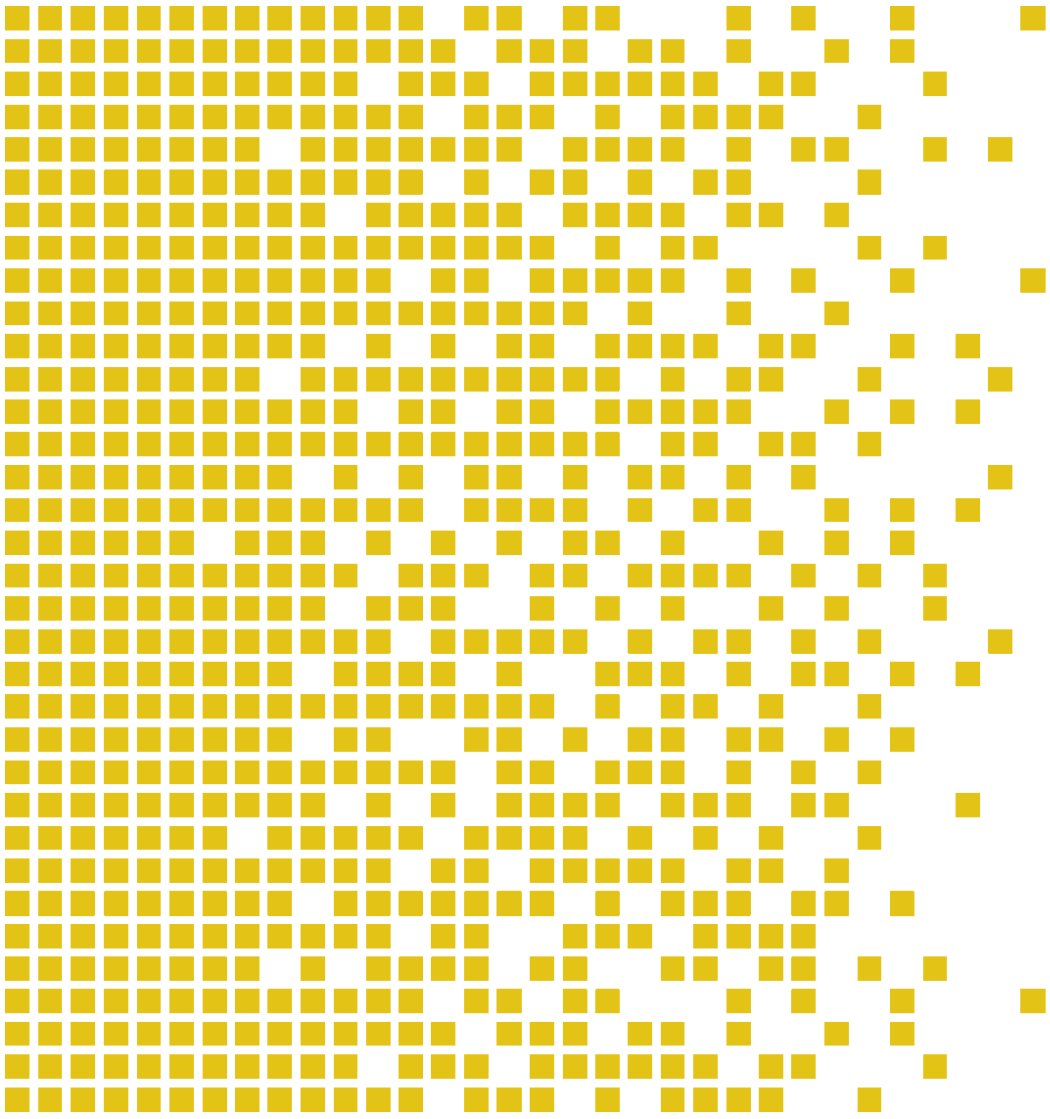
SERTIT-125 CR Certification Report

Issue 1.1 20 June 2023

Expiry date 20 June 2028

XOmail 22.2.0



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 (EVIT) 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 (EVIT) 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

Thales XOmail software is a family of turn-key products tailored for formal military messaging, information handling and transfer in modern C4ISR solutions.

XOmail software version 22.2.0 has been evaluated under the terms of the Norwegian Certification Authority for IT Security [8] and has met the Common Criteria Part 3 (ISO/IEC 15408) [3] conformant components of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 (ISO/IEC 15408) [2] conformant functionality in the specified environment when running on the platforms specified in Annex A.

