Federal Office
for Information Security

Certification Report

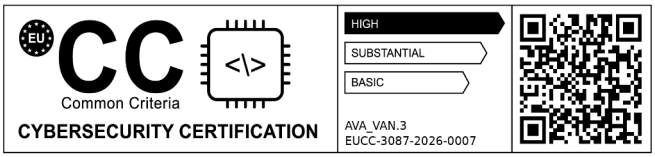
EUCC-3087-2026-0007
Administration ID
BSI-DSZ-CC-1263-2026

for

TactiGuard PG, v1.0.1

from

Saab Danmark A/S



BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Infoline +49 (0)228 99 9582-11

Contents

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. 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 carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation (CC), Version CC:2022[CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation (AIS) [AIS]

3. Recognition Agreements

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

3.1. 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 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] 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

- The TOE TactiGuard PG, v1.0.1 has been certificied by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1263-2026.
- The evaluation of the product TactiGuard PG, v1.0.1 was carried out by SRC Security Research & Consulting GmbH, located at Emil-Nolde-Straße 7, 53113 Bonn, Germany.
- The evaluation was completed on 29 May 2026. SRC Security Research & Consulting GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Saab Danmark A/S.
- The assessed TOE was developed by: Saab Danmark A/S.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in this report, are observed,
- the product is operated in an environment as specified in this 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 issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) to monitor the certified product. Specifically, if certification results should be 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 reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 22 June 2026 is valid until 21 June 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity (i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE TactiGuard PG, v1.0.1 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Saab Danmark A/S
Porten 6-8
DK-6400 Sonderborg
DENMARK

B. Certification Results

The following chapters summarise the assessment results of the

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

The Target of Evaluation is a Software for Data Transfer and Content Filtering. It is used to separate a system into sub-systems with different classification levels. A higher classified sub-system might need to exchange information with lower or non-classified subsystems and requires a security mechanism with high assurance for that purpose. Details can be found in chapter 2.3 of the Security Target [ST].

The product TactiGuard PG, v1.0.1 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. The TOE deliverables are listed in table 1.

The evaluation of the product TactiGuard PG, v1.0.1 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 29 May 2026. SRC Security Research & Consulting GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO],[EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: None.
- Assurance Level: EUCC High with component AVA_VAN.3
- Assurance Package: EAL 4
- Augmentation: ALC_FLR.3

Please note that the evaluation was actually successfully performed and evaluated by SRC for EAL5 augmented by ALC_FLR.3, however, for EUCC conformity reasons, this certificate just confirms the above mentioned assurance.

The Security Target [ST] is the basis for this certification. It is not based on a certified Protection Profile.

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

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

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitely guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology product is identified as follows:

TactiGuard PG, v1.0.1

Holder of the certificate: Saab Danmark A/S
Porten 6-8
DK-6400 Sonderborg
DENMARK
https://www.saab.com/products/tactiguard-xd

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	TactiGuard PG File name: tactiguard-pg-1.0.1.tar.gz	TactiGuard PG v1.0.1	Software digital archive
2	DOC	[AGD_PRE], Installation Guidance for TactiGuard PG, Saab Danmark, SVP-48	R4; 13.03.2026	Documentation digital archive
3	DOC	[AGD_OPE], User Guidance for TactiGuard PG, Saab Danmark, SVP-71	R4; 26.05.2026	Documentation digital archive

Table 1: Deliverables of the TOE

The integrity and authenticity of the manufactured digital archives, and hence the TOE, shall be verified using hash values, which are delivered via a separate secured (authenticity) channel. The secure channel is agreed upon with the individual customer.

3. Security Policy

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. The TOE implements a role-based access control policy to control administrative access to the system. In addition, the TOE implements policies pertaining to the following security functional classes: Security Audit, User Data Protection, Identification and Authentication and Security Management.

Specific details concerning the above mentioned security policies can be found in chapter 7 of the Security Target [ST].

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 uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are listed in the Security Target [ST], chapter 5.2.

5. Architectural Information

The TOE is implemented in the form of four subsystems that run on top of a certified microkernel. They are

- Audit
- Configuration
- Control
- Filter

These applications share functionality from a fifth subsystem, Shared Modules.

The microkernel provides domain separation and serves as an abstraction layer from the hardware.

The TOE is connected to the RED and BLACK networks that it is meant to filter. It can import prepared whitelist files from a block device, and export log data. The user interface is only available on the local console.

