to install the first firmware in factory. For this process the SoC pin for USB boot must be connected during reset. The SoC then acts as USB device accessible via the Mini-USB jack and the initial boot loader can be uploaded to the NOR-flash and started. The internal interface used for this process is not accessible in the operational phase of the connector since the pin can only be set with direct access to the circuit board. Even if USB boot was successful, the SoC would first verify the signature of the boot loader before starting it (High Assurance Boot (HAB)).

The Micro SD-Card Slot is intended for future use. It is not used in the certified TOE configuration. This interface is not accessible outside the casing.

The UART interface for attaching a serial console is unused and deactivated in software. Neither input nor output is possible.

1.4.7 Software Subsystems

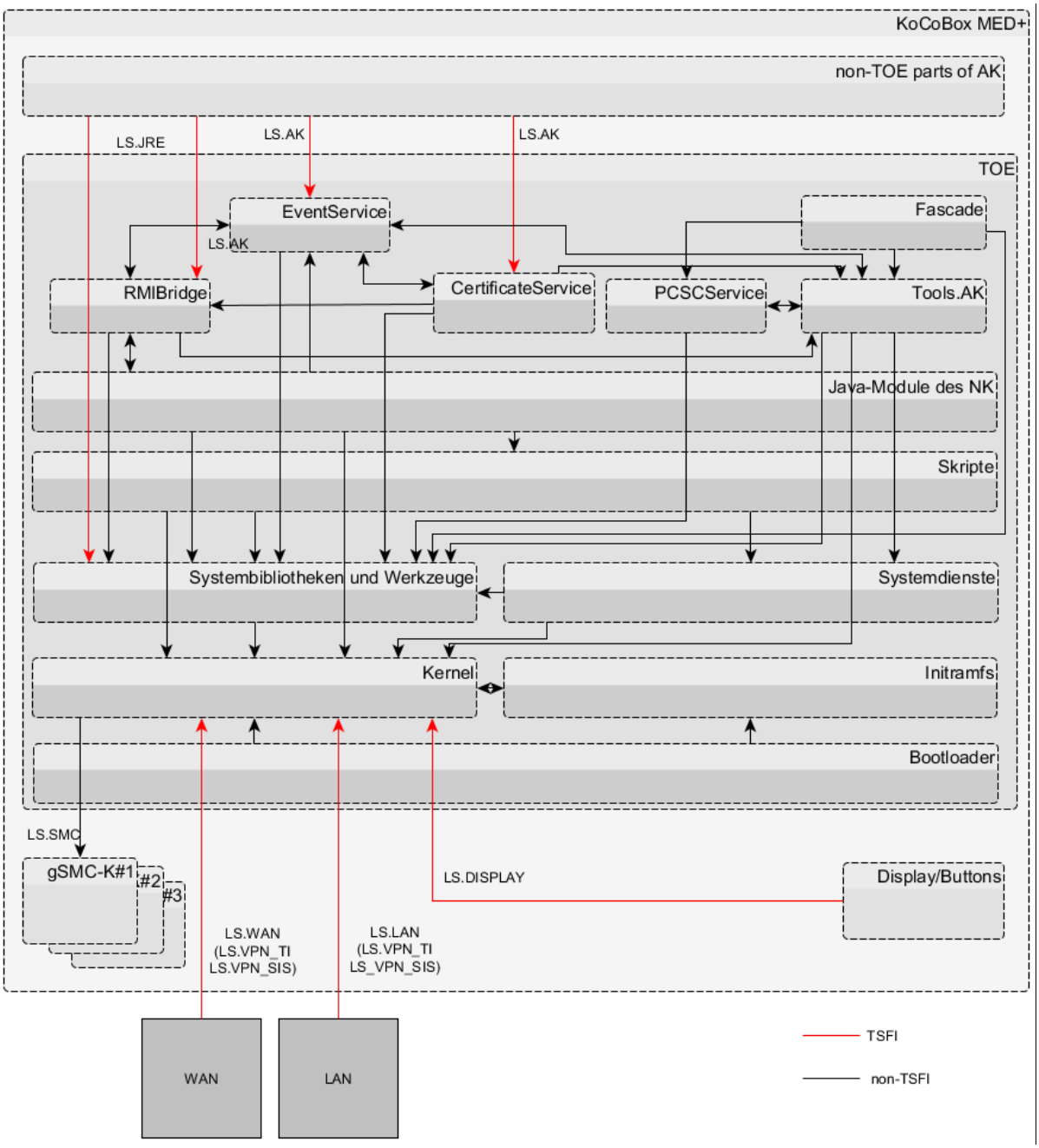


Figure 3: Network connector subsystems and external logical interfaces

The TOE is based on an Arch Linux packet system with a custom kernel adapted to the hardware and Java applications that are dedicated to the implementation of specific functionality. It consists of the following subsystems:

- Bootloader
  - Ensures the integrity of kernel and initramfs.
  - Boots the kernel.
- Kernel

  - The kernel provides basic access to hardware for user applications. It provides security functionality for packet filtering, IPsec channels and cryptographic algorithms.
- Initramfs
  - Contains the file system, tools and scripts to set up the root file system of the operating system.
- Systemdienste
  - System services (in form of daemons) provide services that are used by the rest of the TOE.
- Systembibliotheken und Werkzeuge
  - Provides user space libraries, programs and command line tools used by other subsystems. Programs in user space contribute specific functionality, such as encryption/decryption as well as the JRE for Java NK and all parts of the AK.
- Skripte
  - Provides various script files which are used to boot up and configure the TOE.
- Java-Module des NK
  - Provides Java part of the network connectors that configures the TOE and provides services to other parts of the connector.
- CertificateService
  - Provides an interface for the TOE to check validity of certificates.
- RMIBridge
  - rmibridge facilitates object function calls between Java Virtual Machines (JVMs).
- EventService
  - Acts as an internal event hub for modules and basic services.
- PCSCService
  - Provides access services to use internal smartcards (gSMC-K) by AK.
- Facade
  - Implements interfaces for subsystems and modules which represents the access point to the functionality of the services by using jetty web server.
- Tools.AK
  - Provides programs, tools and frameworks used by other subsystems. Main tools are the Java Runtime Environment (JRE), OSGi as a service and modularization platform and BouncyCastle for cryptographic operations.

All other parts of the KoCoBox are non-TOE parts. The non-TOE parts are Java programs only that run on the JRE of the TOE.

1.4.8 Logical scope: Security Services supplied by the TOE

The TOE fulfills all requirements to security services given in [BSI-CC-PP-0047, 1.3.4. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste]. The following list summarizes all these security services. Implementation-specific information, additions, and notes to the list or the descriptions given in the PP are recognizable as **boldface and underlined text.**

- VPN Client for connecting the application connector to the centralized telematics infrastructure and the SIS
  a) Enforcement of authentication of the VPN concentrators
     The network connector supports IKEv2 as described in [IKEv2].
  b) Protection of integrity and authenticity of transferred data
  c) Rule based information flow control
- Dynamic packet filter
  a) Rule based dynamic packet filter that is able to repel attacks that are executed with high attack potential.
- Network based services
  a) Provision of an NTP server for applications and client systems
  b) Time synchronization with an NTP server in the telematics infrastructure
  c) Provision of a DHCP service for the LAN interface according to [RFC2131] and [RFC2132]
  d) Provision of a DNS service extended by DNSSEC according to [RFC4035] for the LAN interface
  e) Validity check for certificates
- Stateful packet inspection
- Self-protection
  a) Memory treatment
     The TOE clears the memory holding assets (including cryptographic keys) which are no longer needed by overwriting the sections with constant or pseudo-random values.
  b) Self-tests
     Self-tests of software components are run at boot-time and at the request of the authorized user.
  c) Protection of assets (especially keys)
  d) Logging
     i. **The TOE reserves 900 MB memory in the non-volatile memory for the event log.**
     ii. **Users (administrator roles) cannot modify or delete audit log entries. If audit memory is full and a new event shall be logged, the oldest log entry will be overwritten.**
     iii. **The events being logged in addition to the ones described in [BSI-CC-PP-0047, 1.3.4. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste, Protokollierung] are described in FAU_GEN.1.**
     iv. **The TOE implements countermeasures against attacks attempting to flood the audit log in order to use the limited size of the audit log memory and the process of cyclically overwriting log memory to overwrite log entries that provide evidence of the attacker's activity.**
     v. **When the audit log is filled by 80% the TOE will inform the administrator via a dedicated audit event.**
- Administration
  a) Local management interface

i. **The remote management interface can be reached via the interface LS.LAN and is secured with TLS. A web interface and authentication is provided by a non-TOE part of the connector, though.**
ii. **The configurable options are restricted in a way that the certified status of the TOE cannot be compromised (see section 7.1.6 SF.Administration).**
iii. **The filter rules for the dedicated LAN packet filter can be configured using the management interface.**

b) Remote management interface
   i. **The remote management interface can be reached via the interface LS.WAN and is secured with TLS. However, the TOE will initiate the connection. A web interface and authentication is provided by a non-TOE part of the connector, though.**

c) The web interface of the non-TOE part of the connector will use the external interface LS.AK to access the management functionality of the TOE.

d) Secure firmware Update

The following functionality is provided by other non-TOE parts of the whole connector:

- gSMC-Ks
  - Physical random number generator (PRNG) (getRandom)
  - Secure key storage of asymmetric keys and certificates
  - Asymmetric cryptographic operations
- Non-TOE part of connector
  - Web interface for management (reachable over TLS provided by the TOE)
  - Authentication of administrators
  - Audit review
  - Integrity verification of the boot loader

1.4.9 Physical scope

The physical scope of the TOE can be outlined by the list of software and documentation parts:

TOE part	Description	Version
Firmware image	The TOE firmware. This firmware also includes non-TOE parts. It includes the boot loader image.	1.3.0
Guidance documentation (“Administra-tionshandbuch KoCoBox MED+ für die Komponente Netzkonnektor”)	The guidance documentation describes the secure usage of the TOE.	1.3.0
Guidance addendum documentation („Ergänzungen zum Administratorhand-buch KoCoBox MED+ für die Komponente Netzkonnektor“)	The addendum to the guidance documentation describes additional measures that ensure the secure usage of the TOE.	1.0.2

TOE part	Description	Version
End user manual („Allgemeine Gebrauchsanleitung KoCoBox MED+“)	The end user manual describes the overall usage of the connector (including TOE and non-TOE features)	1.3.0

Table 2: Physical scope

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This security target was created according to Common Criteria Version 3.1 Release 4 (September 2012).

This security target is

- CC Part 2 extended and
- CC Part 3 conformant.

The family FPT_EMS and the security functional requirement FPT_EMS.1 which is not defined in CC part 2 has been added. The definition of this SFR can be found in [BSI-CC-PP-0047, 5.1. Definition der erweiterten Familie FPT_EMS und der Anforderung FPT_EMS.1].

2.2 Protection Profile Claim

This security target claims strict conformance to the protection profile “Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen, Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), BSI-CC-PP-0047” by the German Bundesamt für Sicherheit in der Informationstechnik [BSI-CC-PP-0047].

