COMBITECH

CERTIFICATION REPORT
issued by an
Accredited Certification Body

SWEDAC ACKREDITERING
Ackred. nr 1914
Produktcertifiering
ISO/IEC 17065

Ref. No/Order No
CAB-260522-112419-972

Unit/Issued by	Date	Distribution
IQTR / David Carlysle	2026-08-20	Public
Unit/Appoint	Classification	
IQTR / Peter Döös	Unclassified	

Subject

Certification Report Saab SPNP Information Exchange Gateway 1.0.1

Version number	File name	Product name	Sponsor
1.0	CR Saab SPNP Information Exchange Gateway v1.0.pdf	Saab SPNP Information Exchange Gateway 1.0.1	Saab AB
ITSEF	**Reviewed by**	**Certification body**	**Certification ID**
COMBITECH		Combitech	CAB2026007

Contents

1 Executive Summary 3

2 Certified ICT Product 4

3 Security Policy 5

3.1 Security Services 5

3.2 Vulnerability Management Policy 6

3.3 Assurance Continuity Policy 7

4 Assumptions and Clarification of Scope 7

4.1 Assumptions 7

4.2 Clarification of Scope 8

5 Architectural Information 9

6 Supplementary Cybersecurity Information 10

7 TOE Evaluation and Configuration 11

7.1 Testing 13

8 Result of the Evaluation 14

9 Comments and Recommendations 14

10 Security Target 14

11 Scheme Mark and Label 14

12 Glossary 15

13 References 15

1 Executive Summary

Combitech certification id	CAB2026007
TOE identification	Saab SPNP Information Exchange Gateway 1.0.1
Security Target identification	Saab SPNP Information Exchange Gateway 1.0.1 Security Target, version 1.12, 2026-04-16
Assurance package	EAL4 augmented with ALC_FLR.1
Assurance level	High, AVA_VAN.3
Protection Profile	N/A
Sponsor	Saab AB
Developer	Saab AB
ITSEF	Combitech EC/ITSEF
Certification Body	Combitech Certification Center
National Cybersecurity Certification Authority	FMV/ICC
Evaluation completion date	2026-04-27
Final Evaluation Report	Final Evaluation Report – Saab SPNP Information Exchange Gateway 1.0.1, version 1.1, 2026-05-21, CAB-260518-104721-731:001, Combitech AB
Common Criteria version	CC:2022, Revision 1
CEM version	CEM:2022, Revision 1
Scheme	EUCC Scheme
Combitech services	Combitech EUCC Certification and Evaluation Services, v1.7
Recognition Scope	EUCC, EA/MLA
Certification date	2026-08-20
Certificate validity	5 years from certification date
Certificate id	EUCC-3135-2026-0002

The TOE, SPNP Information Exchange Gateway (IEG), enables secure bi-directional information exchange between security domains of equal or differing classification levels, supporting Swedish classifications (Hemlig, Konfidentiell, Begränsad Hemlig) and NATO classifications (SECRET, CONFIDENTIAL, RESTRICTED). The SPNP IEG supports network-centric and data-centric functionality for both central and tactical scenarios, enabling cross-domain communication across land, naval, and air/AEW operations. The SPNP IEG is intended to support multi-national and multi-domain interoperability and

serves as a key enabler for situational awareness and information sharing in NATO-led missions.

There are four assumptions made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these being met to counter the five threats. The ST defines two organisational security policies. The assumptions, the threats, and the organisational security policies are described in chapter 4 Assumptions and Clarification of Scope. The evaluation has been performed by Combitech AB at their premises in Bromma, Sweden, and Växjö, Sweden.

Combitech EC/ITSEF is a licensed evaluation facility for Common Criteria under the EUCC Scheme. Combitech EC/ITSEF is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria. The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL4 augmented with ALC_FLR.1. The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech EC/ITSEF.

2 Certified ICT Product

The TOE is Saab SPNP Information Exchange Gateway 1.0.1 from Saab AB and is a fully programmable network element that runs on a hardware platform that includes a hardware programmable data plane pipeline. The network element hardware, software and build environment constitutes the Programmable Trusted Network Element, PTNE.

