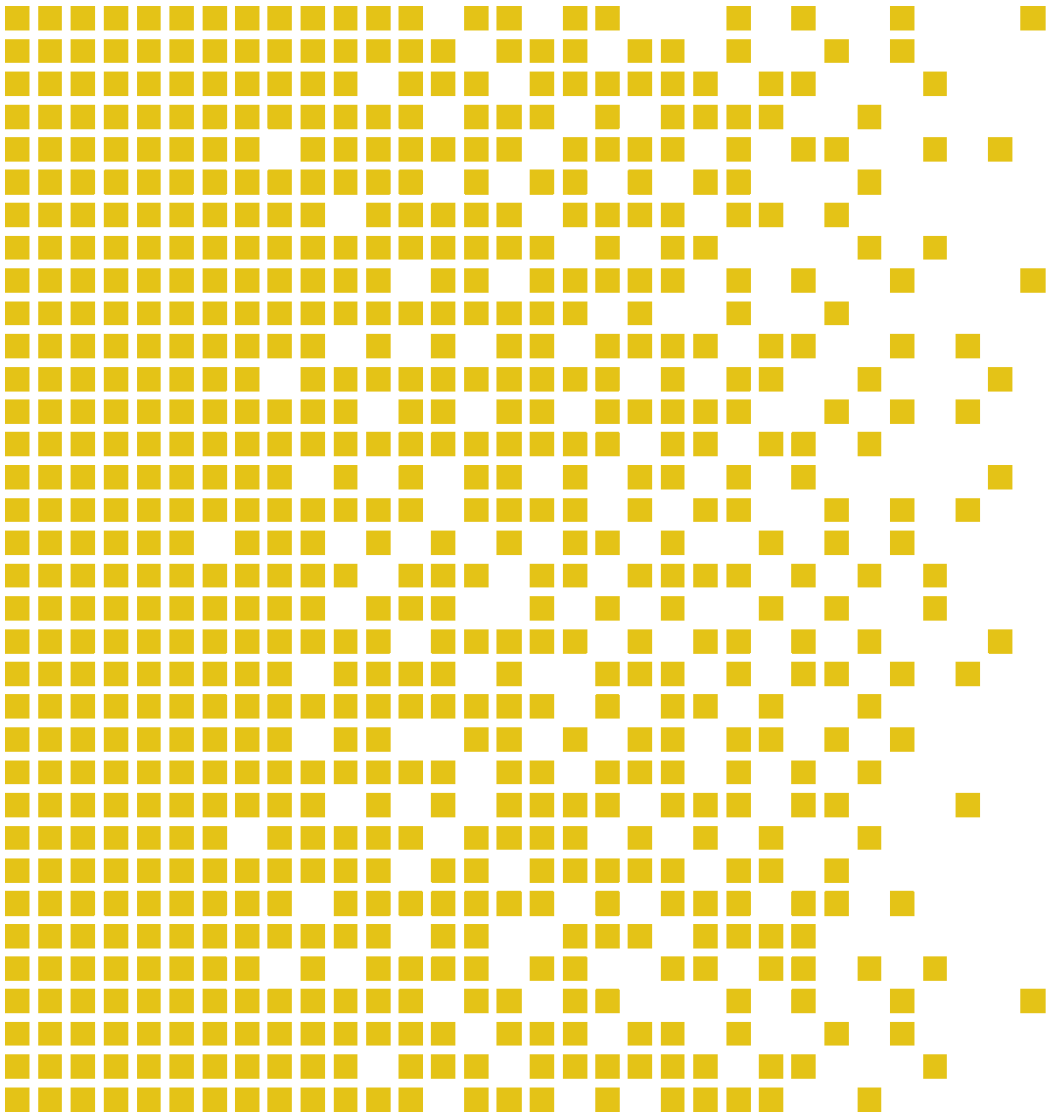
SERTIT-120 CR Certification Report

Issue 1.0 12.05.2022

Expiry date 12.05.2027

TNOR Guard v. 1.1.3



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (ITSEF) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (ITSEF) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

Certification Statement

TNOR Guard is a technology that provides controlled information flow between networks with different system and application security policies. TNOR Guard is developed by Thales Norway AS.

TNOR Guard version 1.1.3 has been evaluated under the terms of the Norwegian Certification Authority for IT Security (SERTIT) and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.3 and AVA_VAN.4 for the specified Common Criteria Part 2 (ISO/IEC 15408) in the specified environment when running on the platforms specified in Table 1.

