Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1071-V6-2023

for

SE 5000-8.1, Version A

from

Stoneridge Electronics AB

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1071-V6-2023 (*)

SE 5000-8.1
Version A

SOGIS
Recognition Agreement

from	Stoneridge Electronics AB
PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.15, 6 June 2021, BSI-CC-PP-0094-V2-2021
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5
valid until:	9 July 2028

Common Criteria

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

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

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

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

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 10 July 2023

For the Federal Office for Information Security

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

Matthias Intemann L.S.
Head of Section

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.

[4] Proclamation of the Bundesministerium des Innern und für Heimat 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 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 SE 5000-8.1, Version A has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1071-V5-2021. Specific results from the evaluation process BSI-DSZ-CC-1071-V5-2021 were re-used.

The evaluation of the product SE 5000-8.1, Version A was conducted by Deutsche Telekom Security GmbH. The evaluation was completed on 7 July 2023. Deutsche Telekom Security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Stoneridge Electronics AB

The product was developed by: Stoneridge Electronics AB.

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 10 July 2023 is valid until 9 July 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product SE 5000-8.1, Version A 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] Stoneridge Electronics AB
Gustav III:s Boulevard 26
SE-169 73 Solna
Sweden

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 a second generation vehicle unit (VU) in the sense of [13] (Annex 1C), intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores human user activities data in its internal data memory. It also records human user activities data in tachograph cards. The VU outputs data to a display, to a printer and to external devices.

The TOE is connected to a motion sensor from which it obtains the vehicle's motion data. Information from the motion sensor is corroborated by vehicle motion information derived from a GNSS receiver, and optionally by other sources independent of the motion sensor.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Digital Tachograph - Vehicle Unit (VU PP) Version 1.15, 6 June 2021, BSI-CC-PP-0094-V2-2021 [12].

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 4 augmented by ATE_DPT.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 9. 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
TSF.ACTIVITIES	Keeps control of all activity done by the user and ensures that user data is written to VU and card. It also enables/disables functionality depending on user (driver, workshop, control and company). It detects event related to user behaviour.
TSF.BIST	Runs test to ensure that tampering of memory is detected. It also run test to ensure correctness of Composite TOE.
TSF.CARD	Controls all secure communication with tachograph card. Ensures that a secure communication channel exists and is used for communication. Detect Card related events. Control start-up /shutdown of card. Ensure that temporary stored cryptographic keys (used for card communication) is removed when not needed.
TSF.CASING	Consists of a physical box that gives protection from tampering and dust/water according to IP class. The enclosure of the VU is made in such way that it is not possible to open once sealed. It is considered as a closed box. The case ensures that the VU will not be physically modified without detection.
TSF.CONFIG	Enforces calibration function modifying parameters.
TSF.CRYPTO	Uses the TOE Platform's hardware co-processors for basic DES, AES, RSA, and ECC operations and the TOE Platform's True Random Number Generator for generation of random numbers. Access to RSA and ECC operations uses a TOE Platform Crypto Library.
TSF.DSRC	Controls all communication and creates messages.
TSF.DOWNLOAD	Provides services for extracting data from the VU (download of data) with corresponding signatures. When data is downloaded a validation is also

TOE Security Functionality	Addressed issue
	done to ensure correctness of data within the download.
TSF.ERRORMGR	Ensures that reported Event/faults are stored in a correct way.
TSF.FRAMEWORK	Handle start-up of the TOE in a controlled way.
TSF.GNSS	Controls all communication received from GNSS satellites including supervision of signal loss.
TSF.IPC	Mange the internal communication. It acts as a gateway and only forwards approved messages.
TSF.MMI	Controls input and output of user by using buttons, display and a printer.
TSF.MMU	Keeps control of memory allocation/deallocation used to ensure that no external interfaces are available at the same time as the secret keys.
TSF.PSI	Is the supervisor for external power to TOE. It also ensures that there is time enough to store relevant data in case of a power loss.
TSF.STORAGE	Is a supporting all TSF:s in storing data and keep control of replacement of oldest data.
TSF.SPEED	Controls all secure communication with motion sensor. Ensures that a secure communication channel exists and is used for communication. Detect Motion sensor related events. Control initialization of motion sensor communication. Ensure that events/faults reported by motion sensor is stored within VU.
TSF.TAM	Synchronise the system and keep control of mode of operation to ensure that all relevant data are stored and functions are enabled/disabled.
TSF.TIME	Provides the VU with a correct time.
TSF.UPDATE	Ensures validation of software package prior of usage.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 10.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 6.1.1. 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], chapter 6.2 to 6.4.