2.3 Package Claim

This security target is conformant to the evaluation assurance level 3 (EAL3) with augmentation of AVA_VAN.5, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 (hereafter called “EAL3+”) in accordance with [BSI-CC-PP-0047, 2.3. Paket-Konformität].

2.4 Conformance Rationale

Since this ST uses an SFR, which is not based upon a functional requirement in CC Part 2, this ST is “CC Part 2 extended”.

Since no additional assurance requirements have been added this ST is “CC Part 3 conformant”.

This ST claims conformance to a single protection profile. This guarantees that no contradictions or inconsistencies between different PPs are present.

This ST claims conformance to all SARs required by the underlying PP.

3 Security Problem Definition

This chapter identifies and explains:

- any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment
- any organizational security policies with which the TOE must comply
- any assumptions about the intended usage of the TOE and the environment of use of the TOE

3.1 Assets

Resources and data that are protected by the TOE, i.e. the assets, are outlined in [BSI-CCPP-0047, 3.1. Zu schützende Werte] which applies without modification.

3.2 Subjects and Objects

The subjects and objects used to formulate the security problem definition are presented in [BSI-CC-PP-0047, 3.2. Subjekte und Objekte]. This definition applies without modification.

3.3 Threats: Considered Threats

The section [BSI-CC-PP-0047, 3.3. Bedrohungen] and its subsections apply without modifications.

3.4 Organizational Security Policies

OSP.SPSP has been added to map a subset of the spanning security properties (“flexibel zuordenbare Funktionalitäten”) from the PP AK-EB [BSI-CC-PP-0046] onto the TOE.

3.4.1 OSP.NK.Zeitdienst

The section from [BSI-CC-PP-0047, 3.4. OSP.NK.Zeitdienst] applies without modifications.

3.4.2 OSP.NK.SIS

The section from [BSI-CC-PP-0047, 3.4. OSP.NK.SIS] applies without modifications.

3.4.3 OSP.NK.BOF

The section from [BSI-CC-PP-0047, 3.4. OSP.NK.BOF] applies without modifications.

3.4.4 OSP.SPSP - Spanning Security Properties

The TOE provides the following additional functionality

- Secure software update for updating the device firmware
- Storage for audit data

3.5 Assumptions: Considered Assumptions

The assumptions in section [BSI-CC-PP-0047, 3.5. Annahmen] apply without modifications.

4 Security Objectives

4.1 Security Objectives for the TOE

O.Update, and O.Logging_Facility have been added to comply with OSP.SPSP.

4.1.1 General Objectives: Protection and Administration

O.NK.Schutz

All security objectives described under [BSI-CC-PP-0047, 4.1.1. O.NK.Schutz] must be met.

O.NK.EVG_Authenticity

All security objectives described under [BSI-CC-PP-0047, 4.1.1. O.NK.EVG_Authenticity] must be met.

Note: The acceptance procedures for the secure delivery process of the TOE include verification of two seals that are attached to the casing. Thereby, the recipient is able to determine whether the TOE has been tampered with. More information on the secure delivery process and the acceptance procedures is given in the delivery documentation (ALC_DEL) and the guidance documentation (AGD).

O.NK.Admin_EVG

All security objectives described under [BSI-CC-PP-0047, 4.1.1. O.NK.Admin_EVG] must be met.

Refinement: The administration concept of the connector is role-based but each user with the privileges to access the management functionality is considered to be an administrator independently from the configured permissions of their role. The term “role” is used in this ST strictly in the sense of “user with authorized access to the management functionality”. To separate this definition of a role from the role used by the management service, the latter is simply called “service-role” within the scope of this document.

Considering this, the TOE provides only one single role:

- Administrator

Rationale: The management service provides a service-role named “Administrator” that cannot be modified or removed. This service-role has all permissions and is thus allowed to access and modify all configuration options. A user with this service-role is allowed to define additional service-roles with a fully configurable set of permissions for various option groups (e.g. IP configuration, VPN connections, DNS server). This enables the possibility to create wide range of different service-roles with different permissions. To simplify matters, each service-role is considered to have the full set of permissions, thus to be an entity of the role “Administrator”.

O.NK.Protokoll

All security objectives described under [BSI-CC-PP-0047, 4.1.1., O.NK.Protokoll] must be met.

O.NK.Zeitdienst

All security objectives described under [BSI-CC-PP-0047, 4.1.1., O.NK.Zeitdienst] must be met.

O.Update - Secure Update

All security objectives described under [BSI-CC-PP-0046, 4.1., O.Update] must be met.

O.Logging_Facility - Fundamental Logging Facility

The TOE provides a centralized logging facility for logging the security-relevant events of the TOE itself and the trusted IT product AK. All log entries are consolidated into a single storage. The log is only accessible to the audit log service process.

Log entries cannot be modified or deleted by unauthorized entities and are cyclically overwritten if the audit memory is full.

4.1.2 Objectives of the VPN Functionality

O.NK.VPN_Auth

All security objectives described under [BSI-CC-PP-0047, 4.1.2., O.NK.VPN_Auth] must be met.

O.NK.Zert_Prüf

All security objectives described under [BSI-CC-PP-0047, 4.1.2., O.NK.Zert_Prüf] must be met.

O.NK.VPN_Vertraul

All security objectives described under [BSI-CC-PP-0047, 4.1.2., O.NK.VPN_Vertraul] must be met.

O.NK.VPN_Integrität

All security objectives described under [BSI-CC-PP-0047, 4.1.2., O.NK.VPN_Integrität] must be met.

4.1.3 Objectives of the Packet Filter Functionality

O.NK.PF_WAN

All security objectives described under [BSI-CC-PP-0047, 4.1.3., O.NK.PF_WAN] must be met.

O.NK.PF_LAN

All security objectives described under [BSI-CC-PP-0047, 4.1.3., O.NK.PF_LAN] must be met.

O.NK.Stateful

All security objectives described under [BSI-CC-PP-0047, 4.1.3., O.NK.Stateful] must be met.

Both WAN and LAN packet filter conduct stateful packet inspection through timely processing of connection tracking data.

4.2 Environment Security Objectives

OE.SW-Update has been added to define processes for providing valid and approved software updates to the TOE.

4.2.1 OE.NK.RNG

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.RNG] must be met.

4.2.2 OE.NK.Echtzeituhr

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.Echtzeituhr] must be met.

4.2.3 OE.NK.Zeitsynchro

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.Zeitsynchro] must be met.

4.2.4 OE.NK.GSMC-K

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.GSMC-K] must be met.

4.2.5 OE.NK.KeyStorage

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.KeyStorage] must be met.

4.2.6 OE.NK.AK

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.AK] must be met.

4.2.7 OE.NK.CS

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.CS] must be met.

4.2.8 OE.NK.Admin_EVG

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.Admin_EVG] must be met.

4.2.9 OE.NK.Admin_Auth

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.Admin_Auth] must be met.

4.2.10 OE.NK.PKI

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.PKI] must be met.

4.2.11 OE.NK.phys_Schutz

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.phys_Schutz] must be met.

4.2.12 OE.NK.sichere_TI

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.sichere_TI] must be met.

4.2.13 OE.NK.kein_DoS

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.kein_DoS] must be met.

4.2.14 OE.NK.Betrieb_AK

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.Betrieb_AK] must be met.

4.2.15 OE.NK.Betrieb_CS

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.Betrieb_CS] must be met.

4.2.16 OE.NK.Ersatzverfahren

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.Ersatzverfahren] must be met.

4.2.17 OE.NK.SIS

All security objectives described under [BSI-CC-PP-0047, 4.2. Sicherheitsziele für die Umgebung, OE.NK.SIS] must be met.

4.2.18 OE.SW-Update

All security objectives described under [BSI-CC-PP-0046, 4.2. Sicherheitsziele für die Umgebung, OE.SW-Update] must be met.

To check plausibility, integrity, and authenticity before applying an update, update images are associated with an ascending version number and are distributed signed (with a manufacturer-specific cryptographic identity).

4.3 Security Objectives Rationale

4.3.1 Correspondence of threats, assumptions and OSPs

	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful	**O.Update**	**O.Logging_Facility**	OE.NK.RNG	OE.NK.Echtzeituhr	OE.NK.Zeitsynchro	OE.NK.GSMC-K	OE.NK.KeyStorge	OE.NK.AK	OE.NK.CS	OE.NK.Admin_EVG	OE.NK.Admin_Auth	OE.NK.PKI	OE.NK.phys_Schutz	OE.NK.sichere_TI	OE.NK.kein_DoS	OE.NK.Betieb_AK	OE.NK.Betrieb_CS	OE.NK.Ersatzverfahren	OE.NK.SIS	**OE.SW-Update**
T.NK.local_EVG_LAN	X			X							X	**Y**							X													
T.NK.remote_EVG_WAN	X			X	X	X	X		X	X		X			X		X	X	X					X		X						
T.NK.remote_EVG_LAN	X			X	X	X	X		X	X	X	**Y**			X		X	X	X					X		X				X		X	
T.NK.remote_VPN_Data				O	X	X	X	X	X			**Z**			X		X	X	X	X				X		X		X		X	X	X	
T.NK.local_admin_LAN	X		X	X								**Y**			X				X			X	X	O	**Y**						**Y**		
T.NK.remote_admin_WAN	X		X	X								**Y**			X				X			X	X	O							O		
T.NK.counterfeit		X																X							X						X		
T.NK.Zert_Prüf				**O**	**Y**		X					**Y**			**Y**			**Y**						X							**Y**		
T.NK.TimeSync				**O**	X				X			**Y**			**Y**		X	**Y**						**Y**							**Y**		
T.NK.DNS				O		X						O																		X		**Y**	
OSP.NK.Zeitdienst					X											X	X																
OSP.NK.SIS										X																						X	
OSP.NK.BOF										X											X												
OSP.SPSP													**Z**	**Z**																			**Z**
A.NK.phys_Schutz																									X								
A.NK.GSMC-K																		X															
A.NK.sichere_TI																										X							
A.NK.kein_Dos																											X						
A.NK.AK																				X													
A.NK.CS																					X												
A.NK.Betrieb_AK																												X					
A.NK.Betrieb_CS																													X				
A.NK.Admin_EVG																						X											
A.NK.Ersatzverfahren																														X			
A.NK.Zugriff_gSMC-K																		X										X					

Table 3: Trace of security objectives to threats, assumptions, and OSPs

Table 2 traces the security objectives to the threats, assumptions and organizational security policies (OSP) and was taken from [BSI-CC-PP-0047, 4.3.1. Überblick: Abbildung der Bedrohungen und Annahmen auf Ziele]. The security objectives O.Update, O.Logging_Facility, and OE.SW-Update have been added. Additionally, the organizational security policy OSP.SPSP has been added.

The following notation has been used in Table 2:

- Unmodified relations defined in the PP are marked with an X.
- Optional relations defined in the PP which were added are marked with Y.
- Relations which were added are marked with a Z.
- Optional relations defined in the PP which were omitted are marked with an O.

Non-optional relations defined in the PP which were removed are marked with R. The present ST does not contain such a relation.

