Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1068-V5-2024

for

KoCoBox MED+ Konnektor, Version 5.5.12

from

KoCo Connector 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 9582-5400

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1068-V5-2024 (*)

Gesundheitswesen: Konnektoren

KoCoBox MED+ Konnektor
Version 5.5.12

from	KoCo Connector GmbH
PP Conformance:	Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-02, Version 1.6.1, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2
valid until:	18 December 2029

SOGIS
Recognition Agreement

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

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 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.

Bonn, 19 December 2024
For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] 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]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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.sogis.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 under SOGIS-MRA for all assurance components selected.

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.

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

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

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+ Konnektor, Version 5.5.12 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1068-V4-2023. Specific results from the evaluation process BSI-DSZ-CC-1068-V4-2023 were re-used.

The evaluation of the product KoCoBox MED+ Konnektor, 5.5.12 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 27 November 2024. 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 product was developed by: 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 19 December 2024 is valid until 18 December 2029. Validity can be renewed 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+ Konnektor, Version 5.5.12 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+ Konnektor, Version 5.5.12. The TOE is the base software part of the product KoCoBox MED+. This product is a decentral component, called “e-Health Konnektor” in the context of the German health care telematics infrastructure. The TOE consists of three parts, the network connector (NK) (German: “Netzkonnektor”), the application connector (AK) (German: “Anwendungskonnektor”) and a healthcare specific module (VSDM) (German: “Fachmodul VSDM”).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-02, Version 1.6.1, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI) [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 AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapters 6.2 and 6.3. 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	Description
SF.VPN	VPN Client
SF.DynamicPacketFilter	Firewall with stateful packet inspection
SF.NetworkServices	DHCP, DNS and NTP networking services
SF.SelfProtection/NK	Mechanisms of self-protection of the TOE: • Key destruction and residual information protection for NK, • Self-tests of TSF and TSF data for NK, and • Mitigation of attacks
SF.Audit/NK	Secure audit service for NK
SF.Administration/NK	Secure administration channels and update mechanism
SF.CryptographicServices/NK	Cryptographic services required by other security functionality of the TOE
SF.CryptographicServices/AK	Cryptographic services for AK
SF.TLS	TLS service for secure communication channel
SF.Authentication	Identification and authentication service
SF.AccessControl	Access control service for connect requests
SF.CardTerminalMgmt	eHealth card terminal management
SF.SmartCardMgmt	Smart card management
SF.SignatureService	Signature Creation and Validation Application (SCaVA)

SF.EncryptionService	Document encryption service
SF.SecureStorage	Secure data storage service
SF.VSDM	Versichertenstammdaten (VSD) management service
SF.Administration/AK	Administration management service for AK
SF.SelfProtection/AK	Mechanisms of self-protection of the TOE: • Verification management of TSL, CRL etc., • Secure state upon failure, • Self-tests of TSF and TSF data for AK, and • Key destruction and residual information protection for AK
SF.Audit/AK	Secure audit service for AK
SF.VAU	VAU protocol functionality
SF.SGD	SGD protocol functionality

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapters 7.1 and 7.2.

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 3.2, 3.3 and 3.4.

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+ Konnektor, Version 5.5.12

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1.	FW	KoCo MED+ Firmware	5.5.12	Initially delivery as firmware included within the KoCo MED+ hardware. Downloadable as firmware image from developer URL or via KSR process as a software update package.
2.	PDF	Administratorhandbuch KoCoBox	5 (2024-07-17)	Download via an internet URL from developer.

		MED+		
	SHA-256: 99e3fe717e67af25e6e48e0b54fa619fa84112cea08b57559e4d286ee9102d5a			
3.	PDF	Ergänzungen zum Administratorhandbuch	1.3.4 (2024-07-17)	Download via an internet URL from developer.
	SHA-256: 6f66420fac43c2ce0466c92b127c172bfd51d9228c27a1f87027aa8486a782a7			
4.	Booklet	Allgemeine Gebrauchsanleitung KoCoBox MED+	1.3.8 (2018-05-01)	Delivered with the delivery package of the TOE.
	SHA-256: 2912d4d5eaa5113edd856e2a53e25f0f14dc820a0d4fce81ebb903ab67d20a7a			
5.	Booklet	Allgemeine Gebrauchsanleitung KoCoBox MED+	2.1 (2022-03-01)	Delivered with the delivery package of the TOE.
	SHA-256: 7c89ada88b58aff3629ab5253bd93fcb7fbc1ecda7cf3ce4675aac06ed145890			
6.	PDF	JSON-Managementschnittstelle der KoCoBox Med+	3.22 (2024-02-19)	Delivered on demand by email.
	SHA-256: ddda22af9bcd665f389daf64e26ef39f1bd77b361570ad6ff0c578ea149d229f			
7.	PDF	Konnektor Security Guidance Fachmodule NFDM, AMTS und ePA	4.3 (2024-06-20)	Delivered on demand by email.
	SHA-256: af0a8ee1b030470f1c1de284d591155495a26606c1f5fa84b2aac399dff15b74			
8.	HTML	Konnektor API für Fachmodule Javadoc (File Konnektor-FM-API-VERSION-javadoc.tar.gz)	7.15.1 (2024-01-30)	Delivered on demand by email.
	SHA-256: 09c2172ee95f215c916c538919b984f8fcb09d5af397cf05912705e2065ea93f			

Table 2: Deliverables of the TOE

2.1. TOE Delivery Process

The TOE is delivered by an authorized service technician to the end user. The service technician installs the TOE 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.