The evaluation addressed the security functionality claimed in the ST Public [11] with reference to the assumed operating environment specified by the ST Public [11]. The evaluated configuration was that specified in Table 1. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

Certification team	Lars Borgos Øystein Hole
Date approved	12.05.2022
Expiry date	12.05.2027

1 Executive Summary

The evaluated product was TNOR Guard version 1.1.3 (TOE). The TOE is developed at Thales Norway AS. The TNOR Guard is comprised of the following four product IDs:

Table 1 TOE Reference

Product Name	Product ID	Supported platforms
STANAG 4406 Message Guard	3AQ 28150	Kontron (B) Generic PC (C)
SMTP Message Guard	3AQ 28151	
XMPP Chat Guard	3AQ 28152	
SOAP XML Guard	3AQ 28153	

The main security feature of the TOE is to mediate a one-way or bidirectional flow between two security domains. The TOE inspects every information object that is requested sent between the security domains, and makes an automated release decision according to configured policy. Requirements regarding Non-TOE hardware, software and firmware can be found in chapter 1.4.3 in the ST Public [11].

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, seven assumptions are made in the ST Public [11]. In order to counter fifteen threats as described in the ST Public [11], the TOE relies on the assumptions made. Details can be found in Chapter 4 Assumptions and Clarification of Scope.

The evaluation was performed by the ITSEF System Sikkerhet AS, a Nemko Company. The evaluation was performed in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in the document SD001E [7], as well as the Common Criteria (CC) Part 3 [3] and the Common Evaluation Methodology (CEM) [4].

The evaluation was performed at the assurance level EAL 4 augmented with ALC_FLR.3 and AVA_VAN.4.

System Sikkerhet AS is an authorised ITSEF under the Norwegian Certification Authority for IT Security (SERTIT). System Sikkerhet AS is an accredited ITSEF according to the standard ISO/IEC 17025 for Common Criteria evaluation. The sponsor for this evaluation was FMA.

The evaluation activities were monitored by the certification team. The security claims stated in the ST [10] was confirmed during the evaluation for the selected assurance level.

The basis for producing this Certification Report is the ST Public [11] and the ETR [9].

2 TOE overview

The TNOR Guard (TOE) is part of the XOmail product family for messaging and information exchange in mission-critical military and civilian networks. The Guard implements high-assurance information flow control for the trusted exchange of information across security domain boundaries. This product is also described in this report as the Target of Evaluation (TOE).

The TOE covers the following four Guard products:

- STANAG 4406 Ed 2 Message Guard
  For connectivity towards the NATO standard Military Message Handling System (MMHS),
- SMTP Message Guard (E-mail)
  For connectivity towards standard e-mail systems such as Microsoft Exchange.
  Supports RFC 6477 for Military Message Handling attributes within the SMTP domain,
- Chat (XMPP) Guard
  Instant Messaging service between security domains.
- XML/SOAP Guard
  Exchange of XML/SOAP data between security domains.

The product IDs are listed in table 1.