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:

SE 5000-8.1, Version A

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1		Digital Tachograph (Vehicle Unit) SE5000-8.1, Version A	900773R xxRyy with software 1014 Please note that the last five characters shows the customer specific revision of the VU, reflected here by xxRyy.	Separate unit in a sealed case
2	DOC	Workshop Manual SE5000-8 Smart Tachograph, Version 9000-103767P_01 10, Stoneridge Electronics AB SHA256: 7dd8d41cb2c9da0f1fab19a2fd38ac6a2f31f1a988e2fc02d047435f3440e3ef [11]	Version 9000-103767P_01 10	paper copies and/or electronically adobe pdf documents
3	DOC	Control Manual SE5000-8 Smart Tachograph, Version 9000-103766P_01 09, Stoneridge Electronics AB SHA256: 860fe2a3204c44ca313f49ae922ece6a9a7e058cdefbbbac830eb3ef4e963f95 [10]	Version 9000-103766P_01 09	paper copies and/or electronically adobe pdf documents
4	DOC	Driver and Company Manual SE5000-8 Smart Tachograph, Version 9000-103765P_01 07, Stoneridge Electronics AB SHA256: be25cc9dbe0137ad02a14ff869b511c46957479bf5a74970a821d33ab344af4e [9]	Version 9000-103765P_01 07	paper copies and/or electronically adobe pdf documents

Table 2: Deliverables of the TOE

The complete SE5000 digital tachograph (VU) will be transported to the customer after manufacturing including personalization and approval. The manuals will be sent together with the VU, separately or be available for download from the Stoneridge Internet homepage depending on the customer's demands. Ordinary delivery routines specified from the logistic department will be used for transport from the manufacturing site in Örebro to the customer.

Before delivery the VU is sealed using a tamper label and the required key material is stored in the VU. The customer is responsible for the transport from the gate at the site in Örebro and will, maybe through a transporting company, confirm their reception of the delivery by signing a waybill.

The customer shall check the received tachograph (VU) in accordance to the checklist in the user documentation (Workshop Manual SE5000-8 Smart Tachograph, Version 9000-103767P_01 10, Stoneridge Electronics AB) to ensure that the VU is an original tachograph.

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, proof of origin, user data protection, identification and authentication, security management, protection of the TSF, trusted channel, cryptographic support.

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. Details can be found in the Security Target [6], chapter 7.2.

5. Architectural Information

The TOE consists of a hardware box including the following subsystems: GNSS receiver, display & visual warning, printer, driver and co-driver card readers, operator inputs, power supply, data memory and TSF subsystem.

There is one subsystem that is relevant for security, TSF subsystem, which is fully represented as modules. The remaining subsystems that make up the TOE are required for TSF subsystem’s interactions with the environment (users, tachograph cards, sensor, GNSS satellites, remote external detection communication facility, external tools etc.) and have no relevance for security and are not further described. The data memory is also considered not relevant to security because the stored user data’s integrity and authenticity is upheld by TSF subsystem.

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 tests:

All properties/characteristics of the TSFI as described in the functional specification, the TSF subsystem behaviour and the interaction among TSF subsystems as described in the design documentation, and all interfaces to the SFR-enforcing modules have been tested by the developer. The TOE responded to the tests as expected.

Evaluator tests:

The evaluators spent adequate testing effort for the desired resistance of the TOE against attackers with high attack potential. The evaluators analysed the test specification and verified based on sampling that the specification has been correctly implemented in the test scripts. In addition the used this analysis for:

- creating ideas for independent evaluator tests,

- ensuring that the test environment delivers correct test results, and
- repeating developer tests as well as carrying out independent tests.

Independent tests:

Independent tests were identified based on the developer tests already available. The developer tests have been compared with the ST, the functional specification, and the design specification in order to define supplementary tests. Furthermore, the evaluator devised tests based on a the tests already performed by the developer. The evaluators conducted independent testing at the developer's site. The evaluator tests have been carried out against the following TOE configurations: The TOE was brought in every production control state. A simulator for the motion sensor was used. Furthermore every card type (Driver card, workshop card, control card, and company card) was used. According to EAL4, functional testing was performed down to the depth of SFR-enforcing module interfaces. The tests showed that the TOE behaves as expected in all configurations that are considered as part of the evaluation. No deviation was found between the expected and the actual test results. The depth of testing is adequate for the evaluation assurance level chosen (EAL4+). The TOE has successfully passed independent testing.