2.2. TOE Identification

The TOE can be identified as follows:

- Display:

  → OK to enter the Menu,

  → Select 4 for Version.

Identification:

- G3 variant:
  - Firmwareversion: 5.5.12,
  - Hardwareversion: 2.0.0.
- G4 variant:
  - Firmwareversion: 5.5.12,
  - Hardwareversion: 4.0.0.

- Web Administration Interface:

  → Check the entry Firmware on the status page of the Web Administration Interface.

  Identification:

  - G3 variant:

    Produktversion: 5.5.12:2.0.0.
  - G4 variant:

    Produktversion: 5.5.12:4.0.0.

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, and
- TOE Access.

Specific details concerning the above mentioned security policies can be found in chapters 6.2 and 6.3 of the Security Target [6].

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 shall be physically protected against unauthorized access.

- OE.NK.Admin_EVG: The TOE shall be configured by a trustworthy and well trained administrator who operates the TOE according to the guidance.
- OE.NK.PKI: If the administrator manually uploads TSLs and CRLs in the admin web GUI. Such files shall only be taken from a trustworthy source.
- When the TOE is stolen or no longer under the control of the owner, the owner shall initiate the blocking of the TOE and its gSMC-Ks.
- OE.NK.Betrieb_CS: The client systems shall be secured by the CS administrators. The owner of the CS shall only operate CS software that follows the developer specific CS implementation guide “Ergänzungen zum Administratorhandbuch KoCoBox MED+”.
- OE.AK.Admin_EVG: The administrators shall keep passwords and secrets confidential.
- OE.AK.Admin_Konsole: The admin shall use a secure web browser and not store password.
- OE.AK.Kartenterminal: For the security of the TOE only certified eHealth card terminals shall be used for communication with the TOE.
- OE.AK.SecAuthData, OE.AK.Clientsystem, OE.AK.ClientsystemKorrekt: The owner of the CS shall only operate CS software that follows the developer specific CS implementation guide “Ergänzungen zum Administratorhandbuch KoCoBox MED+” [10].
- OE.AK.phys_Schutz: The TOE must be physically protected against unauthorized access.
- OE.AK.Personal: Only qualified and trustworthy personnel are allowed to use and maintain the TOE.

Details can be found in the Security Target [6], chapters 4.3 and 4.4.

5. Architectural Information

A high level description of the IT product and its major components can be found in the Security Target [6], chapter 1.4.6.

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

7.1. Developer's Test according to ATE_FUN

TOE test configurations

The Security Target [6] has identified two different TOE variants:

- G3 TOE variant with G3 hardware (i.MX 6 CPU), and
- G4 TOE variant with G4 hardware (i.MX 8 CPU).

For both TOE variants, the developer uses two firmware variants for blackbox and for whitebox testing. For test configuration, the developer used one preparative and four test configurations. Environment simulation is also used. Only the released firmware for both TOE variants is referenced.

TOE test environment configurations

The assumptions and objectives for the operational environment stated in the Security Target [6] are not applicable for testing. Nevertheless, the developer uses seven 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, and
    - Automatic,
  - Whitebox tests:
    - Manual, and
    - Automatic.
- The test descriptions comprise (inter alia)
  - Pre conditions: preparative steps,
  - Test steps: core test steps with expected results, and
  - 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.

7.2. Independent Testing according to ATE_IND

TOE variants and test configurations

The evaluation body used the same TOE variants, 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.

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.

7.3. Penetration Testing according to AVA_VAN

Overview

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 variants based on their hardware generation (G3 (i.MX 6 CPU) and G4 (i.MX 8 CPU)). For each hardware generation a release TOE and a special ATE variant were delivered for testing. 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 variant 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 tests results of the ATE variant are also valid for the TOE.

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

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,
- TOE Services and Network Services, and
- Audit.

Tested security functionality

The evaluator ensured that all areas listed above are tested. Actually, the evaluation body used a more detailed list during 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 defined by the protection profile was actually successful in the TOE’s operational environment provided that all measures required by the developer are applied.

7.4. Summary of Test Results and Effectiveness Analysis

The TOE testing did not reveal vulnerabilities exploitable by an attacker with the attack potential as defined by the protection profile.

8. Evaluated Configuration

The TOE is delivered in two different variants. The two variants are associated with the two hardware platforms G3 and G4. Both of these TOE variants are evaluated configurations of the TOE. The evaluation results are only valid for the configurations defined in the Security Target [6], chapter 1.4.8.

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 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 AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, 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-1068-V4-2023, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on:

- LZV – update of the gSMC-K certificates in case of anticipated expiration,
- End of support for HMAC-SHA-1 algorithm in IKE/IPSec protocol (PRF & integrity),
- End of support of TLS_ECDHE_RSA_WITH_AES_*_CBC_SHA in TLS protocol,
- LDAP authentication mode can be configured, and
- Hardening of XML parser.