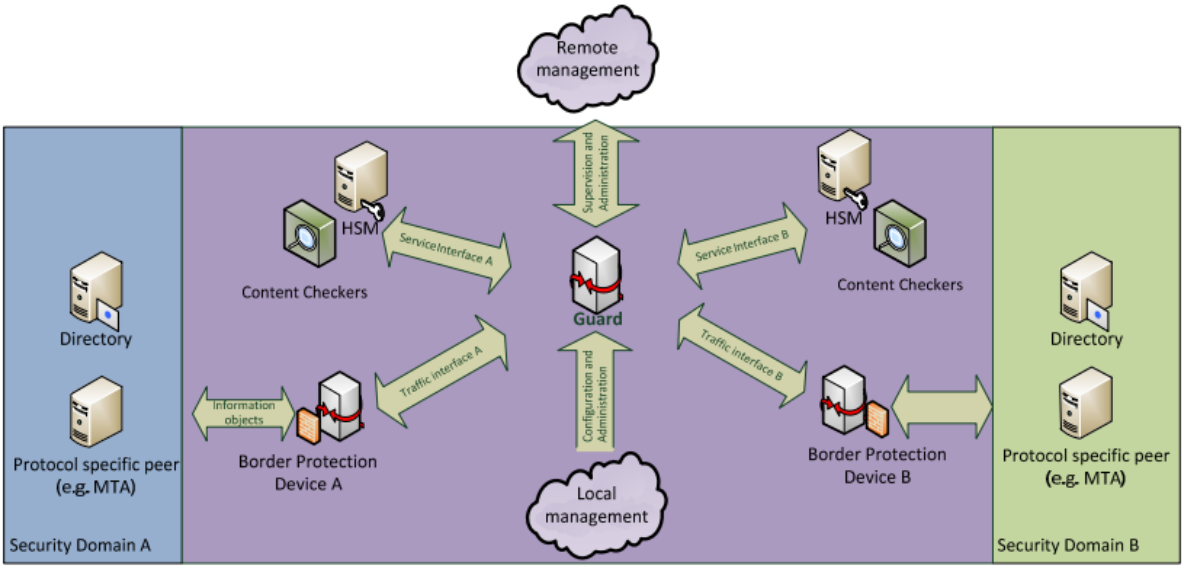


Figure 1 Overview of TOE Environment

The TOE is the TNOR Guard, a high assurance guard providing an automatic and controlled flow of information between two domains that may operate under different security policies. No information is allowed to pass from one of the domains to the other unless the Security Policy of the TOE explicitly allows to pass.

The Guard communicates with one or more peers in each security domain which acts as a proxy for other services within each of the two security domains. The Guard also uses directory services to access certificates and certificate revocation lists in each of the security domains.

The Guard is installed in a protected environment, with border protection devices mitigating as shown in figure 1.

During processing of the information objects (messages) the Guard uses external services, such as directory servers and content checker services to provide necessary information to perform a release decision, and it uses hardware security modules when signing released information objects. Even though the Guard uses external services it ensures that no parts of, or traces of, the information object is released into the destination domain before a positive release decision has been made.

The Guard provides online tools for management of the run-state, logs and configuration data of the Guard.

The Guard Configuration Tool (TOE Environment) is provided for creating configuration vectors for the Guard (TOE). This software runs on separate computers, and the resulting configuration vectors are loaded via the “Local management” interface as shown in Figure 1. The “Remote management” interface is used for management of the Guard (TOE).

The TNOR Guard is transparent to the users of its services in the security domains.

The Guard is not based on store-and-forward principles. The Guard acts as a proxy, and important mechanisms in a Military Messaging System such as queuing and recover / retry must be implemented by adjacent MTAs. The Guard does not provide a routing service, it considers all received information objects from one domain to be requests for information release to the other domain.

The Guard receives the information (message) via the traffic interface, and converts the information to a protocol independent format. The Guard processes the information as described in ST Public [11], and decides whether the security policy allows the information to be released, or whether it must be rejected.

While processing the information release requests, the Guard has not yet accepted the message from the adjacent MTA. If the information release request is accepted the Guard will send the message to the other adjacent MTA, and once that MTA has accepted responsibility for the message the

Guard will free any resources allocated for that messages and acknowledge the message from the MTA in the source domain

If the information release request is rejected the Guard will free any resources allocated for the message, and signal the rejection of the message to the MTA in the source domain. Further handling is the determined by the connected MTA. The Guard does not generate non-delivery reports or provide traffic operator functions.

3 Security Policy

The main security feature of the TOE is to mediate a one-way or bidirectional flow between two security domains. The TOE inspects every information object that is requested sent between the security domains, and makes an automated release decision according to configured policy.

The TOE performs the following security checks in order to support the main security features of the TOE:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Filter
- Content Checking
- Digital Signature validation

Also an Attribute Based Access Control (ABAC) feature is implemented in the TOE due to the combination of different security checks and the results. Chapter 6 of the ST Public [11] describe details regarding the security policy.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The following seven assumptions made regarding the usage and the operational environmental environment of the TOE are:

- APPROVED_CRYPTO
- APPROVED_PKI
- CORRECT_CONFIGURATION
- NETWORK_PROTECTED
- PHYSICAL_ACCESS_MANAGED
- TRUSTED_AND_TRAINED_ADMIN
- TRUSTED_LABELLER

For details on these assumptions, the reader is advised to look at chapter 3.1 in the ST Public [11].

4.2 Threats

The threats and threat agents met by the TOE are diverse and depend on where the TOE is deployed. The following sixteen threats are countered by the TOE:

- ADMIN_MASQUERADE
- AUDIT_COMPROMISE
- OBJECT_TAMPERING
- COVERT_CHANNEL
- DOS
- INFORMATION_LEAK
- INSECURE_STATE
- MALWARE_INJECTION
- METADATA_LEAK
- NETWORK_ATTACK
- RECONNAISSANCE
- RESIDUAL_DATA
- TSF_COMPROMISE
- UNATTENDED_ADMIN_SESSION
- UNAUTHORIZED_ACCESS
- UNNOTICED_ATTACK

For details on these threats, the reader is advised to look at chapter 3.2.4 in the ST Public [11]. The reader should also have a look at the description of the threat agents in chapter 3.2.3 in the ST Public [11].

