Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0928-V2-2019

for

Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5 Version 1.5.3 Build 43

from

T-Systems International GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0928-V2-2019 (*)

Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Version 1.5.3 Build 43

from	T-Systems International GmbH
PP Conformance:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), Version 3.2.2, 11.04.2016, BSI-CC-PP-0047-2015
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2, AVA_VAN.5

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 18 October 2019

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Division

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....13
4. Assumptions and Clarification of Scope....13
5. Architectural Information....13
6. Documentation....13
7. IT Product Testing....14
8. Evaluated Configuration....15
9. Results of the Evaluation....15
10. Obligations and Notes for the Usage of the TOE....18
11. Security Target....18
12. Regulation specific aspects (eIDAS, QES)....18
13. Definitions....19
14. Bibliography....20

C. Excerpts from the Criteria....24

D. Annexes....25

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Version 1.5.3 Build 43 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0928-2018. Specific results from the evaluation process BSI-DSZ-CC-0928-2018 were re-used.

The evaluation of the product Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Version 1.5.3 Build 43 was conducted by T-Systems International GmbH. The evaluation was completed on 20 September 2019. T-Systems International GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: T-Systems International GmbH.

The product was developed by: T-Systems International GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 October 2019 is valid until 17 October 2024. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Version 1.5.3 Build 43 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the product “Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5”, Version 1.5.3 Build 43. The TOE is a software product, implementing the requirements of the Konnektor specification (in particular the Netzkonnektor specification). The Netzkonnektor is part of the overall product “MAP – Medical Access Port – Einboxkonnektor” and is delivered together with a correspondent hardware.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), Version 3.2.2, 11.04.2016, BSI-CC-PP-0047-2015 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 3 augmented by ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF1	VPN-Client providing secure communication channels
SF2	Dynamic packet filter providing user data protection
SF3	Network services providing time server, DHCP and DNS resolver functionality
SF4	Self-protection
SF5	User Authentication for administration and authentication of secure channels
SF6	Cryptographic base services as required for the authentication and encryption
SF7	Firmware-Update

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.3, 3.4 and 3.5.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5,
Version 1.5.3 Build 43

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	UEFI	S1.40.1.1	Software downloaded from servers of the developer Installed to the hardware during initial setup
2	SW	Linux-Betriebssystem	3.16 Patch 57	Software downloaded from servers of the developer Installed to the hardware during initial setup
3	SW	Netzkonnektorsoftware	1.5.3, Build 43, Ausprägung Einboxkonnektor	Software downloaded from servers of the developer Installed to the hardware during initial setup
4	DOC	Produkthandbuch T-Systems Konnektor, T-Systems International GmbH	1.30, 05.09.2019	Download from developer website SHA256: ad7dac16ae2b2c791374e305aa5ecf9bedfe7844eafd7b12269a0ae0fa686dd3
5	DOC	Schnittstellenspezifikation T-Systems Netzkonnektor Firmware-Version 1.5.1, Dokumentationsstand 1.6	04.12.2018	SHA256: abdc0b4270252461861d6c286f90d68894ba7583ff9a52236ae11ffaf440b5b3

Table 2: Deliverables of the TOE

Note that the Netzkonnektor hardware platform is only delivered together with the “Produkthandbuch T-Systems Konnektor” since the UEFI, the Linux OS and the Netzkonnektor software are delivered as part of the Netzkonnektor hardware platform during initial setup. The remaining document “Schnittstellenspezifikation T-Systems Netzkonnektor” is a technical interface specification and only provided on request.

The hardware platform containing the TOE (software and documentation) is a white plastic housing containing an Intel architecture, which provides the necessary hardware interfaces as needed for the usage of the TOE. Part of this hardware environment is the gSMC-K, which is used by the TOE for handling cryptographic keys and generating random numbers.

The requirements for the delivery are described in “Sicherheitskonzept, Sichere Lieferkette Konnektor”, [9]. The security and trustworthy of this delivery process relies on the obligations and organisational measures based on contracts between the involved parties as described in [9].

The TOE documentation “Produkthandbuch T-Systems Konnektor” is delivered in electronic form by the developer. For unique identification the SHA256 checksum of the document is given in the table 2.