The evaluation has confirmed:

- PP Conformance: Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-02, Version 1.6.1, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI) [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 AVA_VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1, 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 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 120 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).

The following tables give an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following tables with '*no*' achieves a security level of lower than 120 Bits (in general context) only. Note that the column "Security Level" given in tables 3 and 4 refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind.

No.	**Purpose**	**Cryptographic Mechanism**	**Implementation Standard**	**Key Size in Bits**	**Security Level above 120 Bits**	**Comments**
1.	Authenticity	Firmware update file signature verification using RSASSA-PSS with SHA-512	[RFC8017] (RSA), [FIPS180-4] (SHA)	2048	No	FDP_ACC.1/ AK.Update, FDP_ACF.1/ AK.Update, FDP_UIT.1/ AK.Update, FCS_COP.1/ NK.SigVer
2.	Authenticity	FW update X.509 certificate verification using RSASSA-PSS with SHA-256	[RFC8017] (RSA), [FIPS180-4] (SHA)	4096	Yes	FDP_ACC.1/ AK.Update, FDP_ACF.1/ AK.Update, FDP_UIT.1/ AK.Update, FCS_COP.1/ NK.SigVer

Table 3: Additional TOE cryptographic functionality (NK)

No.	**Purpose**	**Cryptographic Mechanism**	**Implementation Standard**	**Key Size in Bits**	**Security Level above 120 Bits**	**Comments**
1.	Key Generation	Config Data Backup Encryption: Key generation for PBKDF2	[SP800-132] (PBKDF2)	ca. 124	Yes	FMT_MTD.1/ AK.eHKT_Abf
2.	Authenticat	Config Data	[FIPS197] (AES),	ca. 124,	Yes	FMT_MTD.1/

	ed Encryption	Backup Encryption: AES-GCM (AES256-GCM) encryption and decryption using PBKDF2	[SP800-38D] (GCM), [RFC5084] (AES-GCM in CMS), [SP800-132] (PBKDF2)	AES-GCM-ENC: 256, AES-GCM-DEC: 256, Authentication tag: 128		AK.eHKT_Abf, FMT_MTD.1/ AK.eHKT_Mod
3.	Authenticity	Config Data Backup Signature: Signature generation with SHA-256 and support of SMC-B, and RSA signature verification with signature scheme RSASSA-PSS with SHA-256	[RFC8017] (RSA), [FIPS180-4] (SHA), [RFC5652] (CMS)	1900 – 8192	Yes (for keys >= 2800)	FMT_MTD.1/ AK.eHKT_Abf, FMT_MTD.1/ AK.eHKT_Mod
4.	Key Generation	Generation and hashing of user passwords using PBKDF2WithHmacSHA512	[SP800-132] (PBKDF2), [FIPS180-4] (SHA)	--	Yes	FIA_SOS.1/ AK.Passwörter, FIA_SOS.1/ AK.CS.Passwörter

Table 4: Additional TOE cryptographic functionality (AK)

The following tables give 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	Implementation Standard	Key Size in Bits	Comments
1.	Authenticity	RSA signature verification using signature scheme RSASSA-PKCS1-v1_5 with SHA-256	[RFC8017] (RSA), [FIPS180-4] (SHA)	2048	FPT_TDC.1/NK.Zert, FPT_TDC.1/NK.TLS.Zert, FCS_COP.1/NK.SigVer
2.	Authenticity	RSA signature verification of CRL and OCSP responses using signature scheme RSASSA-PKCS1-v1_5 with SHA-{256, 384, 512}	[RFC8017] (RSA), [FIPS180-4] (SHA)	2048 – 8192	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer
3.	Authenticity	RSA signature verification of TSL using signature	[RFC8017] (RSA), [FIPS180-4] (SHA),	2048	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer,

		scheme RSASSA-PSS with SHA-256	[XMLSig2]		FPT_TDC.1/NK.TLS.Zert
4.	Authenticity	RSA signature verification of CRL and OCSP responses using signature scheme RSASSA-PSS with SHA-{256, 384, 512}	[RFC8017] (RSA), [FIPS180-4] (SHA)	2048 – 8192	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer, FPT_TDC.1/NK.TLS.Zert
5.	Authenticity	ECDSA signature verification of TSL using signature scheme ECDSA with SHA-256	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), [RFC5639] (brainpool)	brainpoolP256r1	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer, FPT_TDC.1/NK.TLS.Zert
6.	Authenticity	ECDSA signature verification of CRL and OCSP responses using signature scheme ECDSA with SHA-{256, 384, 512}	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), [RFC5639] (brainpool)	brainpoolP{256, 384, 512}r1	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer, FPT_TDC.1/NK.TLS.Zert
7.	Authentication	RSA and ECDSA signature creation with support of gSMC-K using signature scheme RSASSA-PKCS1-v1_5 and ECDSA with SHA-256 and signature verification with RSASSA-PKCS1-v1_5 and ECDSA with SHA-256	[RFC8017] (RSA), [FIPS180-4] (SHA), [RFC5639] (brainpool), [FIPS186-4] (ECDSA)	RSA: 2048 and ECC: brainpoolP256r1	FCS_COP.1/NK.Auth
8.	Authentication	RSA and ECDSA signature creation for TLS with support of gSMC-K or SMC-B or imported or self-created signing keys using signature scheme RSASSA-PKCS1-v1_5 and ECDSA with SHA-{256, 384} and signature verification with RSASSA-PKCS1-v1_5 and ECDSA with SHA-{256, 384}	[RFC8017] (RSA), [FIPS180-4] (SHA), [FIPS186-4] (ECDSA, P-256, P-384), [RFC7027] (ECC TLS)	RSA: 2048 – 8192 and ECC: P{256, 384}, brainpoolP{256, 384}r1	FCS_COP.1/NK.TLS.Auth
9.	Key Agreement	Diffie-Hellman (IKEv2) with key	[RFC2631] (DH),	2048 (DH-	FCS_CKM.2/NK.IKE,