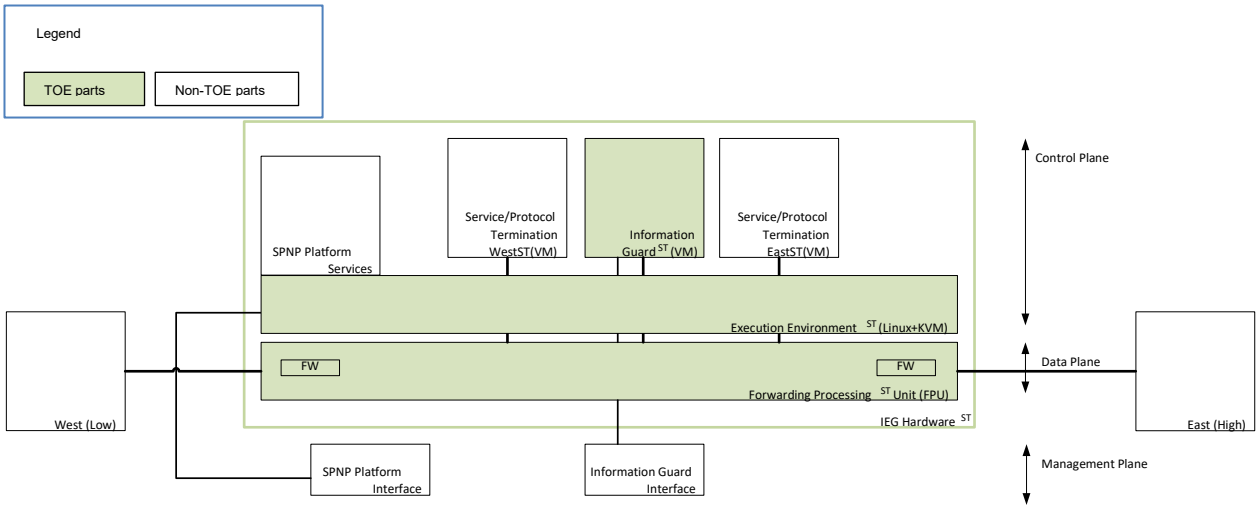


Figure 1, TOE structure

The TOE includes the following parts:

Forwarding Processing Unit (FPU) – Decides what to do with packets arriving on an inbound interface. This may result in dropping the packet, forwarding it to other ports or to

the control plane. The FPU includes firewalls on both the West (high) and the East (low) sides.

Execution Environment (CPU) – Running Linux with KVM hypervisor.

Information Guard – Virtual machines used as a programmable information guards. One is for information flow low-to-high and one is for information flow high-to-low.

Management and configuration for the FPU, Execution Environment, and the Information Guard is done through Execution Environment functionality.

The virtual machines execute on the Linux KVM hypervisor. Two of the virtual machines, West and East parser/proxy are not included in the TOE.

The TOE supports several applications and services with associated protocols details. Transport/protocol specific control messages like SMTP, XMPP, REST, SOAP, HTTP/HTTPS headers and actual payload data content like XML, REST, JSON, MTF, NVG being exchanged are supported. Examples of applications supported are Email (SMTP).

3 Security Policy

3.1 Security Services

Security Audit

Records of security related events are written to a local log trail in persistent memory. The log records are structured according to the Syslog Protocol (RFC 5424). The oldest log entry is overwritten if the log trail gets full. A warning is logged and shown at the management GUI when 25% of the log trail space remains. A warning is also produced if the log trail turns around. Only the Security officer can access and manage the log records.

Cryptographic Support

The TOE relies on the environment to provide the cryptography for TLS v1.2 and TLS v1.3 protected communications. The cryptographic module OpenSSL v3.0.7 provides algorithms for format preserving encryption. Cryptographic security functions requirements around the FCS class serve in specifying the cryptographic operations of the TLS communication.

User Data Protection

Information flow control policies determine if incoming/outgoing packages shall be dropped or forwarded. Policies are applied at two levels, West (low) and East (high) firewall, as well as Information guard. The information guard supports a Security Policy Information Framework, SPIF. XML-based formats and syntax are used for security policies and confidentiality metadata used by the SPIF. FDP_IFF(a) and FDP_IFC(a) handled the enforcement of information guard flow control SFP and FDP_IFF(b) and FDP_IFC(b) handles the same but for the firewall and its technical layer.