The resistance against some threats and some objectives are additionally supported by assurance components from CC Part 3 (list taken from [BSI-CC-PP-0047, 4.3.1. Überblick: Abbildung der Bedrohungen und Annahmen auf Ziele]):

- Resistance against T.NK.local_EVG_LAN is supported by the CC class ADV and the CC family AVA_VAN.
- Resistance against T.NK.counterfeit is supported by the CC components ALC_DEL.1 and AGD_OPE.1.
- The objective OE.NK.Admin_EVG is supported by the CC family AGD_OPE.

4.3.2 Rationale for the Changes in Comparison to the PP

This section gives a rationale for the addition of relations and omission of optional relations between the security objectives and the threats and assumptions presented in section 4.3.1.

Rationales for the unmodified relations defined in the PP is given in [BSI-PP-CC-0047, 4.3.2. Abwehr der Bedrohungen durch die Sicherheitsziele], [BSI-PP-CC-0047, 4.3.3. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele], and [BSI-PPCC-0047, 4.3.4. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung].

Resistance against Threats Provided by the Security Objectives

The rationale for **T.NK.local_EVG_LAN** was extended compared to [BSI-CC-PP-0047, 4.3.2.1. T.NK.local_EVG_LAN]: **O.NK.Stateful** defends against T.NK.local_EVG_LAN by refusing illegitimate packets.

The rationale for **T.NK.remote_EVG_WAN** is given in [BSI-CC-PP-0047, 4.3.2.2. T.NK.remote_ EVG_WAN].

The rationale for **T.NK.remote_EVG_LAN** [BSI-CC-PP-0047, 4.3.2.3. T.NK.remote_EVG_LAN] is specialized as follows: A single-component implementation is used; therefore the TOE also protects the application connector from attacks originating from the LAN. **O.NK.Stateful** also defends against T.NK.remote_EVG_LAN by refusing illegitimate packets.

The rationale for **T.NK.remote_VPN_Data** [BSI-CC-PP-0047, 4.3.2.4. T.NK.remote_VPN_Data] is specialized as follows: **O.NK.Stateful** also defends against T.NK.remote_VPN_Data by refusing illegitimate packets.

The rationale for **T.NK.local_admin_LAN** [BSI-CC-PP-0047, 4.3.2.5. T.NK.local_admin_LAN] is extended as follows: **O.NK.Stateful** also defends against T.NK.local_admin_LAN by refusing illegitimate packets. **OE.NK.phys_Schutz** prevents that attackers gain physical access to the connector. **OE.NK.Ersatzverfahren** ensures that a substitute process is available if cryptographic algorithms for the secure TLS channel cannot be used anymore.

The rationale for **T.NK.remote_admin_WAN** [BSI-CC-PP-0047, 4.3.2.6. T.NK.remote_admin_WAN] is specialized as follows: **O.NK.Stateful** defends against T.NK.remote_admin_WAN by refusing illegitimate packets.

The rationale for **T.NK.counterfeit** [BSI-CC-PP-0047, 4.3.2.7. T.NK.counterfeit] applies without modification.

The rationale for **T.NK.Zert_Prüf** [BSI-CC-PP-0047, 4.3.2.8. T.NK.Zert_Prüf] is specialized as follows: **O.NK.Stateful** defends against T.NK.Zert_Prüf by refusing illegitimate packets.

O.NK.Zeitdienst contributes by ensuring that the time is synchronized used for certificate validation. **OE.NK.RNG** contributes by providing random numbers for use in a challenge-response protocol. **OE.NK.Ersatzverfahren** contributes since cryptographic techniques are employed when verifying certificates. **OE.NK.GSMC-K** contributes by providing keys for establishing the secure VPN channel.

The rationale for **T.NK.TimeSync** [BSI-CC-PP-0047, 4.3.2.9. T.NK.TimeSync] is specialized as follows: **O.NK.Stateful** defends against T.NK.TimeSync by refusing illegitimate packets. **OE.NK.PKI** contributes by helping to establish a secure channel for time synchronization**. OE.NK.RNG** contributes by providing random numbers for use in a challenge-response-protocol. **OE.NK.Ersatzverfahren** contributes since cryptographic techniques are employed when synchronizing the system time. **OE.NK.GSMC-K** contributes by providing keys for establishing the secure VPN channel.

The rationale for **T.NK.DNS** [BSI-CC-PP-0047, 4.3.2.10. T.NK.DNS] is specialized as follows: **OE.NK.SIS** contributes by ensuring that the SIS effectively protects against attacks from the internet.

Enforcement of the OSPs through the Security Objectives

The rationale for **OSP.NK.Zeitdienst** [BSI-CC-PP-0047, 4.3.3.1. OSP.NK.Zeitdienst] applies without modifications.

The rationale for **OSP.NK.SIS** [BSI-CC-PP-0047, 4.3.3.2. OSP.NK.SIS] applies without modifications.

The rationale for **OSP.NK.BOF** [BSI-CC-PP-0047, 4.3.3.3. OSP.NK.BOF] applies without modifications.

OSP.SPSP requires the implementation of certain spanning security properties in the scope of the TOE. **O.Update** and **OE.SW-Update** provide a secure software update for updating the device firmware. Additionally, **O.Update** maintains and enforces certain aspects of the separation mechanism. **O.Logging_Facility** enables the capability of providing one consolidated log to all trustworthy IT products of the connector.

Mapping of the Assumptions to the Security Objectives

The rationale from [BSI-CC-PP-0047, 4.3.4. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung] applies without modifications.

5 Extended components definition

The definition of CC Part 2 extended components can be found in [BSI-CC-PP-0047, 5. Definition zusätzlicher Komponenten]. The definition of the family FPT_EMS and the component FPT_EMS.1 can be found in [BSI-CC-PP-0047, 5.1. Definition der erweiterten Familie FPT_EMS und der Anforderung FPT_EMS.1].

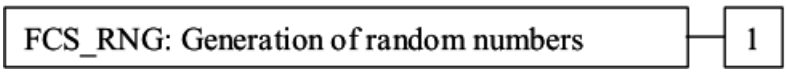
This ST defines another extended component in the following chapter.

5.1 FCS_RNG Generation of random numbers

Family Behavior:

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:



FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1	**Random number generation**
Hierarchical to:	No other component.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet assignment: *a defined quality metric*].

6 Security Requirements

6.1 TOE Security Functional Requirements

The TOE security functional requirements are presented in the same order as they appear in [BSI-CC-PP-0047, 6.1. Funktionale TOE-Sicherheitsanforderungen]. Additional SFRs have been collected in sections 6.1.8 and 6.1.9.

6.1.1 VPN Client

FTP_ITC.1/NK.VPN_TI – Inter-TSF trusted channel

FTP_ITC.1.1/NK.VPN_TI	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.1/NK.VPN_TI] applies without modifications.
FTP_ITC.1.2/NK.VPN_TI	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.2/NK.VPN_TI] applies without modifications.
FTP_ITC.1.3/NK.VPN_TI	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.3/NK.VPN_TI] applies without modifications. The refinement from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.3/NK.VPN_TI] applies without modifications.

FTP_ITC.1/NK.VPN_SIS – Inter-TSF trusted channel

FTP_ITC.1.1/NK.VPN_SIS	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.1/NK.VPN_SIS] applies without modifications.
FTP_ITC.1.2/NK.VPN_SIS	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.2/NK.VPN_SIS] applies without modifications.
FTP_ITC.1.3/NK.VPN_SIS	The section from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.3/NK.VPN_SIS] applies without modifications. The refinement from [BSI-CC-PP-0047, 6.1.1. VPN-Client, FTP_ITC.1.3/VPN] applies without modifications.

6.1.2 Dynamischer Paketfilter mit zustandsgesteuerter Filterung

FDP_IFC.1/NK.PF – Subset information flow control

FDP_IFC.1.1/NK.PF	The section from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FDP_IFC.1.1/NK.PF] applies without modifications.

FDP_IFF.1/NK.PF – Simple Security Attributes

FDP_IFF.1.1/NK.PF	The section from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FDP_IFF.1.1/NK.PF] applies without modifications.
FDP_IFF.1.2/NK.PF	The section from [BSI-CC-PP-0047, 6.2.2. Dynamischer

	Paketfilter mit zustandsgesteuerter Filterung, FDP_IFF.1.2/NK.PF] applies without modifications. **Refinement: The usage of a VPN connection for security relevant data shall be enforced by using an appropriate set of policies of the network subsystem that demand data from the application connector to be routed into the VPN.**
FDP_IFF.1.3/NK.PF	The section from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FDP_IFF.1.3/NK.PF] applies without modifications.
FDP_IFF.1.4/NK.PF	The TSF shall explicitly authorize an information flow based on the following rules: Stateful Packet Inspection, *none.* The refinement from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FDP_IFF.1.4/NK.PF] applies without modifications.
FDP_IFF.1.5/NK.PF	The TSF shall explicitly deny an information flow based on the following rules: 1) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with NET_TI_GESICHERTE_FD, NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL outside VPN channel to VPN concentrator of the TI. 2) The TSF prevents direct communication of active entities in the LAN, application connector and service modules with SIS outside VPN channel to VPN concentrator of the SIS. 3) The TSF prevents communication of active entities in the LAN with destination IP address within ANLW_AKTIVE_BESTANDSNETZE initiated by active entities in the LAN, if MGM_LOGICAL_SEPARATION=Enabled). 4) The TSF prevents communication of active entities in the LAN with entities with IP addresses within ANLW_BESTANDSNETZE but outside ANLW_AKTIVE_BESTANDSNETZE. 5) The TSF prevents communication of service modules with NET_TI_ZENTRAL, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE and internet via SIS or IAG. 6) The TSF prevents communication initiated by entities with IP address within NET_TI_GESICHERTE_FD,

NET_TI_OFFENE_FD, NET_TI_ZENTRAL, NET_TI_DEZENTRAL (except the connector itself), ANLW_BESTANDSNETZE and NET_SIS.

7) The TSF prevents communication of entities with IP addresses in the inner header within NET_TI_ZENTRAL, NET_TI_GESICHERTE_FD, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE, ANLW_LAN_ADDRESS_SEGMENT, ANLW_LEKTR_INTRANET_ROUTES and ANLW_WAN_NETWORK_SEGMENT coming through the VPN tunnel with VPN concentrator of the SIS.
8) The TSF prevents receive of packets from entities in LAN if (MGM_LU_ONLINE=Enabled and MGM_LOGICAL_SEPARATION=Disabled and ANLW_INTERNET_MODUS = KEINER).
9) The TSF prevents inbound packets of the VPN channels from SIS with destination address in the inner header outside
   a) ANLW_LAN_IP_ADDRESS or
   b) ANLW_LEKTR_INTRANET_ROUTES if ANLW_WAN_ADAPTER_MODUS=DISABLED or
   c) ANLW_WAN_IP_ADDRESS if ANLW_WAN_ADAPTER_MODUS=ACTIVE
10) The TSF prevents communication of IAG to connector through LAN interface if (ANLW_WAN_ADAPTER_MODUS= ACTIVE).
11) The TSF prevents communication of IAG to connector through WAN interface of the connector if (ANLW_WAN_ADAPTER_MODUS= DISABLED).
12) *All firewall rules defined in [gemSpecKonnektor, 4.2.1.1.2 Routing und Firewall] that call for traffic to be dropped.*

The refinement from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FDP_IFF.1.5/NK.PF] applies without modifications.