		derivation function PRF-HMAC-SHA-256	[RFC3526] (dh-group), [FIPS180-4] (SHA), [TR-02102-3_2022] / [RFC7296] (IKEv2, PRF_HMAC_SHA-256)	group 14) with DH exponent length ≥ 384 bits, Derived Session Key Length: 256	FCS_CKM.1/NK
10.	Key Agreement	Diffie-Hellman with TLS key derivation function	[RFC2631] (DH), [RFC3526] (dh-group), [FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC3268] (DHE_RSA), [RFC5246] (TLSv1.2)	2048 (DH-group 14) with DH exponent length ≥ 384 bits	FCS_CKM.1/NK.TLS
11.	Key Agreement	EC Diffie-Hellman with TLS key derivation function	[SEC1-2009] (ECDH), [FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4492] (ECDHE_RSA), [RFC5246] (TLSv1.2), [FIPS186-4] (P-256, P-384), [RFC7027] (Brainpool)	P{256, 384}, brainpoolP{256, 384}r1	FCS_CKM.1/NK.TLS
12.	Key Generation	Key generation for RSA and ECC key in X.509 and PKCS#12 (RSA) or PEM (ECC) format using FCS_RNG.1/Hash_DRBG for usage in client system authentication	[RFC5280] (X.509), [RFC7292] (PKCS#12), [RFC4055] (supporting [RFC5280]), [FIPS186-4, Method B.3.3] (Key-Gen), [RFC7027] (ECC Brainpool), [TR-03111] (ECC key generation)	RSA: 2048, 3072 and ECC: brainpoolP256r1, secp256r1	FCS_CKM.1/NK.Zert
13.	Confidentiality	Symmetric encryption and decryption for VPN: AES in CBC	[FIPS197] (AES), [RFC3602] (AES-CBC), [RFC4303] (ESP), [RFC4301] (IPsec)	256	FCS_COP.1/NK.ESP, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE
14.	Confidentiality	Symmetric encryption and decryption for	[FIPS197] (AES), [RFC3602] (AES-	128, 256	FCS_COP.1/NK.TLS.AES

		TLS: AES in CBC	CBC), [RFC3268] (AES-TLS with DH), [RFC4492] (AES-TLS with ECDH)		
15.	Confidentiality	Symmetric encryption and decryption AES in CBC with ESSIV	[FIPS197] (AES), [SP800-38A] (CBC), [ESSIV]	256	FCS_COP.1/Storage.AES
16.	Integrity	HMAC value generation and verification with SHA-{1, 256} (IKE, IPsec)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC4868] (HMAC-SHA256), [RFC7296] (IKEv2)	256	FCS_COP.1/NK.HMAC
17.	Integrity	HMAC value generation and verification with SHA-{1, 256, 384} (TLS)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC5246] (TLS v1.2)	160, 256, 384	FCS_COP.1/ NK.TLS.HMAC
18.	Authenticated Encryption	AES-128 and AES-256 in GCM mode for TLS 1.2	[FIPS197] (AES), [RFC3268] (AES-TLS), [SP800-38D] (GCM), [RFC5289] (AES-GCM-TLS), [RFC5116] (AEAD)	128, 256	FCS_COP.1/NK.TLS.AES
19.	Trusted Channel	IKEv2, IPsec	[RFC7296] (IKEv2), [RFC4301] (IPsec), [RFC4303] (ESP)	--	FTP_ITC.1/NK.VPN_TI, FTP_ITC.1/NK.VPN_SIS
20.	Trusted Channel	TLS v1.2	[RFC5246] (TLSv1.2)	--	FTP_TRP.1/NK.Admin, FDP_ITC.2/NK.TLS
21.	Key Generation	Key generation for RSA and ECC key in X.509 and PEM format using FCS_RNG.1/Hash_DRBG for usage in Konnektor authentication	[RFC5280] (X.509), [RFC4055] (supporting [RFC5280]), [FIPS186-4, Method B.3.3] (Key-Gen), [RFC7027] (ECC Brainpool), [FIPS186-4] (P-256), [TR-03111] (ECC key generation)	RSA: 2048, 3072 and ECC: P256, brainpoolP256r1	FCS_CKM.1/NK.Auth
22.	Key Agreement	Elliptic Curve Diffie-Hellman (IKEv2) with key derivation function PRF-HMAC-SHA-256	[SEC1-2009] (ECDH), [FIPS180-4] (SHA), [TR-02102-3_2022] / [RFC7296] (IKEv2, PRF_HMAC_SHA-	brainpoolP256r1, Derived Session Key Length: 128,	FCS_CKM.2/NK.IKE, FCS_CKM.1/NK