Protection of the TSF

Related to the handling of operational states within the TOE, including the specific functions which each state allows, user access for integrity checks, reliability of time source and self-tests. FPT_FLS handles secure state, FPT_STM handles reliable time and FPT_TST handles self-test.

Identification and Authentication

Management of the TOE is performed by the roles: Administrator, Security officer, Operator, and User Administrator. To create a user, the User Administrator must provide a user account name, password, and limitations on the resources available to the user. These limitations are in the form of defined permissions, i.e., the defined roles. This is managed in the user interface for SPNP IEG. SPNP IEG ensures that users are identified and authenticated prior to being allowed access to database objects or resources.

Security Management

Security Management is provided by enforcing roles, i.e., RBAC. The Administrator is allowed to read and access all configuration and management functions except managing the security event log.
The Security officer is allowed to read TOE configuration and is the only role allowed to read and manage the security event log. The User administrator is allowed to read TOE configuration and to manage user's configuration. The Security officer role cannot be combined with the Administrator nor the User Administrator roles.
The security attributes that the rules in the information flow control policies are based on can be managed by the Administrator. Default values are restricted, which means that all packages are dropped until otherwise is configured.

TOE Access banners

A text describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE is displayed when logging in to the TOE.

3.2 Vulnerability Management Policy

The following vulnerability management and vulnerability disclosure procedures have been identified as applicable to the TOE.

Reporting a Security Vulnerability

Since this product is not publicly available, external reporting is mainly done through the customer channels intended for delivery and maintenance of each project.

Tracking a Security Vulnerability

All potential flaws and weaknesses, internally discovered or reported from external sources, are handled as tickets in Jira.

Triage and Planning

All Jira tickets are handled as change requests and handled according to decisions from the Change Control Board, CCB.

Implementation and Testing

If critical or major issues are found the following applies before the system test can be restarted on a new release candidate:

- Issues will have to be fixed if possible, making minimal impact to the code
- Module and integration tests must be updated to cover the issue found
- Module and appropriate integration tests need to be redone

The software requirements process includes functional, performance, interface and security related requirements. Security reviews include all in-house developed software that will be delivered to customer.

Release

Release decision and acceptance for customer use are made by the Release Control Board, RCB. All changes made are presented in Release Notes referring to the Jira id. The Release Notes are communicated to the customers involved.

3.3 Assurance Continuity Policy

This is a new product certification. An assurance continuity policy was not provided.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The following assumption on the TOE operational environment are made.

ASSUMPTION	DESCRIPTION
A.PHYSICAL_ PROTECTION	The TOE and its administrator management network are assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the TOE's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the TOE and the data it contains.
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the TOE are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are to lack malicious intent when administering the device.
A.LIMITED_ FUNCTIONALITY	The TOE is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.RELIABLE_TIME	The TOE operational environment is assumed to provide a reliable time source.

Table 1, Assumptions

The user guidance as outlined in [ST] section 1.6.5.3 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions and Objectives for the operational environment described in the [ST]. Certain aspects of the TOE's security functionality, particularly the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

All threats identified in the Security Target, [ST] section 3.2 have been countered by the evaluated security functions of the TOE.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.
Threats describe how defined threat agents may perform adverse actions against the assets that the TOE must protect.

The table below identifies:

- the assets requiring protection
- the threat agents and their attack potential
- the adverse actions that could compromise those assets

IDENTIFIER	DESCRIPTION
T.DATA_ACCESS	Threat agents may attempt to bypass the information flow control policy by sending information which may result in exploitation and/or compromise of protected resources, through the TOE.
T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the TOE by nefarious means. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the TOE and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the TOE without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_ FUNCTIONALITY_FAILURE	Threat agents could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 2, Threats against the TOE

Organizational security policies, OSPs, for the TOE are stated according to the following table.

Name	OSP
P.ACCOUNTABILITY	The TOE administrators must be accountable for their actions.
P.ACCESS_BANNER	The TOE must display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE.

Table 3, Organizational Security Policies for the TOE

Supported functionality excluded from the evaluation are:

- Management API
- HTTPS certificate support
- Syslog interface
- SNMP
- USB installation interface

5 Architectural Information

The TOE provides its primary security functionality as an Information Exchange Gateway that enables bi-directional information exchange between security domains of equal or differing security classifications, supporting both network-centric and data-centric functionality.