Refinement of all FDP_IFF.1 requirements: The PF SFP shall also consider the interface a packet is originating from or heading to.

FMT_MSA.3/NK.PF – Static attribute initialization

FMT_MSA.3.1/NK.PF	The section from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung,

	FMT_MSA.3.1/NK.PF] applies without modifications.
FMT_MSA.3.2/NK.PF	The TSF shall allow ~~**the**~~ *nobody* to specify alternative initial values to override the default values when an object or information is created. The refinement from [BSI-CC-PP-0047, 6.2.2. Dynamischer Paketfilter mit zustandsgesteuerter Filterung, FMT_MSA.3.2/NK.PF] applies without modifications.

6.1.3 Netzdienste

FPT_STM.1/NK – Reliable time stamps

FPT_STM.1.1/NK	The section from [BSI-CC-PP-0047, 6.2.3. Netzdienste, FPT_STM.1.1/NK] applies without modifications.
Refinement:	Die Zuverlässigkeit (reliable) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.NK.Echtzeituhr) mit Zeitservern (vgl. OE.NK.Zeitsynchro) unter Verwendung des Protokolls NTP v4 [22] erreicht. Der EVG verwendet den verlässlichen Zeitstempel für sich selbst und bietet anderen Konnektorteilen eine Schnittstelle zur Nutzung des verlässlichen Zeitstempels an. Befindet sich der EVG im Online-Modus, muss er die Zeitsynchronisation mindestens bei Start-up, einmal innerhalb von 24 Stunden und auf Anforderung durch den Administrator durchführen. Die verteilte Zeitinformation weicht nicht mehr als *3600 Sekunden* von der Zeitinformation der darüber liegenden Stratum-Ebene ab.
Refinement:	**The TOE will notify users about critical states via its display.**

FPT_TDC.1/NK.Zert – Inter-TSF basic TSF data consistency

FPT_TDC.1.1/NK.Zert	The section from [BSI-CC-PP-0047, 6.2.3. Netzdienste, FPT_TDC.1.1/NK.Zert] applies without modifications.
FPT_TDC.1.2/NK.Zert	The section from [BSI-CC-PP-0047, 6.2.3. Netzdienste, FPT_TDC.1.2/NK.Zert] applies without modifications. The refinement from [BSI-CC-PP-0047, 6.2.3. Netzdienste, FPT_TDC.1.2/NK.Zert] applies without modifications.
Refinement:	**The interpretation rules are defined in [gemSpecPKI, 8.3.1.1 TUC_PKI_018 "Zertifikatsprüfung in der TI "] considering the verification mode “CRL”.**

6.1.4 Stateful Packet Inspection

The section from [BSI-CC-PP-0047, 6.2.4. Stateful Packet Inspection] applies without modifications.

Stateful packet inspection is modeled in FDP_IFF.1/NK.PF – Simple Security Attributes.

6.1.5 Selbstschutz

FDP_RIP.1/NK – Subset residual information protection

FDP_RIP.1.1/NK	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: cryptographic keys (and session keys) used for the VPN, sensitive user data (zu schützende Daten der TI und der Bestandsnetze und zu schützende Nutzerdaten, *and no other.* The refinement from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FDP_RIP.1.1/NK] applies without modifications. **Refinement: These sensitive objects are overwritten with constant or pseudo-random values.**

FPT_TST.1/NK – TSF testing

FPT_TST.1.1/NK	The TSF shall run a suite of self-tests during initial start-up, at the request of the authorized user to demonstrate the correct operation of *stored TSF executable code*.
FPT_TST.1.2/NK	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3/NK	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. The refinement from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FPT_TST.1/NK] applies without modifications.

FPT_EMS.1/NK – TOE Emanation

FPT_EMS.1.1/NK	The TOE shall not emit sensitive data (as listed below) – or information which can be used to recover such sensitive data – through network interfaces (LAN or WAN) in excess of limits that ensure that no leakage of this sensitive data occurs enabling access to • session keys derived from private VPN authentication keys, • key material used to verify the TOE's integrity during self-tests,

- key material used to verify the integrity and authenticity of software updates,
- none,
- none,
- *none* and
- data to be protected (“zu schützende Daten der TI und der Bestandsnetze”)
- *none.*

FPT_EMS.1.2/NK — The section from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FPT_EMS.1/NK] applies without modifications.

FAU_GEN.1/NK.SecLog – Audit data generation

FAU_GEN.1.1/NK.SecLog — The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the not specified level of audit; and

b)

- start-up, shut down and reset (if applicable) of the TOE
- VPN connection to TI successfully / not successfully established,
- VPN connection to SIS successfully / not successfully established,
- TOE cannot reach services of the transport network,
- IP addresses of the TOE are undefined or wrong,
- TOE could not perform system time synchronization within the last 30 days,
- during time synchronization, the deviation between the local system time and the time received from the time server exceeds the allowed maximum deviation (see refinement to FPT_STM.1/NK);
- changes of the TOE configuration.

The refinement from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FAU_GEN.1.1/NL.SecLog] applies without modifications.

FAU_GEN.1.2/NK.SecLog — The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *and no other audit relevant information.*

The refinement from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FAU_GEN.1.2/NK.SecLog] applies without modifications.

Refinement: The TOE shall implement countermeasures against attacks attempting to flood the audit log in order to use the limited size of the audit log memory and the process of cyclically overwriting log memory to overwrite log entries that provide evidence of the attacker's activity.

FAU_GEN.2/NK.SecLog – User identity association

FAU_GEN.2.1/NK.SecLog The section from [BSI-CC-PP-0047, 6.2.5. Selbstschutz, FAU_GEN.2.1/NK.SecLog] applies without modifications.

6.1.6 Administration

FMT_SMR.1/NK – Security roles

FMT_SMR.1.1/NK The section from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_SMR.1.1/NK] applies without modifications.

FMT_SMR.1.2/NK The section from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_SMR.1.2/NK] applies without modifications.

The refinement and application note 79 from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_SMR.1.2/NK] applies without modifications.

FMT_MTD.1/NK – Management of TSF data

FMT_MTD.1.1/NK The TSF shall restrict the ability to *the operations in the following table on* the real time clock, packet filtering rules *and other TSF data in the following table* to the role Administrator.

Operation	TSF data affected
Modify[1]	System time
Create, Modify, Delete	Packet filtering rules

[1] Only available in offline mode, when there is no connection to the NTP servers.

Perform	Self-tests
Perform	Software update
Perform	Activation/deactivation of VPN connections[2]

The refinement from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_MTD.1.1/NK] applies without modifications.

FIA_UID.1/NK.SMR – Timing of identification

FIA_UID.1.1/NK.SMR	The section from [BSI-CC-PP-0047, 6.2.6. Administration, FIA_UID.1.1/NK.SMR] applies without modifications.
FIA_UID.1.2/NK.SMR	The section from [BSI-CC-PP-0047, 6.2.6. Administration, FIA_UID.1.2/NK.SMR] applies without modifications. **Refinement: The TOE prevents the following TSF-mediated actions on behalf of the user before the user is identified in addition:** • **All operations stated in FMT_MTD.1.1/NK.**

FTP_TRP.1/NK.Admin – Trusted path

FTP_TRP.1.1/NK.Admin	The TSF shall provide a communication path between itself and remote, local 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, disclosure. Rationale: “remote, local users” refers to Administrators using the web interface via WAN OR LAN.
FTP_TRP.1.2/NK.Admin	The TSF shall permit local users, the TSF to initiate communication via the trusted path.
FTP_TRP.1.3/NK.Admin	The section from [BSI-CC-PP-0047, 6.2.6. Administration, FTP_TRP.1.3/NK.Admin] applies without modifications.

FMT_SMF.1/NK – Specification of Management Functions

FMT_SMF.1.1/NK	The section from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_SMF.1.1/NK] applies without modifications.
Refinement:	The TOE shall be capable of performing all security management functions stated in FMT_MTD.1/NK.

[2] Please note that deactivation of a VPN connection also ensures that any network traffic which should be routed via the VPN is not possible at all.

FMT_MSA.1/NK.PF – Management of security attributes

FMT_MSA.1.1/NK.PF	The TSF shall enforce the PF SFP to restrict the ability to query, modify, and delete the security attributes packet filtering rules to the roles „Administrator“, *and no other roles.* The refinement from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_MSA.1.1/NK.PF] applies without modifications.

FMT_MSA.4/NK – Security attribute value inheritance

FMT_MSA.4.1/NK	The section from [BSI-CC-PP-0047, 6.2.6. Administration, FMT_MSA.4.1/NK] applies without modifications.

6.1.7 Kryptographische Basisdienste

FCS_COP.1/NK.Hash Cryptographic operation

FCS_COP.1.1/NK.Hash	The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm SHA-1, SHA-256, *SHA-512* and cryptographic key sizes [none] that meet the following: FIPS PUB 180-4 **[FIPS180-4]**.

FCS_COP.1/NK.HMAC – Cryptographic operation

FCS_COP.1.1/NK.HMAC	The TSF shall perform HMAC value calculation in accordance with a specified cryptographic algorithm HMAC with SHA-1, *SHA-256* and cryptographic key sizes *160 and 256* bit that meet the following: FIPS PUB 180-4 [**FIPS180-4**], RFC 2404 [**RFC2404**], RFC 4868 [**RFC4868**], RFC 5996 **[IKEv2]**.

FCS_COP.1/NK.Auth – Cryptographic operation

FCS_COP.1.1/NK.Auth	The section from [BSI-CC-PP-0047, 6.2.7. Kryptographische Basisdienste, FCS_COP.1.1/NK.Auth] applies without modifications.

FCS_COP.1/NK.ESP – Cryptographic operation

FCS_COP.1.1/NK.ESP	The section from [BSI-CC-PP-0047, 6.2.7. Kryptographische Basisdienste, FCS_COP.1.1/NK.ESP] applies without modifications.

FCS_COP.1/NK.IPsec – Cryptographic operation

FCS_COP.1.1/NK.IPsec	The section from [BSI-CC-PP-0047, 6.2.7. Kryptographische

Basisdienste, FCS_CKM.1.1/NK.IPsec] applies without modifications.

FCS_CKM.1/NK– Cryptographic key generation

FCS_CKM.1.1/NK	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *PRF-HMAC-SHA1, PRF-HMAC-SHA256* and specified cryptographic key sizes *256 bit* that meet the following: specification **[gemSpecKrypt, 3.3.1],** TR-03116 **[TR03116-1]**.

FCS_CKM.2/NK.IKE – Cryptographic key distribution

FCS_CKM.2.1/NK.IKE	The section from [BSI-CC-PP-0047, 6.2.7. Kryptographische Basisdienste, FCS_CKM.2.1/NK.IKE] applies without modifications.
Refinement:	**The following algorithms and preferences are supported for IKEv2 connections:** • **Diffie-Hellman Group: 14** • **DH exponent minimum length: 384 bits** • **Forward secrecy: yes** • **Encryption: AES-256-CBC** • **Authentication: HMAC-SHA-1-96, HMAC-SHA-256-128** • **PRF: PRF-HMAC-SHA1, PRF-HMAC-SHA-256** • **Rekeying: IKE lifetime limited to 86400 seconds, IPSec SA lifetime limited to 3600 seconds** • **Peer authentication: X.509 certificate with RSA 2048 bit keys**

FCS_CKM.4/NK – Cryptographic key destruction

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **by** *overwriting with zeros* that meets the following~~:~~ *none*.