4.3 Organisational Security Policies

During the evaluation of the TOE the following four Organisational Security Policies have been considered:

- ACCOUNTABILITY
- CLASSIFICATION
- CRYPTOGRAPHY
- MINIMAL_POSTURE

For details on these organisational security policies, the reader is advised to look at chapter 3.3 in the ST Public [11].

5 Architectural Information

The TOE (the grey area in figure 2) is comprised by software distributed on three separate hardware instances. The TNOR Guard is composed by three hardware units, each with a set of PikeOS separation kernel and software.

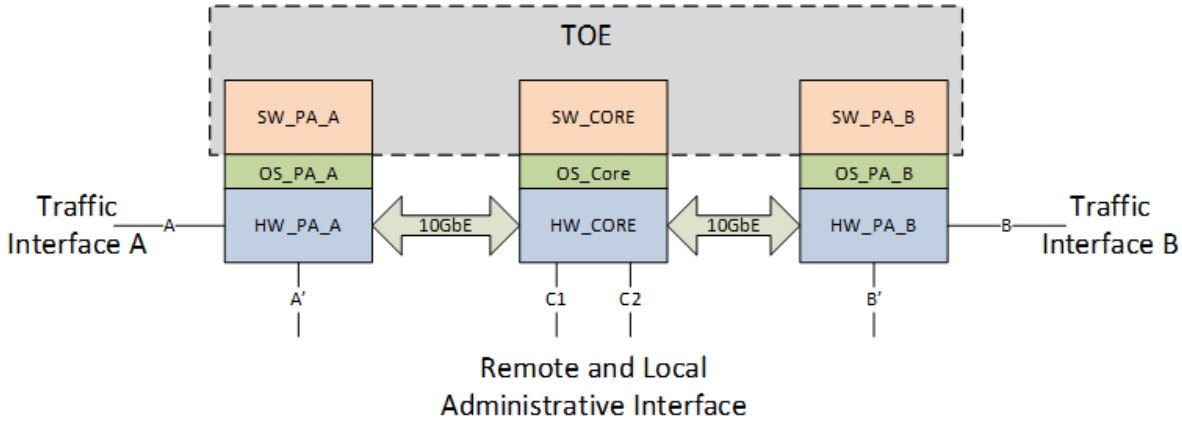


Figure 2 TOE Interfaces and HW deployment

The Guard runs on top of a separation kernel hypervisor that is used to separate different parts of the TOE using partitions. Separate partitions are used to isolate specific security function implementations from other functions, to separate processing of different messages, and to separate the information flow directions. The IPC mechanism features IPC communication between processes in the same partition, between processes in different partition on the same processing unit, and between processes in different partitions on different processing units. The IPC mechanism also provides strict control on inter-process communication and denies all IPC communication that is not explicitly allowed on both process-level and on partition-level.

5.1 Guidance

The guidance documents referenced in [12], [13], [14] are evaluated as a part of the TOE.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

6 Vulnerability Analysis and Testing

6.1 Vulnerability Analysis

The evaluator did not find any specific area of concern when examining the Functional Specification, TOE Design and Security Architecture.

The evaluator searched for known vulnerabilities in Public available sources, without finding any information identifying and describing possible attack scenarios for the TOE type. The evaluator used the search engine Google on the 26.05.2021 as well as on 16.03.2022 without finding any issues of interest regarding “application guard proxy”.

Further, to identify potential vulnerabilities in the TOE, the evaluator successfully conducted and completed a methodological analysis according to the evaluation criteria AVA_VAN.4. This also comprises all threats described in the ST Public [11].

The evaluator recorded potential vulnerabilities that were candidates for testing and applicable to the TOE in its operational environment. The evaluator developed and conducted penetration tests based on the developer’s vulnerability analysis and the evaluator’s independent vulnerability analysis.

6.2 Developer’s Tests

The developer thoroughly tested the TOE at different abstraction levels like the TSFI, TSF, Subsystems and TOE modules.

The evaluator examined the developers tests and concluded that the developer has tested all the TSF subsystems, SFR enforcing modules and the SFR supporting modules against the TOE design and the Security Architecture descriptions.