The TOE can be identified using the management web interface. It will be shown as “Telekom-Konnektor EBK (TKONEBK) in der Produktversion 1.5.3 - Build: 43 - Revision: ofcda6efe2:2.2.4“.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- VPN-Client providing secure communication channels,
- Dynamic packet filter providing user data protection,
- Network services providing time server, DHCP and DNS resolver functionality,
- Self-protection,
- User Authentication for administration and authentication of secure channels,
- Cryptographic base services as required for the authentication and encryption,
- Firmware-Update.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.NK.phys_Schutz: The security measure of the environment must protect the TOE against unauthorized access,
- OE.NK.Admin_EVG: It is assumed that administrators are trustworthy and trained to operate the TOE as required by the guidance.

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The architectural description of the TOE including TOE structure and interfaces is provided in section 1.3 of the Security Target [6].

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The independent testing was partially performed using the developer's testing environment and partially using the test environment of the CLEF. The developer's testing environment implements the external infrastructure required to operate the TOE with the different setup.

Different setups including InReihe Mode and Parallel Mode being intended to be covered by the current evaluation were tested.

Independent testing approach:

The TOE was independently tested with respect to three subject areas: a) An incoming TLS connection, which the TOE provides for giving an administrator access to the management interface, b) an outgoing IKE/IPsec connection, which the TOE provides for connecting itself to the TI and SIS, and c) the packet filter, which the TOE provides for forward or deny network packets.

The TLS and IKE/IPsec tests are strictly based on the RFC conformity requirements. Testing was performed with dedicated test suites focusing on the conformity testing and secure configuration of the TLS server and IKE/IPsec connection.

The firewall tests cover the whole TCP and UDP range of the TOE's LAN and WAN interfaces, so that all firewall rules that are given by the ST are thoroughly tested.

TOE test configurations:

Regarding the TLS server functionality no special configuration is made. The TOE provides a complete configured TLS interface in its default configuration state.

Regarding the IKE functionality the TOE is configured to use special X.509 certificates so that it can connect to a VPN server, which is under complete control of the evaluators and that is not the default VPN server. This is done by replacing the default VPN server by the customized VPN server in the test environment.

Regarding the firewall tests the TOE is tested in different setup, which affects the configuration state of the TOE's packet filter. A setup is defined by a set of the following possible settings: TI VPN (up/down), SIS VPN (up/down), internet mode (IAG/SIS/off), inventory networks (on/off), online mode (on/off), connection (serial/parallel). During testing the TOE is triggered by the evaluators to dynamically switch between all possible configuration sets.

Independent test subset chosen incl. a short justification:

The TSFIs tested by independent evaluator tests are (PS1;LS6), (PS3;LS3), (PS3;LS4), (PS2;LS2), (PS3;LS5), (PS1;LS1), (PS4;LS7), and (PS5;LS8). This includes all major interface functionalities like VPN and packet filtering. Because these interfaces are most critical for the security that the TOE provides, the selection of independent evaluator tests has a good coverage of the possible attack paths an attacker can use from outside the TOE.

Developer's test subset repeated incl. a short justification:

The evaluators repeated developer tests for four important subject areas: a) The factory reset of the TOE, which deletes certain sensitive data, b) test of the secure boot process, which checks the integrity of the TOE at boot time, c) the TOE's network isolation during boot time, and d) the deletion of IPsec keys in the TOE's RAM after their usage. All those tests cover critical security functionalities of the TOE and are developer-coded implementations.

Verdict:

The overall test result is that some minor deviations were found between the expected and the actual test results. The further analysis of the evaluator did not reveal any vulnerability or violation of a Security Functional Requirement.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The Netzkonnektor is only available in one evaluated configuration comprising the versions of the software components as detailed in Table 2: TOE deliverables above.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 3 package including the class ASE as defined in the CC (see also part C of this report).
- The components ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2, AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0928-2018, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

● PP Conformance:	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), Version 3.2.2, 11.04.2016, BSI-CC-PP-0047-2015 [8]
● for the Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2, AVA_VAN.5