			256)	256	
23.	Authenticated Encryption	AES-128 and AES-256 in GCM mode for VPN	[FIPS197] (AES), [SP800-38D] (GCM), [RFC4106] (AES-GCM in IPSec), [RFC5282] (AEAD in IKEv2), [RFC4303] (ESP), [RFC4301] (IPsec)	128, 256	FCS_COP.1/NK.ESP, FCS_COP.1/NK.IPsec, FCS_CKM.2/NK.IKE
24.	Authenticity	RSA signature verification of TSL using signature scheme RSASSA-PSS with SHA-256	[RFC8017] (RSA), [FIPS180-4] (SHA)	2048 - 8192	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer, FPT_TDC.1/NK.TLS.Zert
25.	Authenticity	RSA and ECDSA signature verification of O_Zertifikat_gSMC-K certificates using signature scheme RSASSA-PSS with SHA-256 and ECDSA with SHA-{256, 384, 512}	[RFC8017] (RSA), [FIPS180-4] (SHA), [FIPS186-4] (ECDSA), [RFC7027] (ECC Brainpool)	RSA: 2048 and ECC: brainpoolP{256, 384, 512}r1	FPT_TDC.1/NK.Zert, FCS_COP.1/NK.SigVer, FPT_TDC.1/NK.TLS.Zert

Table 5: TOE cryptographic functionality (NK)

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Comments
1.	Authenticity	PadES based signature generation with SHA-256 and support of HBA, SMC-B, and RSA signature verification using signature schemes RSASSA-PKCS1-v1_5 and RSASSA-PSS with SHA-{256, 384, 512}, and ECDSA signature verification with SHA-256 for QES and nonQES	[PAdES], [PAdES-BL], [ISO_32000-1] (PDF), [RFC8017] (RSA), [RFC7027] (ECC Brainpool), [TR-03111] (ECDSA), [FIPS186-4] (P-256), [FIPS180-4] (SHA)	RSA: 1900 – 8192 (QES), 2048 – 8192 (nonQES) and ECDSA: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	FDP_DAU.2/AK.QES, FDP_DAU.2/AK.Sig, FCS_COP.1/AK.PDF.Sign, FCS_COP.1/ AK.PDF.SigPr, FCS_COP.1/AK.SHA, FCS_COP.1/ AK.SigVer.SSA, FCS_COP.1/ AK.SigVer.PSS, FCS_COP.1/ AK.SigVer.ECDSA
2.	Authenticity	XadES based signature generation including XML	[XMLSig2], [XAdES], [XAdES-BL],	RSA: 1900 – 8192 and	FDP_DAU.2/AK.QES, FCS_COP.1/ AK.XML.Sign, FCS_COP.1/

		signed SAML2 assertions with SHA-256 and support of HBA, SMC-B, and RSA signature verification using signature scheme RSASSA-PKCS1-v1_5 with SHA-{256, 384, 512}, and RSA signature verification using signature scheme RSASSA-PSSwith SHA-{256, 384, 512}, and ECDSA signature verification with SHA-{256, 384, 512} for QES	[RFC8017] (RSA), [RFC5639] (ECC Brainpool), [FIPS186-4] (P-256), [TR-03111] (ECDSA), [FIPS180-4] (SHA), [SAML2]	ECDSA: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	AK.XML.SigPr, FCS_COP.1/AK.SHA, FCS_COP.1/AK.SigVer.SSA, FCS_COP.1/AK.SigVer.PSS, FCS_COP.1/AK.SigVer.ECDSA
3.	Authenticity	CadES based signature generation with SHA-256 and support of HBA, SMC-B, and RSA signature verification using signature schemes RSASSA-PKCS1-v1_5 and RSASSA-PSS with SHA-{256, 384, 512}, and ECDSA signature verification with SHA-{256, 384, 512} for QES and nonQES	[RFC5652] (CMS), [CAdES], [CAdES-BL], [RFC8017] (RSA), [RFC5639] (ECC Brainpool), [FIPS186-4] (P-256), [TR-03111] (ECDSA), [FIPS180-4] (SHA)	RSA: 1900 – 8192 (QES), 2048 – 8192 (nonQES), and ECDSA: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1	FDP_DAU.2/AK.QES, FDP_DAU.2/AK.Sig, FCS_COP.1/AK.CMS.Sign, FCS_COP.1/AK.CMS.SigPr, FCS_COP.1/AK.SHA, FCS_COP.1/AK.SigVer.SSA, FCS_COP.1/AK.SigVer.PSS, FCS_COP.1/AK.SigVer.ECDSA
4.	Authenticity	ECDSA signature verification with SHA-256 (ecdsa-with-Sha256)	[gemSpec_Krypt] (VAU protocol), [gemSpec_SGD_ePA] (SGD protocol), [FIPS186-4] (ECDSA), [RFC5639] (brainpool), [FIPS180-4] (SHA)	brainpoolP256r1	FCS_COP.1/VAU.ECDSA, FCS_COP.1/SGD.ECDSA
5.	Authenticity	Hash functionality SHA-1 (OCSP) and SHA-256 (other hash use cases in VAU and SGD protocols)	[FIPS180-4] (SHA)	--	FCS_COP.1/VAU.Hash, FCS_COP.1/SGD.Hash, FIA_SOS.1/AK.Passwörter, FIA_SOS.1/AK.CS.Passwörter