6.1.8 Additional Security Functional Requirements

FCS_COP.1/TLS – Cryptographic operation

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] is not fulfilled since the generation of the ephemeral keys is performed in the TLS protocol as already required by this SFR. The key

	pair and certificate used as TOE identity during TLS handshake is stored in the gSMC-K#2 and generated during production of the card.FCS_CKM.4 Cryptographic key destruction fulfilled in this ST by: FCS_CKM.4/NK (for all ephemeral keys)
FCS_COP.1.1/TLS	The TSF shall perform *TLS protocol version 1.1 and 1.2 in server and client mode* in accordance with a specified cryptographic algorithm *according to Table 4* and cryptographic key sizes *according to Table 4* that meet the following: *standards according to Table 4*.
Refinement:	**The following algorithms and preferences are supported for TLS connections:** • **Diffie-Hellman Group 14 according to [RFC3526] for key establishment during TLS** • **DH exponent shall have a minimum length of 384 bits** • **Forward secrecy shall be provided** • **Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves according to [FIPS186-4] as well as the brainpoolP256r1 and the brainpoolP384r1 curves according to [RFC5639] and [RFC7027]** • **Peer authentication (if required): X.509 certificate with RSA 2048 bit keys**

Algorithms / cipher suites	Standard	Purpose
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[RFC4346]	TLS 1.1 and TLS 1.2 for local and remote management
TLS_DHE_RSA_WITH_AES_256_CBC_SHA		
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[RFC5246]	TSL 1.2 for local and remote management
TLS_DHE_RSA_WITH_AES_256_CBC_SHA		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	[RFC4492]	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	[RFC5289]	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		

Table 4: TLS cipher suites

FCS_RNG.1/Hash_DRBG - Random number generation for TLS and signature creation

Hierarchical to:	No other component.
Dependencies:	No dependencies.
FCS_RNG.1.1/Hash_DRBG	The TSF shall provide a deterministic random number

	generator that implements:
(DRG.3.1)	*If initialized with a random seed using PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 100 bits min-entropy.*
(DRG.3.2)	*The RNG provides forward secrecy.*
(DRG.3.3)	*The RNG provides backward secrecy even if the current internal state is known.*
FCS_RNG.1.2/Hash_DRBG	The TSF shall provide random numbers that meet
(DRG.3.4)	*The RNG gets initialized during every startup and after 2048 requests with a random seed of minimal 384 bits using a PTRNG of class PTG.2. The RNG generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability w > $1 - 2^{-16}$.*
(DRG.3.5)	*Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.*
Application Note:	FCS_RNG.1/Hash_DRBG is implemented by Hash_DRBG with SHA-256 according to [NIST800-90A, 10.1.1]. It is used for generation of ephemeral keys for Diffie-Hellman and nonces in the TLS protocol.

FCS_COP.1/Sign – Cryptographic operation

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] not fulfilled in this ST as no keys have to be generated for signature verification. The key pair for signature generation/verification is stored on the gSMC-K#1 and has been created during production. FCS_CKM.4 Cryptographic key destruction is not fulfilled in this ST as only public keys are used for this operation.
FCS_COP.1.1/Sign	The TSF shall perform *signature verification* in accordance with a specified cryptographic algorithm *according to Table 5* and cryptographic key sizes *according to Table 5* that meet the following: *standards according to Table 5*.

Algorithm	Key size (bits)	Standard	Purpose
RSASSA-PSS with SHA-256	2048	[PKCS#1] [FIPS180-4]	Algorithm is used to • verify signatures for TSF data integrity verification (secure

Algorithm	Key size (bits)	Standard	Purpose
			storage in NAND-flash)[3]
RSASSA-PSS with SHA-256	2048	[PKCS#1] [FIPS180-4]	Algorithm is used to • verify signatures of TSL and CRL
RSASSA-PSS with SHA-512	2048	[PKCS#1] [FIPS180-4]	Algorithm is used to • verify firmware update signatures • verify signatures for TSF and TSF data integrity verification (root file system in NAND-flash)
RSASSA-PKCS1-1.5 with SHA-256	2048	[PKCS#1] [FIPS180-4]	Algorithm is used to • verify signatures for TSF integrity verification (kernel and initramfs)
RSASSA-PSS with SHA-256	4096	[PKCS#1] [FIPS180-4]	Algorithm is used to • verify signatures for x509 certificates during the firmware update process

Table 5: Algorithms for signature verification

6.1.9 Requirements of the Spanning Security Properties

Secure Software Update

FDP_ACC.1/Update – Teilweise Zugriffskontrolle / Update

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 fulfilled by FDP_ACF.1/Update.

FDP_ACC.1.1/Update The TSF shall enforce the *Update SFP* on

Subjects:

- *Administrator*

Objects:

- *Firmware image*

Operations:

- *Install update*.

FDP_ACF.1/Update – Zugriffskontrolle basierend auf Sicherheitsattributen / Update

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 fulfilled by FDP_ACC.1/Update,
FMT_MSA.3 not fulfilled by any SFR as there are no security

[3] Please note that signature generation for verification of secure storage integrity is performed by the gSMC-K#1 with a private key stored on the gSMC-K#1.

	attributes to be managed.
FDP_ACF.1.1/Update	The TSF shall enforce the *Update SFP* to objects based on the following: *Subjects:* • *Administrator* *Objects:* • *firmware image with security attributes* o *signature* o *list of allowed firmware versions ("Firmwaregruppe")*.
FDP_ACF.1.2/Update	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The TOE shall update firmware images only if* *1. the signature of the new firmware could be verified, and* *2. the firmware version of the new firmware is allowed according to the list of allowed firmware versions.*
FDP_ACF.1.3/Update	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/Update	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *The TOE shall not install firmware updates automatically but on the explicit request of the administrator.*

FDP_ITC.1/Update – Import von Benutzerdaten ohne Sicherheitsattribute (Update)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1, or FDP_IFC.1] fulfilled by FDP_ACC.1/Update FMT_MSA.3 not fulfilled by any SFR as there are no security attributes to be managed.
FDP_ITC.1.1/Update	The TSF shall enforce the *Update SFP* when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2/Update	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3/Update	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *The TSF shall verify the integrity and authenticity of the firmware image before it performs the update process*.

FDP_UIT.1/Update – Einfache Integrität des Datenaustausches (Update)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1, or FDP_IFC.1] fulfilled by FDP_ACC.1/Update [FTP_ITC.1, or FTP_TRP.1] fulfilled by FDP_ITC.1/Update
FDP_UIT.1.1/Update	The TSF shall enforce the *Update SFP* to receive user data in a manner protected from modification, deletion, insertion errors.
FDP_UIT.1.2/Update	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

Common Logging Facility

FAU_STG.1 – Geschützte Speicherung des Protokolls

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 fulfilled in this ST by: FAU_GEN.1/NK.SecLog
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 – Schutz vor Protokolldaten-Verlust

Hierarchical to:	FAU_STG.3
Dependencies:	FAU_STG.1 fulfilled in this ST by: FAU_STG.1
FAU_STG.4.1	The TSF shall overwrite the oldest stored audit records and *perform no other action* if the audit trail is full.
Refinement:	**The TOE reserves memory in the non-volatile NAND flash for the event log. If the size of the log exceeds 80% of the reserved memory, the TOE shall inform the administrator via the display.**

Data encryption

FCS_COP.1/Crypt.AES – Cryptographic operation

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] not fulfilled by the TOE. The symmetric key is generated by the gSMC-K. FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/NK
FCS_COP.1.1/Crypt.AES	The TSF shall perform *symmetric encryption/decryption* in accordance with a specified cryptographic algorithm *AES CBC with ESSIV* and cryptographic key sizes *256 bit* that meet the following: *[FIPS197]*, *[SP800-38A]*, and *[ESSIV]*.

FCS_COP.1/Crypt.RSA – Cryptographic operation

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] not fulfilled in this ST as no keys have to be generated for RSA-encryption. The key pair is stored on the gSMC-K and is generated during card production. FCS_CKM.4 Cryptographic key destruction not fulfilled in this ST as only public keys are used for this operation.
FCS_COP.1.1/Crypt.RSA	The TSF shall perform *asymmetric encryption* in accordance with a specified cryptographic algorithm *RSAES-OAEP with SHA-256* and cryptographic key sizes *2048 bit* that meet the following: *[PKCS#1] and [FIPS180-4].*

6.2 TOE Security Assurance Requirements

The assurance level for this security target is EAL3 augmented (EAL3+), as in denoted in [BSI-CC-PP-0047]. The augmentations to EAL3 for EAL3+ are:

- ADV_IMP.1
- ADV_TDS.3
- ADV_FSP.4
- ALC_TAT.1
- AVA_VAN.5
- ALC_FLR.2

Based on the AVA_VAN.5 requirement, the TOE has to resist attackers with a “high” attack potential.

6.2.1 Refinement of ALC_DEL.1

The refinements of ALC_DEL.1 stated in [BSI-CC-PP-0047, 6.3.1.] apply without modifications.

6.2.2 Refinement of AGD_OPE.1

The refinements of AGD_OPE.1 stated in [BSI-CC-PP-0047, 6.3.2.] apply without modifications.

6.2.3 Refinement of ADV_ARC.1

The refinements of ADV_ARC.1 stated in [BSI-CC-PP-0047, 6.3.3.] apply without modifications.

6.3 Security Requirements Rationale

6.3.1 Relation between the Security Objectives

The section [BSI-CC-PP-0047, 6.4.1.1. Abbildung der TOE-Ziele auf Anforderungen] and the according rationals from [BSI-CC-PP-0047, 6.4.1.2. Erfüllung der Sicherheitsziele durch die Anforderungen] apply without modifications if not stated otherwise.

Overview: Relation Between the Security Requirements and the Security Objectives

Table 6 gives an overview over the relation between the security requirements and the stated security objectives fulfilled by them.