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
1	Authenticity	RSA signature verification with encoding RSASSA-PKCS1-1.5 using SHA-256	[RFC3447] (RSA), [FIPS180-4] (SHA)	2048	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.Auth, FTP_TRP.1/NK.Admin
2	Authentication	RSA signature creation with support of gSMC-K and verification with encoding RSASSA-PKCS1-1.5 using SHA-256	[RFC3447] (RSA), [FIPS180-4] (SHA)	2048	FCS_COP.1/NK.Auth, FTP_TRP.1/NK.Admin
3	Key Agreement	Diffie-Hellman (IKEv2) with key derivation function PRF-HMAC-SHA-{1, 256, 384, 512}	[HaC] (DH), [RFC3526] (DH-group), [FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC7296] (IKEv2)	2048 (dh-group 14) with DH exponent length = 384 bits	FCS_CKM.2/NK.IKE
4		Diffie-Hellman with TLS key derivation function	[HaC] (DH) [RFC3526] (DH-group), [FIPS180-4] (SHA), [RFC1321] (MD5), [RFC2104] (HMAC), [RFC4346] (TLSv1.1) [RFC5246] (TLSv1.2)	2048 (dh-group 14) with DH exponent length = 384 bits	FTP_TRP.1/NK.Admin
5		EC Diffie-Hellman with TLS key derivation function	[SEC1] (ECDH) [RFC4492] (ECC for TLS), [RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2)	Key sizes corresponding to the used elliptic curves P-{256, 384} [FIPS 186-4], brainpoolP{256, 384, 512}r1 ([RFC5639], [RFC7027])	FTP_TRP.1/NK.Admin
6	Confidentiality	AES in CBC mode	[FIPS197] (AES), [RFC3602] (AES-CBC)	256	FCS_COP.1/NK.ESP, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE
7		AES in CBC mode	[FIPS197] (AES), [RFC3602] (AES-CBC)	128, 256	FTP_TRP.1/NK.Admin
8	Integrity	HMAC with SHA-	[FIPS180-4] (SHA),	160, 256,	FCS_COP.1/NK.HMAC

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
		{1, 256, 384} (IKE, IPsec)	[RFC2104] (HMAC), [RFC2404], [RFC4868], [RFC7296] (IKEv2)	384	
9		HMAC with SHA-{1, 256, 384} (TLS)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2)	160, 256, 384	FTP_TRP.1/NK.Admin
10	Authenticated Encryption	AES in GCM mode (TLS)	[SP 800-38D] (GCM), [RFC5288] (GCM for TLS), [RFC5116] (AEAD), [RFC5246] (TLSv1.2)	128, 256	FTP_TRP.1/NK.Admin
11	Trusted Channel	IKEv2, IPsec	[RFC7296] (IKEv2) [RFC4301] (IPsec), [RFC4303] (ESP), [14]		FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS
12		TLS v1.1 and v1.2	[RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2), [15]		FTP_TRP.1/NK.Admin

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to [gemSpec_Kon], [gemSpec_Krypt] and [TR03116-1] the algorithms in table 3 are suitable for the corresponding purpose.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column 'Security Level above 100 Bits' of the following table with 'no' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comment
1	Authenticity	RSA signature verification with encoding RSASSA-PKCS1-1.5 using SHA-256	[RFC3447] (RSA), [FIPS180-4] (SHA)	4096	yes	FDP_ITC.1/ NK.FWUpdate

Table 4: TOE cryptographic functionality (firmware update)

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

In addition, the following recommendations and directions should be followed when using the TOE:

The TOE is only able to provide its security services under the following conditions:

- The TOE is configured with mandatory TLS and mandatory client authentication.
- The connected client systems verify the authenticity of the Netzkonnektor when using services and receiving events.
- The user is able to identify whether a client system connection is secure.

The TOE user shall only operate the TOE under the conditions above. A violation of these conditions is considered a vulnerability of the TOE in the operational environment. In this case, the TOE user is responsible to counter the vulnerability.

The Netzkonnektor supports different setups. The main setups are “Parallel” Mode, “InReihe” Mode and Offline Mode. The “InReihe” Mode is recommended since it provides a higher protection of the connected LAN, refer to section 4.7 of Produkthandbuch T-Systems Konnektor [11].

The user has to contact the developer for the final removal from service as required in section 4.13.2 of Produkthandbuch T-Systems Konnektor [11].