The TOE is based on a hardware platform from APS Networks, APS BF2156X-1T. The hardware platform includes Intel Tofino Technology hosting a P4 programmable data plane pipeline. TOE software is developed for the Intel Barefoot Tofino ASIC and the Intel x86 CPU.

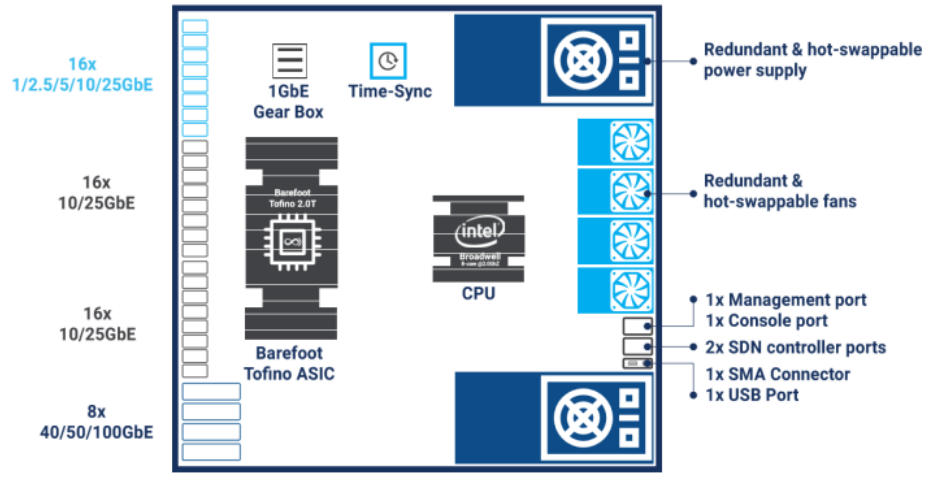


Figure 2: TOE hardware overview

The network element hardware, software and build environment constitutes the Programmable Trusted Network Element.

The responsibilities and functions of the TOE parts are as follows:

Intel Barefoot Tofino ASIC (FPU) – Decides what to do with packets arriving on an inbound interface. This may result in dropping the packet, forwarding it to other ports or to the control plane. The FPU includes firewalls on both the West (high) and the East (low) sides.

Intel x86 CP (CPU) – Running Linux with KVM hypervisor.

Information Guard – Virtual machines used as a programmable information guards. One is for information flow low-to-high and one is for information flow high-to-low.

Management and configuration for the FPU, Execution Environment, and the Information Guard is done through Execution Environment functionality.

The virtual machines execute on the Linux KVM hypervisor. Two of the virtual machines, West and East parser/proxy are not included in the TOE.

6 Supplementary Cybersecurity Information

The Sponsor and Developer web site is reached at:
https://www.saab.com/

The TOE includes the following guidance documentation:
SPNP IEG Installation Instructions for PTNE.CCC.1.0.1
SPNP IEG User Manual for PTNE.CCC.1.0.1

Additional TOE operational guidance and installation procedures are provided in the TOE, Guidance Documents – Saab SPNP Information Exchange Gateway 1.0 [AGD].

7 TOE Evaluation and Configuration

The TOE was evaluated according to Common Criteria, CC:2022, and Common Methodology, CEM:2022, [CCpart1], [CCpart2], [CCpart3], [CCpart4], [CCpart5], and [CEM].

No protection profile was claimed. No EUCC state-of-the-art documents were used for this evaluation.

The evaluation was performed according to EAL4 augmented with ALC_FLR.1, Basic flaw remediation.

The assessment classifications used during this evaluation are: PASS, FAIL, and INCONCLUSIVE which have been drawn from [CEM]. In addition, the classification REMARK has been used. REMARK is used for errors that are not judged serious enough to cause the work unit to receive a FAIL verdict.

The overall verdict of the evaluation is: **PASS.** The following assurance components were used.