6.	Key Agreement	ECDH with key derivation function HKDF with SHA-256	[gemSpec_Krypt] (VAU protocol), [SP800-56A] (ECDSA), [RFC5639] (brainpool), [RFC5869] (HKDF), [FIPS180-4] (SHA)	brainpoolP256r1	FCS_CKM.1/VAU
7.	Key Generation	Key generation for hybrid encryption	[SP800-133, Kp. 6.1] (Direct Key-Gen)	256	FCS_CKM.1/AK.AES
8.	Authenticated Encryption	CMS document hybrid encryption and decryption[7] using encryption schemes (RSAESOAEP or ECIES) with AES-GCM, and XML document hybrid encryption and decryption[8] using encryption scheme RSAESOAEP with AES-GCM	[XMLEnc] (XML), [RFC5652] (CMS), [RFC8017] (RSA), [FIPS197] (AES), [SP800-38D] (GCM), [RFC5084] (AES-GCM in CMS), [SEC1-2009] (ECIES), [TR-03111] (ECKA (for ECIES)), [TR-03110-3] (KDF (for ECIES)), [FIPS180-4] (SHA-256 (for ECIES)), [SP800-38A] (CBC (for ECIES)), [SP800-38B] (CMAC (for ECIES))	RSA-ENC: 2048 – 8192 and RSA-DEC: depending on cards and ECIES: brainpoolP256r1 and AES-GCM-ENC: 256 and AES-GCM-DEC: 128, 192, 256 and Authentication tag: 128, AES-CBC-256 and 8 byte CMAC	FCS_COP.1/AK.XML.Ver, FCS_COP.1/AK.CMS.Ver, FCS_COP.1/AK.XML.Ent, FCS_COP.1/AK.CMS.Ent, FCS_CKM.4/AK, FCS_COP.1/AK.AES, FCS_COP.1/AK.ECIES
9.	Authenticated Encryption	AES-256 in GCM mode	[FIPS197] (AES), [SP800-38D] (GCM)	256 and Authentication tag: 128	FCS_COP.1/VAU.AES
10.	Authenticated Encryption	ECIES based authenticated hybrid encryption and decryption for SGD protocol	[gemSpec_SGD_ePA] (SGD protocol), [SEC1-2009] (ECIES),	ECC: brainpoolP256r1 and AES-	FCS_COP.1/SGD.ECIES

[7] The asymmetric decryption is performed within the smart cards, e.g. HBA.

[8] The asymmetric decryption is performed within the smart cards, e.g. HBA.

			[SP800-56A] (ECDH), [RFC5869] (HKDF), [FIPS180-4] (SHA), [FIPS197] (AES), [SP800-38D] (GCM)	GCM: 256 bit key, 128 bit tag	
11.	Trusted Channel	VAU protocol	[gemSpec_Krypt]	--	FTP_ITC.1/VAU
12.	Trusted Channel	SGD protocol	[gemSpec_SGD_ePA]	--	FTP_ITC.1/SGD
13.	Authenticity	RSA signature verification of BNetzA-VL using signature scheme RSASSA-PKCS1-v1_5 with SHA-{256, 384, 512}	[RFC8017] (RSA), [FIPS180-4] (SHA)	1900 – 8192	FCS_COP.1/ AK.SigVer.BNetzA-VL
14.	Authenticity	RSA signature verification of BNetzA-VL using signature scheme RSASSA-PSS with SHA-{256, 384, 512}	[RFC8017] (RSA), [FIPS180-4] (SHA)	1900 – 8192	FCS_COP.1/ AK.SigVer.BNetzA-VL
15.	Authenticity	ECDSA signature verification of BNetzA-VL using signature scheme ECDSA with SHA-{256, 384, 512}	[FIPS186-4] (ECDSA), [FIPS180-4] (SHA), [RFC5639] (brainpool)	brainpoolP{256, 384, 512}r1	FCS_COP.1/ AK.SigVer.BNetzA-VL

Table 6: TOE cryptographic functionality (AK)

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 [12] the algorithms are suitable for the corresponding purpose. An explicit validity period is not given.