For the active VPN connections using IPsec no countermeasures against statistic traffic analysis are implemented.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CLEF	Commercial Licensed Evaluation Facility
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IKE	Internet Key Exchange
IAG	Internet Access Gateway
IPsec	Internet Protocol Security
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIS	Secure Internet Service
ST	Security Target
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
WAN	Wide Area Network

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0928-V2-2019, Version 2.14, 06.09.2019, Sicherheitsvorgaben für den Medical Access Port_1BK_1.0.0 Netzkonnektor Bauform Einboxkonnektor 1.5, Dokumentversion 2.13, T-Systems International GmbH

[7] Evaluation Technical Report, Version 2.1, 06.09.2019, Evaluation Technical Report BSI-DSZ-CC-0928-V2, T-Systems International GmbH, (confidential document)

[8] Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP), Version 3.2.2, 11.04.2016, BSI-CC-PP-0047-2015

[9] Sicherheitskonzept, Sichere Lieferkette Konnektor, T-Systems International GmbH, Version 1.0.1, 05.04.2018

[10] Configuration list for the TOE (confidential document):

EVG-Config-List: binary_config_list_sha256_Rev_2bc8b5ae4.txt, device_config_list_sha256_CNN-1.5.3.40_Rev_b0123e90e4_filtered.txt, extern_config_list_sha256_CNN-1.5.3.40_Rev_54edeba01_filtered.txt, konnektor-crypto_config_list_sha256_Rev_81a0025_filtered.txt, konnektor-doc_config_list_sha256_Rev_3eecfe2_filtered.txt, konnektor-site_config_list_sha256_Rev_ae35964_filtered.txt, konnektor-test_config_list_sha256_Rev_688ca2b_filtered.txt, patched_source_config_list_sha256_Rev_29bc5eab1.txt, ptxdist_2016.06.1_config_list_sha256_CNN-1.5.2.37_Rev_3804c05e_filtered.txt, T-Systems International GmbH, Stand: 06.09.2019

[11] Guidance documentation for the TOE:

Produkthandbuch T-Systems Konnektor, T-Systems International GmbH, Version 1.30, 05.09.2019

Schnittstellenspezifikation T-Systems Netzkonnektor Firmware-Version 1.5.1, Dokumentationsstand 1.6, T-Systems International GmbH, 4.12.2018

[12] Implementation standards:

[HaC] A. Menezes, P. van Oorschot und O. Vanstone. Handbook of Applied Cryptography. CRCPress, 1996.

[FIPS180-4] FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST, March 2012

[FIPS186-4] FIPS PUB 186-4 Digital Signature Standard (DSS), NIST, July 2013

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results

[FIPS197] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[PKCS#1] B. Kaliski: PKCS #1: RSA Encryption, Version 2.1, RFC 3447, Version 2.2, October 2012

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm ", April 1992.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, „HMAC: Keyed-Hashing for Message Authentication", February 1997

[RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH, Network Working Group, November 1998

[RFC3268] Chown, P., Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS), June 2002

[RFC3447] J. Jonsson, B. Kaliski: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. February 2003

[RFC3526] More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003

[RFC3602] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003

[RFC4301] Security Architecture for the Internet Protocol (IPsec), S. Kent, K. Seo, December 2005

[RFC4303] IP Encapsulating Security Payload (ESP), RFC 4303 (ESP), S. Kent, December 2005

[RFC4346] The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, E. Rescorla, April 2006

[RFC4492] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller, May 2006

[RFC4868] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, S. Kelly, S. Frankel, May 2007

[RFC5116] An Interface and Algorithms for Authenticated Encryption, D. McGrew, January 2008

[RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, Network Working Group

[RFC5639] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, J. Merkle, March 2010

[RFC5996] The Internet Key Exchange Protocol Version 2 (IKEv2), D. Harkins, D. Carrel, September 2010

[RFC7027] Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), J. Merkle, M. Lochter, October 2013

[RFC7296] C. Kaufman et. al, Internet Key Exchange Protocol Version 2 (IKEv2), October 2014

[SEC1] Daniel R. L. Brown: SEC 1: Elliptic Curve Cryptography, May 21. 2009, Version 2.0

[SP800-38A] Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001

[SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[SP800-38D] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[SP800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90A, Revision 1, June 2015.

[13] Application standards:

[gemSpec_Kon] Einführung der Gesundheitskarte: Spezifikation Konnektor, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 4.11.1, 27.04.2017

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.9.0, 19.12.2017

[TR03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für die eCard-Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Technische Arbeitsgruppe TR-03116, Version 3.20, 21.09.2018

[14] RFC Conformity Report IKE, Evaluation Facility T-Systems International GmbH, Version 2.0, 15.07.2019 (confidential document)

[15] RFC Conformity Report TLS, Evaluation Facility T-Systems International GmbH, Version 2.0, 15.07.2019 (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report