	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.Update	O.Logging_Facility	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FTP_ITC.1/NK.VPN_TI								X		X	X			
FTP_ITC.1/NK.VPN_SIS								X		X	X			
FDP_IFC.1/NK.PF												X	X	X
FDP_IFF.1/NK.PF												X	X	X
FMT_MSA.3/NK.PF												X	X	
FPT_STM.1/NK				X	X									
FPT_TDC.1/NK.Zert						Y			X					
FDP_RIP.1/NK	X													
FPT_TST.1/NK	X													
FPT_EMS.1/NK	X									X	X			
FAU_GEN.1/NK.SecLog				X										
FAU_GEN.2/NK.SecLog				X										
FMT_SMR.1/NK			X									X	X	
FMT_MTD.1/NK			X											
FIA_UID.1/NK.SMR			X											
FTP_TRP.1/NK.Admin			X											
FMT_SMF.1/NK			X									X	X	
FMT_MSA.1/NK.PF			X									X	X	
FMT_MSA.4/NK			X											
FCS_COP.1/NK.Hash	X										X			
FCS_COP.1/NK.HMAC											X			
FCS_COP.1/NK.Auth		X						X						

	O.NK.Schutz	O.NK.EVG_Authenticity	O.NK.Admin_EVG	O.NK.Protokoll	O.NK.Zeitdienst	O.Update	O.Logging_Facility	O.NK.VPN_Auth	O.NK.Zert_Prüf	O.NK.VPN_Vertraul	O.NK.VPN_Integrität	O.NK.PF_WAN	O.NK.PF_LAN	O.NK.Stateful
FCS_COP.1/NK.ESP										X				
FCS_COP.1/NK.IPsec										X				
FCS_CKM.1/NK	X	X						X		X	X			
FCS_CKM.2/NK.IKE								X		X	X			
FCS_CKM.4/NK	X	X						X		X	X			
FCS_COP.1/Sign	Y	Y						Y						
FDP_ACC.1/Update	Y					Y								
FDP_ACF.1/Update	Y					Y								
FDP_ITC.1/Update	Y					Y								
FDP_UIT.1/Update	Y					Y								
FAU_STG.1							Y							
FAU_STG.4							Y							
FCS_COP.1/Crypt.AES	Y													
FCS_COP.1/Crypt.RSA	Y													
FCS_COP.1/TLS			Y											
FCS_RNG.1/Hash_DRBG			Y											

Table 6: Relation between the security requirements and the security objectives

The following notation has been used in Table 6:

- Unmodified relations defined in the PP are marked with an X.
- Additional relations are marked with Y.

Rationale for the Fulfillment of the Security Objectives through the Security Requirements

The rationales given in [BSI-CC-PP-0047, 6.4.1.2. Erfüllung der Sicherheitsziele durch die Anforderungen] apply without modifications. These rationales from the PP are augmented by the following rationales.

FCS_CKM.1/NK generates the session keys used in VPN connections. Therefore, this SFR helps to fulfill the objectives O.NK.VPN_Vertraul and O.NK.VPN_Integrität. Additionally, FCS_CKM.1/NK helps to prove the authenticity by helping to establish a valid connection to the telematics infrastructure (O.NK.EVG_Authenticity, O.NK.VPN_Auth).

FCS_COP.1/Sign has been added to represent the signature generation/verification algorithms used/provided by the TOE. The algorithms contribute to fulfilling these objectives (integrity hashes, verified TSL/CRL for VPN trust anchors) (O.NK.Schutz, O.NK.EVG_Authenticity, and O.NK.VPN_Auth).

FDP_ACC.1/Update, FDP_ACF.1/Update, FDP_ITC.1/Update, FDP_UIT.1/Update, and FPT_TDC.1/NK.Zert implement the secure software update process required by O.Update and guarantee that the integrity of the TOE is maintained even if the update process fails (O.NK.Schutz).

FAU_STG.1 and FAU_STG.4 fulfill the requirement of providing a secure common logging facility (O.Logging_Facility) for all trusted IT products of the connector.

FCS_COP.1/Crypt.AES and FCS_COP.1/Crypt.RSA help to protect user data and the TOE itself as intended by O.NK.Schutz.

FCS_COP.1/TLS contributes to ensure that the administrator can interact with the TOE using a trusted channel protected by cryptography.

FCS_RNG.1/Hash_DRBG contributes to ensure that the trusted channel is established using random ephemeral keys.

6.3.2 Fulfilment of the Dependencies

Fulfilment of the Functional Requirements

All dependencies of the stated SFRs are fulfilled. Evidence for the SFRs defined in the PP is given in [BSI-CC-PP-0047, 6.4.2.1. Erfüllung der funktionalen Anforderungen].

The fulfilment of all dependencies of the additionally added SFRs FCS_CKM.1/NK, FCS_COP.1/Sign, FAU_STG.1, FAU_STG.4, FCS_COP.1/Crypt.AES, FCS_COP.1/Crypt.RSA, FCS_COP.1/TLS is demonstrated by the statement “fulfilled in this ST by” at the description of the respective SFR in chapter 6.1.

Fulfilment of the Assurance Requirements Dependencies

The section [BSI-CC-PP-0047, 6.3.2.2. Erfüllung der Anforderungen an die Vertrauenswürdigkeit] applies without modifications.

6.4 Rationale for the chosen EAL

The rationale for the chosen EAL is given in [BSI-CC-PP-0047, 6.6].

7 TOE Summary Specification

This chapter provides an overview of the TOE's IT security functions stated in the functional specification. It offers a description of the general technical mechanisms that the TOE uses to satisfy all the SFRs.

Section 7.2 presents the relation between the security functional requirements (SFR) of the TOE and the TOE IT security functions (SF) from section 7.1.

7.1 TOE Security Functions

7.1.1 SF.VPN

SF.VPN provides secure communication channels between the TOE and a remote trusted IT product using the strongSwan IPsec implementation. These channels are logically distinct from other communication channels, provide assured identification of the end points and protection of the channel data from modification and disclosure. Such channels are used for connections to the telematics infrastructure (**FTP_ITC.1/NK.VPN_TI**) and to the SIS (**FTP_ITC.1/NK.VPN_SIS**). The TOE uses its cryptographic identity stored on the gSMC-K to authenticate against remote VPN concentrators.

Certificates are checked both mathematically and with the use of certificate revocation lists (CRLs) and Trusted Service Status List (TSL). The signature of TSL and CRL is also checked by the TOE. TSL and CRL are updated every 24 hours (via an HTTP download).

Furthermore, the TOE tracks expiration dates for cryptographic algorithms and will stop operation of the TOE when algorithms expire. Expiration dates and algorithms can be updated via software updates only (**FPT_TDC.1/NK.Zert**).

The implementation supports IPSec as required by [gemSpecKonnektor]: IKEv2 [IKEv2] without vendor-specific extensions and Main Mode Exchange are used and NAT traversal is supported.

If the TOE is configured to connect to the telematics infrastructure, this VPN connection is established automatically whenever technically possible (i.e. if the VPN concentrator can be reached over the network). In case of connection problems, retries have to wait a certain time period in order to avoid flushing of the audit log. An automatic VPN connection is not applied if the TOE is not configured to connect to the access the telematics infrastructure (e.g. in offline mode).

Establishment and termination of the VPN connections are written to the audit log.

In order to protect the central telematics infrastructure from potential attacks, communication over this VPN tunnel is restricted to specific components (by SF.DynamicPacketFilter). Currently, the only components which may transfer data over the VPN connection established to the telematics infrastructure are the application connector (AK), Fachdienste, client systems, and services responsible for name resolution (DNS), time synchronization (NTP) and TSL/CRL download.

7.1.2 SF.DynamicPacketFilter

SF.DynamicPacketFilter provides a firewall (dynamic packet filter) for network connections over the LAN and the WAN interface (**FDP_IFC.1/NK.PF**).

Firewall rules can filter packets based on (including, but not limited to) (**FDP_IFF.1/NK.PF**):

- IP address (source and destination),
- port number (source and destination),
- protocol type,
- physical interface (source or destination),
- the network interface used for ingress or egress (LAN, WAN, VPN),
- connection state.

The default rule set is designed to provide maximum protection by allowing only necessary communication (**FMT_MSA.3/NK.PF**). To prevent an intentional or unintentional undermining of the TOE security measures, the addition of new rules is allowed for the administrator (**FMT_MSA.3/NK.PF**) but is highly constrained (**FDP_IFC.1/NK.PF**). The administrator may only add rules that allow traffic between LAN and WAN. It is not possible to allow traffic that is already explicitly forbidden by the default rule set since the administrator defined rules are evaluated after the default rule set. New rules are set via LS.AK.

It is possible to select between the following two modes of operation for which there are two separate rule sets:

- **Serial/gateway mode (ANLW_ANBINDUNGS_MODUS is “InReihe”)**
  Connector is installed between local network and the internet access gateway. Internet access is therefore possible via then WAN interfaces.
- **Parallel mode (ANLW_ANBINDUNGS_MODUS is “Parallel”)**
  Connector is installed inside the local network together with the internet access gateway and other client systems. Internet access is therefore only possible via LAN interface.

Furthermore, the administrator can select how client systems are allowed to access the internet. There are the following three modes:

- **SIS (ANLW_INTERNET_MODUS is “SIS”)**
  Traffic from the LAN will be routed via VPN SIS.
- **IAG (ANLW_INTERNET_MODUS is “IAG”)**
  Traffic from the LAN will be routed via IAG. Requires that serial/gateway mode is selected.
- **None (ANLW_INTERNET_MODUS is “Keiner”)**
  Traffic from the LAN will not be routed.

The defined sets of filter rules (see refinement of **FMT_MSA.1/NK.PF**) cannot be modified or removed (**FMT_MSA.1/NK.PF**) unless policies are updated by a firmware update.

The following connections are explicitly allowed (**FDP_IFC.1/NK.PF**, **FDP_IFF.1/NK.PF**):

- All firewall rules defined in [gemSpecKonnektor, 4.2.1.1.2 Routing und Firewall] that call for traffic to be allowed.

The following connections are explicitly disallowed (**FDP_IFC.1/NK.PF**, **FDP_IFF.1/NK.PF**):

- All firewall rules defined in [gemSpecKonnektor, 4.2.1.1.2 Routing und Firewall] that call for traffic to be dropped.

The firewall rules ensure that only the following protocols are allowed when communicating with the TI: IPv4 (network layer), TCP, UDP, ICMP, ESP (transport layer).

Routing tables in the TOE ensure that outgoing WAN traffic is only routed to the telematics infrastructure via the TI VPN if the destination address is part of TI subnets or legacy subnets (“Bestandsnetze”). All other outgoing WAN traffic is routed via SIS VPN.

The packet filter also allows the TOE to identify network packets which do not belong to either a connection being established or an already established connection. Those non-well-formed packets are discarded.

The TOE keeps track of all network connections' states and relevant related information. For this the TOE uses the Linux kernel Netfilter modules.

Start-up and shutdown of the packet inspection functionality and information needed for subsequent basic intrusion prevention are stored in the audit log. Precautions are implemented in order to avoid flooding of the audit log with crafted messages in order to overwrite important events in the log.

The stateful packet inspection functionality is modelled by **FDP_IFF.1/NK.PF**.

7.1.3 SF.NetworkServices

SF.NetworkServices provides reliable time stamps to the TOE. A reference time is obtained from a trustworthy network time server of the telematics infrastructure using the VPN channel and the NTP protocol v4 (as specified in [SpecNTPv4]). A maximum deviation of 1h between the network time and the local TOE time is allowed. The TOE uses the time mainly to check the validity of certificates and record audit events. Time synchronization will continuously be performed after the TOE booted. The poll interval varies between 64 and 1024 seconds according to the NTP protocol (**FPT_STM.1/NK**).

All applications on the TOE can obtain the current time using SF.NetworkServices (**FPT_STM.1/NK**).

The time is especially needed for the implemented certificate validity check functionality. It is also distributed to client systems via the local network LS.LAN using the NTPv4 protocol.