Assurance Components	Action Element	Verdict
ASE_INT.1		Pass
	ASE_INT.1.1E	Pass
	ASE_INT.1.2E	Pass
ASE_CCL.1		Pass
	ASE_CCL.1.1E	Pass
ASE_SPD.1		Pass
	ASE_SPD.1.1E	Pass
ASE_OBJ.2		Pass
	ASE_OBJ.2.1E	Pass
ASE_ECD.1		Pass
	ASE_ECD.1.1E	Pass
	ASE_ECD.1.2E	Pass
ASE_REQ.2		Pass
	ASE_REQ.2.1E	Pass
ASE_TSS.1		Pass
	ASE_TSS.1.1E	Pass
	ASE_TSS.1.2E	Pass
ALC_CMC.4		Pass
	ALC_CMC.4.1E	Pass
ALC_CMS.4		Pass

Assurance Components	Action Element	Verdict
	ALC_CMS.4.1E	Pass
ALC_DEL.1		Pass
	ALC_DEL.1.1E	Pass
ALC_DVS.1		Pass
	ALC_DVS.1.1E	Pass
	ALC_DVS.1.2E	Pass
ALC_LCD.1		Pass
	ALC_LCD.1.1E	Pass
ALC_TAT.1		Pass
	ALC_TAT.1.1E	Pass
ALC_FLR.1		Pass
	ALC_FLR.1.1E	Pass
ADV_ARC.1		Pass
	ADV_ARC.1.1E	Pass
ADV_FSP.4		Pass
	ADV_FSP.4.1E	Pass
	ADV_FSP.4.2E	Pass
ADV_IMP.1		Pass
	ADV_IMP.1.1E	Pass
ADV_TDS.3		Pass
	ADV_TDS.3.1E	Pass
	ADV_TDS.3.2E	Pass
AGD_OPE.1		Pass
	AGD_OPE.1.1E	Pass
AGD_PRE.1		Pass
	AGD_PRE.1.1E	Pass
	AGD_PRE.1.2E	Pass
ATE_COV.2		Pass
	ATE_COV.2.1E	Pass
ATE_DPT.1		Pass
	ATE_DPT.1.1E	Pass
ATE_FUN.1		Pass
	ATE_FUN.1.1E	Pass
ATE_IND.2		Pass
	ATE_IND.2.1E	Pass
	ATE_IND.2.2E	Pass
	ATE_IND.2.3E	Pass

Assurance Components	Action Element	Verdict
AVA_VAN.3		Pass
	AVA_VAN.3.1E	Pass
	AVA_VAN.3.2E	Pass
	AVA_VAN.3.3E	Pass
	AVA_VAN.3.4E	Pass

Table 4, Evaluation verdicts

7.1 Testing

Both the developer's and the evaluator's independent tests were performed on a configuration similar with the configuration described in chapter 5.

7.1.1 Developer Testing

The testing effort, outlining the testing approach, configuration, depth and results for the developer testing is described in the [ATE], [TD], [STR] and [IBTR].

All developer tests are structured as test cases consisting of step-by-step procedures that specify interactions with the TOE interfaces, as described in Chapter 3 [ATE].

The actual results from each test step are compared with the expected results and with the results from the developer's test effort.

The developer testing was done between 2025-12-17 and 2026-01-14.

All developer tests result in a Pass.

7.1.2 Evaluator Independent Testing

Testing was performed on a subset of the developer's tests, with a passing result.

The tests were divided into the following test groups:

- **Test Group 1 Installation**
  TOE Installation, verification of installation and configuration of the TOE as stated in the [STR] and [IBTR].
- **Test Group 2 Re-testing of developer tests**
  Re-run of a chosen subset of developer tests, a number of developer tests are sampled and re-tested by the evaluator. This activity is performed as part of the assessment of the developer test effort and test accuracy.
- **Test Group 3 Evaluator devised tests**
  Tests devised by the evaluator with the purpose to broaden the test coverage.

- **Test Group 4 Vulnerability scanning**
  Tests that complement the vulnerability assessment; this activity mainly consists of vulnerability scanning, assessment of exposed services, and similar tasks.

Each test case contained descriptions of the test steps, the expected result for each step, and an indication of whether the test met the expected result. Additional evidence of the test steps and results was provided in each test case's test-execution table.

8 Result of the Evaluation

The certificate Common Criteria Certificate Saab SPNP Information Exchange Gateway 1.0.1 was issued 2026-08-20. The certificate is valid for a maximum of five years but can be changed over time. For information regarding the current status of the certificate, please contact Combitech, Ljungadalsgatan 2B, Växjö,https://www.combitech.com/certificationcenter.