You may find further information in the ST [ST], chapter 2.4.3.

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 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.

The developer's website as stated in chapter 2 shall provide the following supplementary information:

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers
- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT, ICT service or ICT process and to any relevant cybersecurity advisories

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

All tests have been carried out by ITSEF:

SRC Security Research & Consulting GmbH
Emil-Nolde-Straße 7
53113 Bonn
Germany

under the responsibility of certification Body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 for details on assurance levels or packages involved into testing.

The developer uses different test scenarios to test different aspects of the TSF implementation. This includes manual functional tests in a configuration that is equivalent to deployment in the field. The other two test scenarios are automatic module tests and Automatic functional tests..

The evaluators used the same test approach and environment as the developer to repeat the developer tests. The main part of the test coverage consists of unit tests, i.e. tests that access a limited part of the TSF implementation directly and evaluate the response to the input given. Some tests are integration tests that test the TOE as a whole in a real or (partly) simulated operating environment. Additionally, the evaluators performed independent code reviews to ascertain specific features of the TOE implementation.

Although the evaluators found a sufficient test coverage by the developer, they additionally ascertained the following points by doing additional code reviews:

- Parameter values are checked against a rule set to determine if the network packet containing them may pass or not.
- A user must be authenticated and authorised before an action on their behalf is performed.
- An imported whitelist must be confirmed before being activated; to this end, the con-tent of the whitelist is displayed to the user.
- The TOE is initialised with secure default values, in particular there is no data flow before a valid configuration is present.
- The number respectively frequency of login attempts is limited to 3 every 60 seconds to mitigate brute-force attacks on the user authentication.

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

Please refer to chapter 11 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

8. Evaluated Configuration

The TOE has only a single security configuration of the TSF, which has been evaluated. The TOE software and guidance documents are the same for each TOE instance.

The TOE is prepared for deployment individually for each customer, depending on their target hardware, operating environment and organisatorial requirements. This does however not change the configuration of the TSF.

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to the the requirements of the Scheme [EUCC-VO], [EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines (AIS) [AIS].

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS] (AIS 34) was applied:

(i) AIS 1 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC

(ii) AIS 14 Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC

(iii) AIS 19 Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)

(iv) AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE. The corresponding TOE is identified in chapter 2 of this report.

The certificate

- is uniquely identified by EUCC-3087-2026-0007
  Administration ID BSI-DSZ-CC-1263-2026
- was issued on: 22 June 2026
- is valid until: 21. June 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account for the system risk management process. The user should define measures in the risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been reassessed.

The user also has to consider in the risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

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. Until the TOE has been re-certified, the user should examine the use 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 [ST] of the TOE is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the provisions of the EUCC certification scheme policy (see Implementing Regulation (EU) 2024/482, Annex V, V.2).

12. Regulation specific aspects (eIDAS, QES)

None

13. Acronyms

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
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation Technical Report
EUCC	European Common Criteria-based cybersecurity certification scheme
ICT	Information and communications technology
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

14. 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.

15. Bibliography

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
and
Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

as mirrored by CCRA's edition:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.commoncriteriaportal.org

[CEM] ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

as mirrored by CCRA's edition:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[EUCC_SOTA] EUCC state-of-the-art documents:
https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[EUCC_PROG]	EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung
[EUCC_CERT]	EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/) but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)
[AIS]	Application Notes and Interpretations (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS
[ST]	Security Target BSI-DSZ-CC-1263-2026, Security Target (ST) for TactiGuard PG, Saab Danmark, SVP-35; Revision 18, 29.05.2026 (confidential document), and Security Target Lite BSI-DSZ-CC-1263-2026, Security Target (ST) Lite for TactiGuard PG, Saab Danmark, SVP-425; Revision 8, 29.05.2026 (public sanitised document)
[ETR]	Evaluation Technical Report BSI-DSZ-CC-1263 for TactiGuard PG (TactiGuard PG v1.0.1), Version 1.1, Date: 29.05.2026, SRC Security Research & Consulting GmbH, (confidential document)
[ConfList]	Configuration List for TactiGuard PG, Saab Danmark, SVP-88, R6, 29.05.2026 (confidential document)
[AGD_PRE]	Installation Guidance for TactiGuard PG, Saab Danmark, SVP-48; R4; 13.03.2026
[AGD_OPE]	User Guidance for TactiGuard PG, Saab Danmark, SVP-71; R4; 26.05.2026

[6]See section 9.1 for detailed list of used AIS

C. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report