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 aspects need to be fulfilled when using the TOE:

- The administrator shall only configure the TOE by using the functionality of the web administration interface as presented in the recommended web browser.
- The TOE is only able to provide its security services under the following conditions:
  - The TOE is configured with mandatory TLS and mandatory client system authentication.
  - The connected client systems verify the authenticity of the Konnektor when using services and receiving events.
  - The user is able to identify whether a client system connection is secure.
  - The user operates technical peers of the TOE, which use AES-GCM cipher suites for TLS connection and avoids AES-CBC cipher suites for any connections.
- 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 TOE 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 Chapter 5 of [10].
- "The TOE user may use the button “Zufallspasswort generieren” to generate secure passwords for the client systems."
- Implementers of client systems shall oblige to the requirements for client systems as stated in [10].
- 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. Definitions

12.1. Acronyms

AEAD	Authenticated Encryption with Associated Data
AIS	Application Notes and Interpretations of the Scheme
AK	Application connector
AMTS	Arzneimitteltherapiesicherheit
API	Application Programming Interface

BNetzA-VL	Vertrauensliste der Bundesnetzagentur
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
CadES	CMS Advanced Electronic Signatures
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation
CMS	Cryptographic Message Syntax
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
DH	Diffie-Hellman
DOC	Documentation
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FW	Firmware
gSMC-K	Secure module for the connector
GUI	Graphical User Interface
HBA	Heilberufsausweis
HMAC	Keyed-Hash Message Authentication Code
HW	Hardware
IKE	Internet Key Exchange Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JSON	JavaScript Object Notation

KSR	Konfigurations- und Software-Repository
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
LZV	Laufzeitverlängerung
NK	Network connector
NTP	Network Time Protocol
PP	Protection Profile
RNG	Random Number Generator
SAK	Signaturanwendungskomponente
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIS	Secure Internet Service
SMC-B	Secure Module Card – Type B: Praxisausweis / Institutionsausweis
ST	Security Target
SW	Software
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSL	Trust-Service Status List
VAU	Vertrauenswürdige Ausführungsumgebung
VPN	Virtual Private Network
VSDM	Versichertenstammdatenmanagement
WAN	Wide Area Network
XadES	XML Advanced Electronic Signatures
XML	Extensible Markup Language

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 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[9] https://www.bsi.bund.de/AIS

[9] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

[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-1068-V5-2024, Version 4.10, 02.09.2024, Security Target Konnektor, KoCoBox MED+ Konnektor Version 5.5.12, KoCo Connector GmbH

[7] Evaluation Technical Report, Version 1, 15.11.2024, Evaluation Technical Report Summary (ETR Summary), TÜV Informationstechnik GmbH, (confidential document)

[8] Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098-V3-2021-MA-02, Version 1.6.1, 15.03.2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] Configuration lists for the TOE (confidential documents)

Configuration Items os-cillation for G3 HW Generation, v5.5.12, KoCo Connector GmbH. SHA-1: 348c28e91786a8a68d7452278a516fdb79eb4987

Configuration Items n-design, v7.15.1, KoCo Connector GmbH. SHA-1: 9eb0802d0745941e1517430ed809436266f1a67c

Configuration Items KoCo Hamburg for G4 HW Generation, v5.5.12, KoCo Connector GmbH. SHA-1: db4346cc849d31018e4db0388055733a3d5adcf8

[10] Guidance documentation for the TOE:

Administratorhandbuch KoCoBox MED+, KoCo Connector GmbH, Version 5, 17.07.2024

Ergänzungen zum Administratorhandbuch KoCoBox MED+, KoCo Connector GmbH, Version 1.3.4, 17.07.2024

Allgemeine Gebrauchsanleitung KoCoBox MED+ (G3), KoCo Connector GmbH, Version 1.3.8, 01.05.2018

Allgemeine Gebrauchsanleitung KoCoBox MED+ (G4), KoCo Connector GmbH, Version 2.1, 01.03.2022

JSON-Managementschnittstelle der KoCo-Box MED+, KoCo Connector GmbH, Version 3.22, 19.02.2024

Konnektor Security Guidance Fachmodule NFDM, AMTS und ePA, KoCo Connector GmbH, Version 4.3, 20.06.2024

Konnektor API für Fachmodule Javadoc, KoCo Connector GmbH, Version 7.15.1, 30.01.2024

[11] Implementation standards:

[CAdES] Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733, V1.7.4, 2008-07, European Telecommunications Standards Institute (ETSI).

[CAdES-BL] Electronic Signatures and Infrastructure (ESI) - CAdES Baseline Profile - ETSI Technical Specification TS 103 173, V2.1.1, 2012-03, European Telecommunications Standards Institute (ETSI).

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

[ESSIV] New Methods in Hard Disk Encryption, Clemens Fruhwith.

[FIPS180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), 2015-08, National Institute of Standards and Technology (NIST).

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07, National Institute of Standards and Technology (NIST).

[FIPS197] Federal Information Processing Standards Publication PUB 197, Advanced Encryption Standard (AES), Updated Version, 2023-05-09, National Institute of Standards and Technology (NIST).

[ISO_32000-1] Document management — Portable document format — Part 1: PDF 1.7, Version 2008-7-1, 2008, Adobe Systems Incorporated.

[PAdES] Advanced Electronic Signature Profiles, Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles, ETSI Technical Specification, V1.2.1, 2010-07, European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI).

[PAdES-BL] PAdES Baseline Profile, ETSI Technical Specification, V2.2.2, 2013-04, European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI).

[RFC2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, 1997-02, Network Working Group, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2104.txt.

[RFC2631] RFC 2631 - Diffie-Hellman Key Agreement Method, 1999-06, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2631.txt.