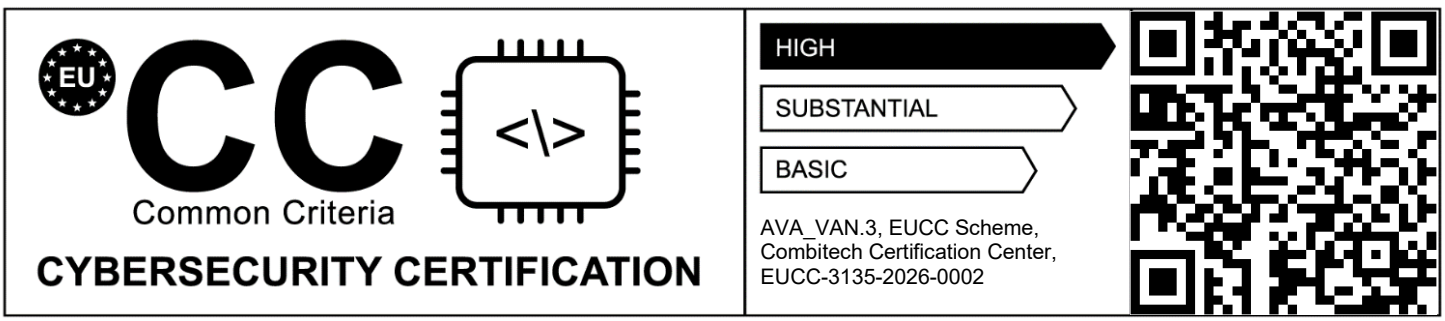
9 Comments and Recommendations

The evaluation activities did not result in any comments, observations, or recommendations to be included in this report.

10 Security Target

The evaluated Security Target is: Security Target - Saab SPNP Information Exchange Gateway 1.0, revision 1.12, 2026-04-21.

11 Scheme Mark and Label



12 Glossary

CCRA	Common Criteria Recognition Arrangement
EA/MLA	European Accreditation Multilateral Agreement
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
PGP	Pretty Good Privacy
TLS	Transport Layer Security

13 References

[CCpart1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022, revision 1, November 2022, CCMB-2022-11-001

[CCpart2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022, revision 1, November 2022, CCMB-2022-11-002

[CCpart3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022, revision 1, November 2022, CCMB-2022-11-003

[CCpart4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, version CC:2022, revision 1, November 2022, CCMB-2022-11-004

[CCpart5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, version CC:2022, revision 1, November 2022, CCMB-2022-11-005

[ISO] ISO/IEC 15408:2022, Fourth edition, 2022-08

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version CEM:2022, Revision 1, November 2022, CCMB-2022-11-006

[ERR] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), version 1.2, 2025-10-15

[CSA] 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)

[EUCC] Commission Implementing Regulation (EU) 2024/482 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-amd-1] Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

[EUCC-amd-2] Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

[EUCC Vuln] EUCC Scheme GUIDELINES on Vulnerability Management and Disclosure, Version 1.1, January 2025

[STAFS] 2020:1, Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om ackreditering

[QM] Quality Manual 17065, issue 1.3, CAB-23-8937-8630-87-00, Combitech AB

[ST] Security Target - Saab SPNP Information Exchange Gateway 1.0, version 1.12, 2026-04-21

[CCC] Combitech EUCC Certification and Evaluation Services, issue 1.7, CAB-250902-103410-916:007, Combitech AB

[FER] Final Evaluation Report – Saab SPNP Information Exchange Gateway 1.0.1, version 1.1, 2026-05-21, CAB-260518-104721-731:001, Combitech AB

[AGD] Guidance Documents – Saab SPNP Information Exchange Gateway 1.0, version 1.0, 2026-02-03, Saab AB

[INSTALL] SPNP IEG Installation Instructions for PTNE.CCC.1.0.1, T-MCI-0538, Issue B, 2026-01-07, Saab AB

[TD] PTNE Test Description, 2025-12-11

[ATE] Test Plan - Saab SPNP Information Exchange Gateway 1.0, 1.1, 2026-04-16

[IBTR] PTNE Information Barrier Test Report PTNE.CCC.1.0.1, T-MCI-0545, 2, 2025-12-19

[STR] PTNE System Test Report PTNE.CCC.1.0.1, T-MCI-0541, version 2.0, 2025-01-14