The TOE further provides network services for client systems in the LAN:

- DHCP server for IP address configuration
- DNS server for DNS address resolution

7.1.4 SF.SelfProtection

SF.SelfProtection is responsible for protecting the TOE and data passing through it in order to impede attacks and manipulations.

Sensitive data are deleted from memory (RAM) as soon as they are no longer needed. This includes cryptographic keys, session keys and ephemeral key data during encryption and decryption as well as sensitive user data. Deletion is performed by actively overwriting the respective memory areas with zeros or pseudo-random values (**FDP_RIP.1/NK**).

The TOE can perform a suite of self-tests in order to demonstrate the integrity and correct operation of all the TOE's security functions and components. Depending on their nature, these tests will be run either on start-up, during normal operation, or both. Execution of the run-time tests can be requested by the Administrator (**FPT_TST.1/NK**). The following self-tests are implemented:

- Check for integrity of secure data storage,
- Check for integrity of stored TSF executable code,

The secure data storage stores the configuration of the TOE on an encrypted file system. The integrity of the secure data storage is ensured by a functionality that iterates all data files within the secure data storage and verifies a SHA-256 hash for each file, which is separately signed with a dedicated private RSA key located in the gSMC-K. The signature is stored in a separate file alongside the data file. Additionally, a journal file stores the path names of all data and signature files. The journal file is also signed and accompanied with a dedicated signature file. By verifying that all files from the journal file do exist and that the signature of the journal file is correct, it can be ensured that no file has been added or removed.

The integrity of the root file system in NAND-flash (part of TSF) is ensured by verifying a single SHA-512 hash over a hash database during boot-up. The hash database is created during boot-up and contains the filenames and hashes of all files[4] in the root file system. If the hash of the created database corresponds to a signed reference hash value, the check passes. The relevant scripts are stored in the initramfs (for the check during boot-up) and the root file system (for the check during operation). The reference hash value is signed using a dedicated private key belonging to the vendor. The signature is verified using the corresponding public key and RSASSA-PSS. During boot, a failed TSF integrity test will result in a halt. During operation, a failed test will force the TOE to stop all services but administration.

Integrity of the Linux kernel and the initramfs (parts of TSF) is ensured in the boot loader. The TOE verifies a RSASSA-PKCS1-1.5 signature and verifies that the SHA-256 hashes for the kernel and the initramfs correspond to the signed hashes. The public key for the signature verification is stored in the boot loader (**FPT_TST.1/NK**).

The boot loader (part of the TSF) is secured by a SHA-256 hash and a signature which are verified by the SoC in the environment of the TOE. The public key for signature verification is stored inside the boot loader. A hash value of the public key is stored in a write-once memory area of the SoC that is stored there during production. This hash is also verified.

The TSF integrity check can also be performed manually by the administrator. The TOE employs the gSMC-K for signature generation relevant for integrity checks of configuration data in the secure storage in which all TSF data are stored.

The logical properties and operations of the TOE are implemented in a way so that they resist side-channel attacks (**FPT_EMS.1/NK**). In particular, the TOE ensures that the following information is not leaked via the network interfaces:

[4] Except the file containing the signed reference hash of the hash database.

- VPN session keys,
- any used and stored key material,
- data to be protected (“zu schützende Daten der TI und der Bestandsnetze”)

The TOE enforces SELinux policies to employ an additional mandatory access control (MAC) for resources like files, directories, sockets and devices. It also employs grsecurity to deny root user access to process memory of other users. Furthermore, data areas in memory are marked as non-executable and memory addresses are randomized to protect against buffer overflow exploitations (**refinement ADV_ARC.1**).

The TOE ensures that the secure data storage is automatically encrypted (see SF.CryptographicServices).

Furthermore, the TOE permanently checks the time deviation during time synchronization using NTP according to SF.NetworkServices.

7.1.5 SF.Audit

The TOE generates audit records. Audit records are generated for the events stated in **FAU_GEN.1/NK.SecLog**.

Audit records contain at least the following information (**FAU_GEN.1/NK.SecLog**):

- Topic of the event
- date and time of the event
- event type
- severity
- subject identity (system or identifier of the corresponding “Fachmodul”)
- the outcome (success or failure) of the event if relevant
- user id of administrator for configuration changes (**FAU_GEN.2/NK.SecLog)**

Security-relevant events are stored in a permanent audit-log of the logging facility, which is adequately in size (900 MB) and cyclically overwritten (**FAU_STG.4**). There is no other mechanism for deleting or modifying log entries (**FAU_STG.1**).

The TOE provides flooding protection. Audit events that are externally triggered will be stored directly, if the same event did not occur within the last 2 seconds. If the event did already occur within the last 2 seconds, only the number of occurrence is incremented. If the same event does not occur again within 2 seconds, the event is removed from the list and will be treated as new event the next time it occurs. If an event occurs several times and the number is incremented several times the maximum time for incrementing the number is 20 seconds. 20 seconds after first occurrence of an event it will be logged again. Furthermore, if more than 80 percent of the log memory is used the TOE will inform the administrator via the display.

Logs are stored in a database file and are automatically encrypted (see SF.CryptographicServices).

7.1.6 SF.Administration

The management service defines a security role named “administrator” (**FMT_SMR.1/NK**). After the TOE made sure that users are identified as administrators (**FIA_UID.1/NK.SMR**) and authenticated in the environment of the TOE thereby using a TLS channel

(**FTP_TRP.1/NK.Admin**) they are authorized to configure various TSF data parameters and perform TSF-related actions (**FMT_MTD.1/NK**, **FMT_SMF.1/NK**):

- modify the system clock / real time clock
- manage dynamic packet filtering rules (compare SF.DynamicPacketFilter and **FMT_MSA.1/NK.PF**)
- query the audit log
- trigger the self-tests (see SF.SelfProtection)
- perform a software update

Please note that the web interface is a non-TOE part of the connector which uses the interface LS.AK to access management functionality of the TOE.

The TOE will also notify about critical states via the display (**FTP_STM.1**).

Administrators have to authenticate themselves before being able to use the services's functionality. Management is possible locally via LS.LAN and remotely via LS.WAN. For local management, the TOE provides a TLS server which is configured to support server authenticated TLS. For remote management the TOE will initiate the connection as a TLS client which supports mutual authentication. Both client and server support TLS version 1.1 and 1.2 (**FMT_SMR.1**, **FIA_UID.1/NK.SMR**).

All actions performed via the management service (login, logout, configuration modification) are stored in the audit log. The TOE uses the authentication service of the non-TOE part of the connector (**FMT_MSA.4/NK**) and enforces the authentication before establishing a trusted TLS channel (**FTP_TRP.1/NK.Admin**). For local management, the TOE assumes the role of a TLS server and provides the service via LS.LAN. For remote management, the TOE assumes the role of a TLS client. A remote management session is always invoked by the local administrator and the TOE connects to the remote administration services (RAS) via LS.VPN_SIS. In both scenarios the underlying application protocol is not part of the TOE.

This SF provides a component to update the complete device firmware including the bootloader securely via a management function. This functionality is used to update all software-based trusted IT products of the connector. Non-TOE software parts of the connector are only responsible for firmware download. On request of the administrator the update component of the TOE verifies the integrity and authenticity of update images by calculating a SHA-512 hash over the image and validating its cryptographic signature using RSASSA-PSS and the developer's public signing certificate. The certificate itself is verified against a CA certificate which is located on the root file system in the NAND-flash. Furthermore, the firmware update is only installed if the version number is in a list of allowed firmware versions ("Firmwaregruppe"). This list is part of the TOE and updated with each firmware update. (**FDP_ACC.1/Update**, **FDP_ACF.1/Update**, **FPT_ITC.1/Update**, **FPT_UIT.1/Update**).

Firmware updates always update the whole system partition (including the AK and other future software parts of the connector). First they will be installed on an alternative partition in flash memory (eMMC). After successful installation the TOE is rebooted and the newest partition becomes active. Thus it is guaranteed that the device falls back into a consistent and secure firmware state if the validation fails or the update cannot be successfully applied (installation or activation failure).

The contents of the secure storage, especially the configuration data and configuration files, as well as the logs, are preserved during the update process.

7.1.7 SF.CryptographicServices

This SF provides the following hashing algorithms (**FCS_COP.1/NK.Hash**)

- SHA-1
- SHA-256
- SHA-512

The SF also provides HMAC generation for IPsec using the following algorithms according with the above hash algorithms (**FCS_COP.1/NK.HMAC**)

- HMAC-SHA-1(-96)
- HMAC-SHA-256(-128)

Within the context of TLS (and only there) the TOE also implements the SHA-384 algorithm for certain cipher suites.

The TOE verifies x509 certificate signatures using the RSA-PKCS1-v1.5 algorithm and signatures of software updates using RSASSA-PSS signature scheme. Furthermore, the latter scheme is used to verify hashes of the secure data storage, to verify the integrity of the TSF and to verify signatures during TSL and CRL verifications (**FCS_COP.1/Sign**). The signing of hashes for the secure data storage is not performed by the TOE but the gSMC-K. The hash generation and the random number generation is performed by the TOE (**FCS_RNG.1/Hash_DRBG**).

The TOE performs the IPSec protocol (**FCS_COP.1/NK.IPsec**) and verifies signatures for the authentication of VPN concentrators during the IKEv2 protocol according to RSA-PKCS1-1.5 (**FCS_COP.1/NK.Auth**). During authentication a shared secret between the TOE and the concentrator is established with Diffie-Hellman according to IKEv2 [IKEv2] (**FCS_CKM.2/NK.IKE**). Keying material for integrity protection and encryption during IKE and ESP is generated according to [IKEv2, 2.14] using a PRF-HMAC-SHA-256 based on the established shared secret (**FCS_CKM.1/NK**). VPN traffic is encrypted by performing the ESP protocol using the generated keys (**FCS_COP.1/NK.ESP**). Integrity protection to VPN traffic is applied by calculating HMACs using dedicated generated keys (**FCS_COP.1/NK.HMAC**). The keys that are no longer needed are deleted securely by overwriting them with zeros (**FCS_CKM.4/NK**).

The TOE stores its log files and its secure data storage in the persistent memory. The log file storage and the secure storage are implemented as encrypted file systems utilizing AES with 256 bit keys in CBC mode. To guarantee unpredictable choices of initialization vectors for CBC, the Encrypted Salt-Sector IV (ESSIV) method is employed (**FCS_COP.1/Crypt.AES**). The AES key is generated during initial start of the TOE by the gSMC-K#1, encrypted using RSAES-OAEP encryption scheme and stored in the persistent storage (NAND flash). The TOE, however, is only responsible for the encryption of the key (**FCS_COP.1/Crypt.RSA**). Key generation and decryption will be performed by the gSMC-K. The key is securely erased from memory by overwriting the key with constant or pseudo-random values after usage (**FCS_CKM.4/NK**).

The TOE provides TLS version 1.1 and version 1.2 in server and client mode which is used for the secure channel between administrator and TOE. It ensures the integrity and

confidentiality of the management sessions (**FCS_COP.1/TLS**). For nonce and key generation, the TOE uses the Hash_DRBG random number generator specified in [NIST800-90A] which is seeded by the gSMC-K#2 (**FCS_RNG.1/Hash_DRBG**). However, the management web interface and the authentication of the administrator during TLS are performed by non-TOE parts of the connector. Session keys are securely erased from memory by overwriting the key with constant or pseudo-random values (**FCS_CKM.4/NK**).

