Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0950-V2-2018

for

KoCoBox MED+ Netzkonnektor v1.3.4

from

KoCo Connector GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0950-V2-2018 (*)

KoCoBox MED+ Netzkonnektor
v1.3.4

from	KoCo Connector 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, AVA_VAN.5, ALC_FLR.2

SOGIS
Recognition Agreement
for components up to
EAL 4

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 4

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, 13 February 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

This page is intentionally left blank.

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 are 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: http://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 KoCoBox MED+ Netzkonnektor, v1.3.4 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0950-2017. Specific results from the evaluation process BSI-DSZ-CC-0950-2017 were re-used.

The evaluation of the product KoCoBox MED+ Netzkonnektor, v1.3.4 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 10.11.2017. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: KoCo Connector 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 13 February 2018 is valid until 12 February 2023. Validity can be re-newed by re-certification.

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

[5] Information Technology Security Evaluation Facility

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 KoCoBox MED+ Netzkonnektor, v1.3.4 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] KoCo Connector GmbH
Dessauer Str. 28/29
10963 Berlin

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 KoCoBox MED+ Netzkonnektor, Version 1.3.4. 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”). 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 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, AVA_VAN.5, ALC_FLR.2.

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
SF.VPN	VPN Client
SF.DynamicPacketFilter	Firewall with stateful packet inspection
SF.NetworkServices	DHCP, DNS and NTP networking services
SF.SelfProtection	Self-tests, attack counter mechanisms, deletion of confidential data and non-emanation of data
SF.Audit	Secure audit
SF.Administration	Secure administration channels and update mechanism
SF.CryptographicServices	Cryptographic services required by other functionality

Table 1: TOE Security Functionalities

For more details please refer to the Security Target, 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:

KoCoBox MED+ Netzkonnektor, v1.3.4

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	FW	Firmware Image	1.3.4	Either: Initially included in the e-Health Konnektor product KoCoBox MED+ or as a software update package via KSR process.
2	DOC	KoCoBox MED+ Allgemeine Gebrauchsanleitung Purpose: Guide for the end user	1.3.4	Delivered with the delivery package of the product KoCoBox MED+.
3	DOC	Administratorhandbuch KoCoBox MED+ für die Komponente Netzkonnektor Purpose: Guide for the Administrator	1.3.4	Delivered to the authorized service technician, who installs the TOE at the end user site. The service technician performs administration tasks.
4	DOC	Guidance addendum documentation („Ergänzungen zum Administratorhandbuch KoCoBox MED+ für die Komponente Netzkonnektor“)	1.0.3	See 3.

Table 2: Deliverables of the TOE

TOE Delivery Process

The TOE is delivered to the end user as part of the product KoCoBox MED+. An authorized service technician will deliver the product to the end user. The service technician installs the product KoCoBox MED+ within the premises of the end user. Prior to installation, the service technician must be identified via a photo ID by the end user. The service technician is trained, instructs the end user and provides security advice.

TOE Identification

The TOE can be identified within the KoCoBox MED+ follows:

- Display
  - OK to enter the Menu
  - Select 4 for Version

  Identification: Firmwareversion 1.3.4, Hardwareversion 2.0.0
- Web Administration Interface:
  - Check the entry Firmware on the status page of the Web Administration Interface Identification: Produktversion: 1.3.4:2.0.0

The hardware is not part of the TOE and therefore not relevant for the TOE identification.

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:

- Security Audit,
- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- Trusted Path/Channels.

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 TOE must be physically protected against unauthorized access,
- OE.NK.Admin_EVG: The TOE must be configured by a trustworthy and well trained administrator, who operates the TOE according to the guidance.

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

5. Architectural Information

A high level description of the IT product and its major components can be found in the Security Target [6], chapter 1.4.7.

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

Developer's Test

TOE test configurations:

The Security Target [6] has not identified different TOE variants or configurations. Only the released TOE is referenced. Nevertheless, the developer uses two firmware variants for blackbox and for whitebox testing. For test configuration, the developer used two preparative and four test configurations. Environment simulation is also used.

TOE test environment configurations:

The assumptions and objectives for the operational environment stated in [6] are not applicable for testing. Nevertheless, the developer uses five test environment configurations which cover a large amount of the real environment.

Testing approach:

- Coverage and depth tests are done together.
- The test specifications give mappings to the tested TSFI(s), SFR(s), subsystem(s), and module(s).
- Different testing approaches are used:
  - Code analysis,
  - Blackbox tests:
    - Manual,
    - Automatic.
  - Whitebox tests:
    - Manual,
    - Automatic.
- The test descriptions comprise (inter alia):
  - Pre conditions: preparative steps,
  - Test steps: Core test steps,
  - Post conditions: clearance steps to tidy up before the next test.
- Testing results: The developer’s testing efforts have been proven sufficient to demonstrate that the TSFIs and subsystems perform as expected.