Penetration tests:

Penetration tests were performed using the TOE as delivered to the customer. In addition the developer delivers dedicated prepared test samples for the casing and the security control to support the penetration testing in the evaluator’s lab. All configurations of the TOE covered by the current evaluation were tested. On the basis of the methodical vulnerability analysis potential vulnerabilities have been identified by the evaluator. These potential vulnerabilities have been analysed, if they are exploitable in the operational environment as defined in the Security Target. For every potential vulnerability which was identified to be a candidate to be exploitable in the intended operational environment the evaluator devised and conducted penetration tests. The overall results of the penetrations tests showed that attacks with high attack potential are not successful in the TOE’s operational environment as defined in [6].

8. Evaluated Configuration

This certification covers the following configurations of the TOE: SE5000-8.1 Rev A, 900773E /01R12 with software 1014, 01R12 represents customization variances of the evaluated TOE.

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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [15, 16] have been applied in the TOE evaluation.

(iv) Terminology and preparation of Smartcard-Evaluations

(v) Use of Interpretation for Security Evaluation and Certification of Digital Tachographs

(see [4], AIS 25, AIS 26, AIS 36, AIS 37).

For RNG assessment the scheme interpretations AIS 31 was used (see [4]).

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ATE_DPT.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1071-V5-2021, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

● PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.15, 6 June 2021, BSI-CC-PP-0094-V2-2021 [8]
● for the Functionality:	PP conformant, Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 table presented in appendix A of the Security Target [6] gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

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 Commission Implementing Regulation (EU) 2016/799 [13] the algorithms are suitable for Digital Tachograph Systems in the sence of Annex 1C [13] of Commission Implementing Regulation (EU) 2016/799 [13]. 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.

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. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GNSS	Global Navigation Satellite System
IT	Information Technology

ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VU	Vehicle Unit

13.2. Glossary

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

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.

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.

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

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

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

14. Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-1071-V6-2023, Revision 09, Date: 2023-06-30, SE5000-8.1 Security Target Vehicle Unit, Stoneridge Electronics AB

Security Target BSI-DSZ-CC-1071-V6-2023, Revision 01, Date: 2023-07-06, SE5000-8.1 Security Target Lite, Stoneridge Electronics AB (sanitised public document)

[7] Evaluation Technical Report, Version 6.4, Date: 07.07.2023, Evaluation Technical Report - Summary, Digital Tachograph (Vehicle Unit) SE5000-8.1 Version A, Deutsche Telekom Security GmbH, (confidential document)

[8] Configuration list for the TOE, SE5000-8.1A Security R01 Security.xml, Bill of Material, dated 06.07.2023, Stoneridge Electronics AB (confidential document)

[9] Guidance documentation for the TOE, Driver and Company Manual SE5000-8 Smart Tachograph, Version 9000-103765P_01 07, Stoneridge Electronics AB

[10] Guidance documentation for the TOE, Control Manual SE5000-8 Smart Tachograph, Version 9000-103766P_01 09, Stoneridge Electronics AB

[11] Guidance documentation for the TOE, Workshop Manual SE5000-8 Smart Tachograph, Version 9000-103767P_01 10, Stoneridge Electronics AB

[12] Digital Tachograph - Vehicle Unit (VU PP) Version 1.15, 6 June 2021, BSI-CC-PP-0094-V2-2021

[13] Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, Annex 1 C, as amended by Commission Implementing Regulation (EU) 2021/1228 of 16 July 2021

[14] Certification report NSCIB-CC-0173264-CR4, TÜV Rheinland Nederland B.V. 06.2023

[15] ETR for Composition der Plattform, ETRfC for NSCIB-2200060-01, TÜV Informationstechnik GmbH, Version 2, 23.06.2023

[7] specifically

- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results

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.

Annex B: Evaluation results regarding development
and production environment

Annex B of Certification Report BSI-DSZ-CC-1071-V6-2023

Evaluation results regarding development and production environment

The IT product SE 5000-8.1, Version A (Target of Evaluation, TOE) 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 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 10 July 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Stoneridge Electronics AB, Gustav III:s Boulevard 26, 169 73 Solna, Sweden (HW and SW development, HW and SW tests)

b) Stoneridge Electronics AB, Adolfsbergsvägen 3, 701 14 Örebro, Sweden (manufacturing and delivery of the final TOE)

c) Stoneridge Electronics AB, Stoneridge Electronics AB Avenida Alan Turing, 385 – Cidade Universitária, Campinas - São Paulo, Brazil (SW development and testing)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

Note: End of report