7.2 Security Functions / Security Functions Requirements

The following table maps the IT security functions to the TOE security functional requirements.

	SF.VPN	SF.DynamicPacketFilter	SF.NetworkServices	SF.SelfProtection	SF.Audit	SF.Administration	SF.CryptographicServices
FTP_ITC.1/NK.VPN_TI	X						
FTP_ITC.1/NK.VPN_SIS	X						
FDP_IFC.1/NK.PF		X					
FDP_IFF.1/NK.PF		X					
FMT_MSA.3/NK.PF		X					
FPT_STM.1/NK			X			X	
FPT_TDC.1/NK.Zert	X						
FDP_RIP.1/NK				X			
FPT_TST.1/NK				X			
FPT_EMS.1/NK				X			
FAU_GEN.1/NK.SecLog					X		
FAU_GEN.2/NK.SecLog					X		
FMT_SMR.1/NK						X	
FMT_MTD.1/NK						X	
FIA_UID.1/NK.SMR						X	
FTP_TRP.1/NK.Admin						X	
FMT_SMF.1/NK						X	
FMT_MSA.1/NK.PF		X				X	
FMT_MSA.4/NK						X	
FCS_COP.1/NK.Hash							X
FCS_COP.1/NK.HMAC							X
FCS_COP.1/NK.Auth							X
FCS_COP.1/NK.ESP							X

	SF.VPN	SF.DynamicPacketFilter	SF.NetworkServices	SF.SelfProtection	SF.Audit	SF.Administration	SF.CryptographicServices
FCS_COP.1/NK.IPsec							X
FCS_CKM.1/NK							X
FCS_CKM.2/NK.IKE							X
FCS_CKM.4/NK							X
FCS_COP.1/Sign							X
FDP_ACC.1/Update						X	
FDP_ACF.1/Update						X	
FDP_ITC.1/Update						X	
FDP_UIT.1/Update						X	
FAU_STG.1					X		
FAU_STG.4					X		
FCS_COP.1/Crypt.AES							X
FCS_COP.1/Crypt.RSA							X
FCS_COP.1/TLS							X
FCS_RNG.1/Hash_DRBG							X

Table 7: Security Functions / Security Function Requirements

8 Appendix

8.1 Referenced Documents

Document ID	Document	Version (Date)
BSI-CC-PP-0046	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor Online-Rollout (Stufe 1); Bundesamt für Sicherheit in der Informationstechnik (BSI)	1.2.8 (10.02.2016)
BSI-CC-PP-0047	Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen, Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP); Bundesamt für Sicherheit in der Informationstechnik (BSI)	3.2.2 (11.04.2016)
BSI-CC-PP-0082	Common Criteria Protection Profile: Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V2, Bundesamt für Sicherheit in der Informationstechnik (BSI)	1.9 (November 18, 2014)
BSI-DSZ-CC-0916-2015	CC Zertifizierung und Anerkennung BSI-DSZ-CC-0916-2015 STARCOS 3.6 COS C1, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Gesundheitswesen_SmartCards/0916.html	07.08.2015
ESSIV	New Methods in Hard Disk Encryption, Clemens Fruhwirth, http://clemens.endorphin.org/nmihde/nmihde-A4-os.pdf	July 18, 2005
FIPS180-4	FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST	March 2012
FIPS186-2	Federal Information Processing Standards Publication 186-2: DIGITAL SIGNATURE STANDARD (DSS); National Institute of Standards and Technology (NIST)	January 27, 2000
FIPS186-4	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 186-4: Digital Signature Standard (DSS); National Institute of Standards and Technology	July 2013
FIPS197	Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES); National Institute of Standards and Technology (NIST)	November 2001
gemSpecKonnektor	Einführung der Gesundheitskarte: Konnektorspezifikation; gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH	4.10.0 (06.02.2017)

Document ID	Document	Version (Date)
gemSpecKrypt	Einführung der Gesundheitskarte: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.7.0 (28.10.2016)
gemSpecPKI	Einführung der Gesundheitskarte: Verwendung von Zertifikaten in der Telematikinfrastruktur; gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH	1.11.0 (06.02..2017)
SpecNTPv4	D. Mills, U. Delaware, J. Martin, J. Burbank, W. Kasch: Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5905 (NTPv4), http://www.ietf.org/rfc/rfc5905.txt	June 2010
CEM	Common Methodology for Information Technology Security Evaluation, http://www.commoncriteriaportal.org/thecc.html	Version 3.1 Revision 4 (September 2012)
IKEv2	C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296, http://www.ietf.org/rfc/rfc7296.txt	October 2014
CC_PART2	Common Criteria for Information Technology Security Evaluation; Part 2: Security functional components, http://www.commoncriteriaportal.org/thecc.html	Version 3.1 Revision 4 CCMB-September 2012
NIST800-90A	NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Elaine Barker and John Kelsey, Computer Security Division Information Technology Laboratory, NIST.	June 2015
MODP	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), http://www.ietf.org/rfc/rfc3526.txt	May 2003
PKCS#1	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, RFC 3447, J. Jonsson, B. Kaliski, http://www.ietf.org/rfc/rfc3447.txt	Version 2.1, February 2003
PKCS#7	Public-Key Cryptography Standards (PKCS) #7: Cryptographic Message Syntax, RFC 2315, B. Kaliski, http://www.rfceditor.org/rfc/rfc2315.txt	Version 1.5
RFC2131	R. Droms: Dynamic Host Configuration Protocol., RFC 2131, http://www.ietf.org/rfc/rfc2131.txt	March 1997
RFC2132	S. Alexander, R. Droms: DHCP Options and BOOTP Vendor Extensions, RFC 2132, http://www.ietf.org/rfc/rfc2132.txt	March 1997
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, Network Working Group, http://www.ietf.org/rfc/rfc2404.txt	November 1998

Document ID	Document	Version (Date)
RFC3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), RFC 3526 http://tools.ietf.org/html/rfc3526	Mai 2003
RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec, RFC 3602, S. Frankel, R. Glenn, S. Kelly, http://www.rfc-editor.org/rfc/rfc3602.txt	September 2003
RFC4035	R. Arends, R. Austein, M. Larson, D. Massey, S. Rose: Protocol Modifications for the DNS Security Extensions., RFC 4035, http://www.ietf.org/rfc/rfc4035.txt	March 2005
RFC4301	Security Architecture for the Internet Protocol, RFC 4301 (IPsec), S. Kent, K. Seo, http://www.ietf.org/rfc/rfc4301.txt	December 2005
RFC4303	IP Encapsulating Security Payload (ESP), RFC 4303 (ESP), S. Kent, http://www.ietf.org/rfc/rfc4303.txt	December 2005
RFC4346	The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, T. Dierks, E. Rescorla, http://www.ietf.org/rfc/rfc4346.txt	April 2006
RFC4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), RFC 4492, S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller, http://www.rfc-editor.org/rfc/rfc4492.txt	May 2006
RFC4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, RFC 4868, S. Kelly, S. Frankel, http://www.rfc-editor.org/rfc/rfc4868.txt	May 2007
RFC5246	T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol, RFC 5246, http://www.ietf.org/rfc/rfc5246.txt	Version 1.2, August 2008
RFC5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, RFC 5282, D. Black, D. McGrew, http://www.ietf.org/rfc/rfc5282.txt	August 2008
RFC5289	TLS Elliptic Curve Cipher Suites withSHA-256/384 and AES Galois Counter Mode (GCM), RFC 5289, E. Rescorla, http://www.ietf.org/rfc/rfc5289.txt	August 2008
RFC5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, M. Lochter, J. Merkle, http://www.ietf.org/rfc/rfc5639.txt	March 2010
RFC5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC, NLnet Labs, http://tools.ietf.org/html/rfc5702	October 2009

Document ID	Document	Version (Date)
RFC7027	Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), RFC 7027, J. Merkle, M. Lochter, http://www.ietf.org/rfc/rfc7027.txt	October 2013
SP800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST	December 2001
TR03116-1	Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Technische Arbeitsgruppe TR-03116.	03.12.2015 (Version 3.19)

8.2 Conventions

References to documents or chapters follow these conventions:

- Documents are referenced by the Document ID enclosed in squared brackets: [<**DocumentID**>]
- To reference a certain chapter within a document, the following syntax is used: [<**DocumentID**>, <**Chapter**>]
- Additional information after the chapter reference refers to certain sub-sections of the chapter or PP application notes.

If sections of the protection profile [BSI-CC-PP-0047] apply for this security target (ST) without modifications, references are used wherever feasible, instead of duplicating text from the PP to this ST.

For operations like assignments and refinements completed in this ST, the surrounding text of the concerned section from the PP is duplicated in this ST, the filled out operations are identified by typographical distinctions, as demanded in [CEM]:

- Refinements are set in **bold** font
- Selections are set in underlined font
- Assignments are set in *italic* font

Assignments already filled out in the protection profile [BSI-CC-PP-0047] that were copied to this ST are not highlighted; they are clearly identified in the protection profile.

Each SFR is uniquely identified by their identifier even if an SFR is iterated. Iterations of an SFR are made visible by adding different suffixes “/<suffix>” to the identifier. Please note that suffixes are also sometimes used for SFRs that are not iterated.

8.3 Terminology and Abbreviations

Abbreviation/Acronym	Expansion
AK	Application connector
Bestandsnetz	Legacy or future networks that eventually shall be connected to the TI.
CC	Common Criteria
CIFS	Common Internet File System

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
eGK	Elektronische Gesundheitskarte
ESSIV	Encrypted Salt-Sector IV
gSMC-K	Secure module for the connector
HAB	High Assurance Boot
HBA	Heilberufsausweis
ICMP	Internet Control Message Protocol
Initramfs	Initial file system which is loaded into RAM during boot-up.
IPSec	Internet Protocol Security
IAG	Internet Access Gateway
IP	Internet Protocol
JRE	Java Runtime Environment
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
KSR	Konfigurations- und Software Repository
LAN	Local Area Network
MAC	Mandatory Access Control
NAT	Network Address Translation
NK	Network connector
NTP	Network Time Protocol
OSP	Organizational Security Policy
OTG	On-The-Go
PF	Packet Filter
PP	Protection Profile
RNG	Random Number Generator
RTC	Real-Time Clock
SAK	Signature application component
SAR	Security Assurance Requirement
SELinux	Security-Enhanced Linux
SFP	Security Functional Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable ChipCard Terminal
SIM	Subscriber Identity Module
SIS	Secure Internet Service
SMC-B	Secure Module Card – Type B: Praxisausweis / Institutionsausweis
SNTP	Simple Network Time Protocol

SF	Security Function
SoC	System on a chip
SSL	Secure Sockets Layer
ST	Security Target (i.e. this document)
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UART	Universal Asynchronous Receiver/Transmitter
VODD	Verordnungsdatendienst
VPN	Virtual Private Network
VSDD	Versichertenstammdatendienst
WAN	Wide Area Network
xTV	Extended Trusted Viewer