The testing performed on the TOE by the developer and the evaluator showed the EAL 4 assurance components requirements are fulfilled.

6.3 Evaluators’ Tests

The selected test strategy for the TSFIs and the two TSF modules was based on the test coverage and an analysis of the depth of testing. The selected sample testing constitutes about 21% of the total developer tests.

The evaluator tested both TSFIs, all TSF subsystems, and a subset of the TSF modules that constituted a scope of the SFRs.

The interfaces, subsystems, modules and security functions were tested at the Developers facility at 18-19.08.2021.

All scenarios from the sample testing and all the scenarios from the evaluators testing were successfully performed with the expected results.

7 Evaluated Configuration

The certified TOE, in table 1, can be used on the supported platforms as specified. Details regarding the hardware specifications can be found chapter 1.4.3.3 in the ST Public [11].

Installation of the TOE must be performed completely in accordance with the guidance documents [12], [13], [14] provided by the developer. The TOE should be used in the operational environment as specified in the ST Public [11], as well as the guidance documents referenced in this chapter.

8 Evaluation Results

The evaluation addressed the requirements specified in the ST Public [11]. The ITSEF reported the results of this work in the ETR [9] on the 18 March 2022.

The evaluators examined the following assurance classes and components taken from CC Part 3 [3]. These classes comprise the EAL 4 assurance package augmented with ALC_FLR.3 and AVA_VAN.4.

Assurance classes	Assurance components		Verdict
Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation of TSF	PASS
	ADV_TDS.3	Basic modular design	PASS
Guidance documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_FLR.3	Systematic flaw remediation	PASS
Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_DPT.1	Testing: Basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS

Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis	PASS

After due consideration of the ETR [9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that TNOR Guard version 1.1.3 meet the specified Common Criteria Part 3 [3] components of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.3 and AVA_VAN.4 for the specified Common Criteria Part 2 [2] in the specified environment, when running on platforms specified in table 1.

9 Recommendations

Prospective consumers of TNOR Guard version 1.1.3 should understand the specific scope of the certification by reading this report in conjunction with the ST Public [11]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST Public [11].

Only the evaluated TOE configuration should be installed.

The TOE should be installed and operated in accordance with the supporting guidance [12], [13], [14] and the recommended configuration.

There are no specific remarks regarding the auditing and testing of the TOE.

10 Security Target

The complete ST [10] used for the evaluation of the TOE is sanitised for the purpose of publishing. The open version is the ST Public [11] provided as a separate document.

Sanitisation was performed according to the CCRA framework – *ST sanitising for publication* [5].

11 Glossary

ABAC	Attribute Based Access Control
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)
cPP	collaborative Protection Profile
CPR	Content-based Protection and Release
DAC	Discretionary Access Control
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FMA	Forsvarsmateriell
HSM	Hardware Security Modules
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
IPC	Inter-Process Communication
MAC	Mandatory Access Control
MHS	Message Handling Service
MMHS	Military Message Handling System
MTA	Mail Transfer Agent
PKE	Public Key Enablement
PKI	Public-Key Infrastructure
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirements
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol

SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
STANAG	Standardization Agreement
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

12 References

[1] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[2] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[6] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[7] SERTIT (2020), *The Norwegian Certification Scheme*, SD001E, Version 10.5, SERTIT, 03 December 2020.

[8] SOGIS (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3, Management Committee, January 2010.

[9] System Sikkerhet AS (2022), *Evaluation Technical Report of TNOR Guard* (2022), version 1.1, P-110, System Sikkerhet AS, 18.03.2022.

[10] Thales Norway AS (2022), *Security Target for the TNOR Guard*, version 10.4 Classified, 739 20726 AAAA SC, Thales Norway AS, 09.05.2022.

[11] Thales Norway AS (2022), *Security Target for the TNOR Guard*, version 10.4 Public, 739 20726 AAAA SC, Thales Norway AS, 09.05.2022.

[12] Thales Norway AS (2021), *Guard Release Notes Guard 1.1.3,* version 4.4, 739 20781 AAAA EO, Thales Norway AS, Aug 2021.

[13] Thales Norway AS (2021), *Guard Administration Guide,* version 4.4, 739 20749 AAAA EO, Thales Norway AS, Sept 2021.

[14] Thales Norway AS (2021), *Guard for x86_64 hardware platform Release Notes,* version 1, 739 20833 AAAC EO, Thales Norway AS.