[RFC3268] RFC 3268 - Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), 2002-06, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc3268.txt.

[RFC3526] RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003-05, Network Working Group, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc3526.txt.

[RFC3602] RFC 3602 - The AES-CBC Cipher Algorithm and Its Use with IPsec, 2003-09, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc3602.txt.

[RFC4055] RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2005-06, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4055.txt.

[RFC4106] RFC 4106 - The Use of Galois/Counter Mode(GCM) in IPsec Encapsulating Security Payload (ESP), 2005-06, J. Viega and D. McGrew, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4106.txt.

[RFC4301] RFC 4301 - Security Architecture for the Internet Protocol (IPsec), 2005-12, S. Kent, K. Seo, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4301.txt.

[RFC4303] RFC 4303 - IP Encapsulating Security Payload (ESP), 2005-12, S. Kent, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4303.txt.

[RFC4492] RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), 2006-05, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4492.txt.

[RFC4868] RFC 4868 - Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, 2007-05, S. Kelly, S. Frankel, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4868.txt.

[RFC5084] RFC 5084 - Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), 2007-11, Housley, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5084.txt.

[RFC5116] RFC 5116 - An Interface and Algorithms for Authenticated Encryption, 2008-01, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5116.txt.

[RFC5246] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, 2008-08, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5246.txt.

[RFC5280] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (ProposedStandard), 2008-05, 2008-05, Cooper, et al., The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5280.txt.

[RFC5282] RFC 5282 - Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol. RFC5282 (Proposed Standard), 2008-08, D. Black and D. McGrew, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5282.txt.

[RFC5289] RFC 5289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), 2008-08, Network Working Group, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5289.txt.

[RFC5639] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03, M. Lochter (BSI), J. Merkle (secunet Security Networks), The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5639.txt.

[RFC5652] RFC 5652 - Cryptographic Message Syntax (CMS), IETF Trust and the persons identified as the document authors, 2009-09, The Inter-net Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5652.txt.

[RFC5869] RFC 5869 - HMAC-based Extract-and-Expand Key Derivation Function (HKDF), 2010-05, H. Krawczyk and P. Eronen, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5869.txt.

[RFC7027] RFC 7027 - Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), 2010-06, J. Merkle (secunet Securi-ty Networks), M. Lochter (BSI), The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc7027.txt.

[RFC7292] RFC 7292 - PKCS #12: Personal Information Exchange Syntax v1.1 (Informational), 2014-07, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc7292.txt.

[RFC7296] RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2), 2014-10, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc7296.txt.

[RFC8017] RFC 8017 - PKCS #1: RSA Cryptography Specifications, Version 2.2, 2016-11, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc8017.txt.

[SAML2] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, 2015-09-08, OASIS Security Services Technical Committee.

[SEC1-2009] SEC1: Elliptic Curve Cryptography - Standards for Efficient Cryptography, Version 2.0, 2009-05-21, Daniel Brown, Hrsg (Certicom Corp).

[SP800-132] NIST Special Publication 800-132 – Recommendation for Password-Based Key Derivation, 2010-12, National Institute of Standards and Technology (NIST).

[SP800-133] NIST Special Publication 800-133 – Recommendation for Cryptographic Key Generation, 2012-12, National Institute of Standards and Technology (NIST).

[SP800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation – Methods and Techniques, 2001-12, National Institute of Standards and Technology (NIST).

[SP800-38B] NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation – The CMAC Mode for Authentication, Updated Version, 2016-10-06, National Institute of Standards and Technology (NIST).

[SP800-38D] NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007-11, National Institute of Standards and Technology (NIST).

[SP800-56A] NIST Special Publication 800-56A – Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptog-raphy, 2018-04, National Institute of Standards and Technology (NIST).

[TR-02102-3_2022] BSI - Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2022-01, 2022-01-24, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03110-3] Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 3: Common Specification. Technische Richtlinie BSI TR-03110-3, Version 2.21, 2016-12-21, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[TR-03111] Elliptic Curve Cryptography, Technische Richtlinie BSI TR-03111, Version 2.10, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[XAdES] XML Advanced Electronic Signatures (XAdES): Technical Specication XML Advanced Electronic Signatures (XAdES); ETSI Technical Specication TS 101 903, Version 1.4.2, 2010, European Telecommunications Standards Institute (ETSI).

[XAdES-BL] Electronic Signatures and Infrastructure (ESI); XAdES Baseline Profile; ETSI Technical Specification TS 103 171, Version 1.4.2, 2010, European Telecommunications Standards Institute (ETSI).

[XMLEnc] XML Encryption Syntax and Processing, Version 1.1, 2013-04, W3C Recommendation.

[XMLSig2] XML Signature Syntax and Processing (Second Edition), 2008-06-10, IETF/W3C XML Signature Working Group, https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

[12] Further documents:

[gemSpec_Kon] Spezifikation Konnektor, Version 5.18.0, 28.11.2022, gematik.

[gemSpec_Krypt] Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.26.0, 09.03.2023, gematik.

[gemSpec_SGD_ePA] Spezifikation Schlüsselgenerierungsdienst ePA, Version 1.5.0, 31.01.2022, gematik.

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

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 detailed 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