All test cases in each test scenario were run successfully on the TOE and they all passed according to their expected result.

Evaluator Tests

TOE test configurations:

The evaluation body used the same test configurations and test environment as the developer during functional testing.

Test subset chosen:

The evaluation body chose to repeat and inspect a broad set of developer tests. Effectively more than 50% of the tests were covered.

Interface selection criteria:

The evaluation body chose to broadly cover the existing interfaces without specific restrictions.

Interfaces tested:

Services at the LAN and the WAN ports were considered during testing.

Developer tests performed:

The evaluation body chose to perform a random sampling with the intent to broadly cover the existing interfaces and the implemented security functionality.

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results.

Penetration Testing

The configuration defined in the ST was tested. Furthermore, different TOE variants were used during penetration testing to verify different mechanisms.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential High was actually successful.

- Penetration testing approach:

  The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms. The areas were prioritized with regard to various factors, e.g. attack surface, estimated flaw likelihood, developer testing coverage and detectability of flaws during developer testing.

  Medium and high areas were guaranteed to be penetration tested, with a stronger emphasis on high priorities. Low priorities were also considered during penetration, but could be less emphasized, if developer tests were found to be sufficient.

  The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluators chose the analytical approach. Analytical activities were especially applied in the areas Update, Random Number Generation and Hardening Mechanisms. Combined approaches were also applied.

- TOE test configurations:

  The TOE was delivered by the developer in two different configurations: A release TOE and a special ATE variant. The ATE variant is an enhanced variant of the software running on the same hardware and using the same smart cards (gSMC-K). The ATE configuration is used to enable tests that are not possible due to security mechanisms applied in the release TOE. The differences between release TOE and the ATE variant are clearly defined. Therefore, two goals can be achieved:

  (1) Perform detailed testing using the target hardware and smart card,

  (2) ensure that the test results of the ATE variant are also valid for the TOE.

  During the evaluation process, the TOE was updated several times. Penetration tests were performed with versions 1.3.0 and 1.3.4. The developer provided a change analysis which documents, the differences between the versions. The evaluation body did not identify changes that would render the 1.3.0 test results invalid for 1.3.4. The most important tests were conducted with the final version 1.3.4.

- Attack scenarios having been tested:

  The evaluation body considered security analysis and penetration testing in the following areas:

  - VPN Connections,
  - Administration Connections,
  - Random Number Generation,
  - Update,
  - Hardening Mechanisms,
  - Filtering and Routing,
  - Self-Protection,
  - Network Services,
  - Audit.

- Tested security functionality:

  The evaluator ensured that all areas listed above are tested. Actually, the evaluation body used a more detailed list during the analysis and testing. The penetration testing was then conducted based on priorities as described above. Therefore, a complete coverage of security functional testing based on technical areas of concern is performed.

- Verdict for the sub-activity:

  The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment provided that all measures required by the developer are applied.

Summary of Test Results and Effectiveness Analysis

The TOE testing did not reveal vulnerabilities exploitable by an attacker with high attack potential.

8. Evaluated Configuration

The evaluation results are only valid for the single configuration defined in the Security Target [6].

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, AVA_VAN.5, ALC_FLR.2 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-0950-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on

- Support of new TLS cipher suites with elliptic curve ECDHE key exchange and GCM mode of operation,
- Update of software components, and
- Detail implementation changes according to changes of the gematik specification.

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, AVA_VAN.5, ALC_FLR.2

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 cryptographic algorithms are used by the TOE to enforce its security policy:

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
1	Authenticity	RSA signature verification with encoding RSASSA-PSS and RSASSA-PKCS1-1.5 using SHA-256	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	FPT_TDC.1/NK.Zert, FCS_COP.1/TLS, FCS_COP.1/Sign
2	Authentication	RSA signature creation with support of gSMC-K and verification with encoding RSASSA-PKCS1-1.5 using SHA-256 (sha256withRSAEncryption)	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	FCS_COP.1/NK.Auth, FCS_COP.1/TLS
3	Key Agreement	Diffie-Hellman (IKEv2) with key derivation function	[HaC] (DH) [RFC2526] (dh-group), [FIPS180-4] (SHA),	2048 (dh-group 14) with DH exponent	FCS_CKM.2/NK.IKE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comment
		PRF-HMAC-{SHA-1, SHA-256}	[RFC2104] (HMAC), [RFC5996] (IKEv2)	length ≥ 384 bits	
4		Diffie-Hellman with TLS key derivation function	[HaC] (DH) [RFC2526] (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	FCS_COP.1/TLS
5		EC Diffie-Hellman with TLS key derivation function	[SEC1] (ECDH), [FIPS180-4] (SHA), [RFC1321] (MD5), [RFC2104] (HMAC), [RFC4346] (TLSv1.1) [RFC5246] (TLSv1.2)	Key sizes corresponding to the used elliptic curves P-{256,384} [FIPS186-4] and brainpoolP{256,384}r1 [RFC7027]	FCS_COP.1/TLS
6	Confidentiality	AES in CBC	[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	[FIPS197] (AES), [RFC3602] (AES-CBC)	128, 256	FCS_COP.1/TLS
8	Integrity	HMAC with SHA-{1, 256} (IKE, IPsec)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC2404], [RFC4868], [RFC5996] (IKEv2)	160, 256	FCS_COP.1/NK.HMAC
9		HMAC with SHA-1 (TLS)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC2404], [RFC4868], [RFC5996] (IKEv2)	160	FCS_COP.1/TLS
10	Trusted Channel	IKEv2, IPsec	[RFC5996] (IKEv2) [RFC4301] (IPsec), [RFC4303] (ESP)		FTP_ITC.1/NK.VPN_TI
11		IKEv2, IPsec	[RFC5996] (IKEv2) [RFC4301] (IPsec), [RFC4303] (ESP)		FTP_ITC.1/NK.VPN_SIS
12		TLS v1.1 and v1.2	[RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2)		FTP_TRP.1/NK.Admin

Table 3: TOE cryptographic functionality

The strength of the 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 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-PSS using SHA-256	[PKCS#1] (RSA), [FIPS180-4] (SHA)	4096	yes	FCS_COP.1/ Sign for x.509 certificate verification
2		RSA signature verification with encoding RSASSA-PSS using SHA-512	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	yes	FCS_COP.1/ Sign for firmware update signatures verification

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.

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. Definitions

12.1. 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
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DH	Diffie-Hellman
EAL	Evaluation Assurance Level
eGK	Elektronische Gesundheitskarte
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
gSMC-K	Secure module for the connector
HBA	Heilberufsausweis
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KSR	Konfigurations- und Software-Repository
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
NK	Network connector
PKI	Public Key Infrastructure
PP	Protection Profile
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SFP	Security Function Policy

SFR	Security Functional Requirement
SIS	Secure Internet Service
SMC-B	Secure Module Card – Type B: Praxisausweis / Institutionsausweis
ST	Security Target
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network
WAN	Wide Area Network

12.2. 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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012

Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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-0950-V2-2018, Version 1.8.5, 18 October 2017, KoCoBox MED+ Netzkonnektor Common Criteria Certification Security Target, KoCo Connektor GmbH

[7] Evaluation Technical Report, Version 2, 10 November 2017, TÜV Informationstechnik 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] Configuration list for the TOE (confidential documents):

- KoCo-Box_Med+_NK_Konfiguration Items N-Design (ALC_CMS.3 + ADV_IMP.1)_v1.3.4.xlsx, n-design GmbH, Version 1.3.4
- Konfiguration_items_osc_(ALC_CMS.3+ADV_IMP.1)_v1.3.4.xlsx, os-cillation GmbH, Version 1.3.4

[10] Guidance documentation for the TOE:

- KoCoBox MED+ Allgemeine Gebrauchsanleitung, KoCo Connektor GmbH, Version 1.3.4, 25 October 2017
- Administratorhandbuch KoCoBox MED+ für die Komponente Netzkonnektor, KoCo Connektor GmbH, Version 1.3.4, 8 November 2017
- Ergänzungen zum Administratorhandbuch KoCoBox MED+ für die Komponente Netzkonnektor, KoCo Connektor GmbH, Version 1.0.3, 13 October 2017

[11] Implementation standards:

[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
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[Brainpool] ECC Brainpool Standard Curves and Curve Generation. Version 1.0, October 19, 2005.

[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] 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), 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

[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

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

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

[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), RFC 7027, J. Merkle, M. Lochter, http://www.ietf.org/rfc/rfc7027.txt, October 2013

[SEC1] SEC 1: Elliptic Curve Cryptography, Certicom Research. Version 2.0, 21.05.2009, http://www.secg.org/download/aid-780/sec1-v2.pdf

[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

[12] Application standards:

[gemSpec_Kon] Einführung der Gesundheitskarte: Konnektorspezifikation, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 4.6.0, 26.08.2014

[gemSpec_Krypt] Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 2.3.0, 17.06.2014

[TR03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für die eCard-Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Technische Arbeitsgruppe TR-03116, 30.01.2014 (Version 3.18)

This page is intentionally left blank.

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://www.commoncriteriaportal.org/cc/

This page is intentionally left blank.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report