The evaluation addressed the security functionality claimed in the ST Public [10][9] with reference to the assumed operating environment specified by the ST Public [10]. The evaluated configuration was that specified in Chapter 1 and Annex A. 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	Øystein Hole, SERTIT Lars Borgos, SERTIT
Date approved	20 June 2023
Expiry date	20 June 2028

1 Executive Summary

Prospective consumers are advised to read this report in conjunction with the ST Public [10] which specifies the functional, environmental and assurance evaluation components.

The version of the product evaluated was XOmail 22.2.0.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thales Norway AS.

The XOmail Server software (TOE) enforces controlled message and information flow according to military requirements with integrated multi-level security and mandatory access control. The TOE provides priority handling for messaging, ensuring flash message traffic is delivered with minimal delay even with heavy traffic or congestion.

The TOE preserves message security through consistent interpretation of security labels across all supported messaging protocols, and supports use of digital signatures to ensure message integrity.

The TOE ensures all users are authenticated, and provides user management functions such as automated logout, lockout, and verification. The TOE provides fine grained access control for messaging operations and administrative commands, with complete accountability of all operations.

No Protection Profiles are claimed.

Regarding the usage and the operational environment of the TOE, twelve assumptions are made in the ST Public [10]. In order to counter seventeen threats as described in the ST Public [10], 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 Norconsult AS. The evaluation was performed in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in the document SD001E [8], 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.

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

The evaluation activities were monitored by the certification team. The security claims stated in the ST [9] was confirmed during the evaluation for the selected assurance level.

The basis for producing this Certification Report is the ST Public [10] and the ETR [11].

2 TOE overview

The TOE is the XOmail Server, the main building block of the XOmail product family. The XOmail Server provides secure message handling, transfer, storage, and administration functionality.

The TOE can be deployed in the product configurations below. Multiple configurations may be deployed to a single instance of the TOE.

XOmail Enterprise

Dedicated to meet specific needs for military message handling in strategic and tactical networks at any scale, from autonomous nodes to large-scale Messaging as a Service deployments. XOmail Enterprise is available with a number of options:

- XOmail SMTP Interface Provides the functionality of the standalone XOmail SMTP XD (shown below).
- XOmail ACP 127 Interface Provides the functionality of the standalone XOmail ACP 127 XD (shown below).
- XOmail ACP 145 Interface Provides the functionality of the standalone XOmail ACP 145 XD (shown below)
- XOmail Central Archive Assured automatic storage of all messages.

XOmail product family

XOmail Afloat

Functionality tailored for surface vessels and submarines.

XOmail Broadcaster
Broadcast, Ship-Shore and Maritime Rear Link through STANAG 4406, STANAG 5066 and ACP 127.

XOmail SMTP XD

Provides interoperability with Battle Force E-mail and standard Internet Mail.

XOmail ACP 127 XD

Automatic gateway between ACP 127 and STANAG 4406.

XOmail ACP 145 XD

Implements NATO standard for connecting networks with different security policies and PKI implementations, allowing communication between nations and between national systems and NATO. Unlike the other components, the ACP 145 XD is deployed on a separate instance of the TOE.

XOmail Clients (TOE Environment)

XOmail Admin and XOmail Web Admin clients (TOE Environment) are provided for local or remote administration of the XOmail Server (TOE). The Admin Clients provide the management interfaces required for configuring the XOmail Server.

The XOmail MS Client and XOmail Web Client (TOE Environment) provide thick client and web interfaces for end users.

For use in an evaluated configuration, the XOmail installation must be located in a physically secure environment to which only authorized administrators has access.

3 Security Policy

The TOE has the following main characteristics and functionality:

- Military messaging system built according to STANAG 4406 Ed. 1 and Ed. 2 military extensions.
- Multi-Level Security and Priority attributes embedded at every level of the system.
- Local and remote administration and supervision.
- ACP133 Ed. D Directory Service supporting military messaging. Integrates with an external master Directory Service or acts as a standalone or intermediate Directory Service. Optimized tactical directory shadowing protocol for low-bandwidth unreliable networks.
- Support for integration with a wide range of platform services: PKI, Antivirus, Monitoring and Supervision and software management systems.
- Message integrity protection using S/MIME over STANAG 4406 Ed 2 and E-Mail networks. Integration with third-party Public Key Infrastructures to support certificate validation, including revocation lists and validation of certificate chains.
- Automated printing of messages.
- Tailored for high-availability requirements.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

- PHYSICAL
- PHYSICAL_LOC
- ADM_TRAINING
- AUDIT_REVIEW
- CONFIDENCE
- INVALIDATE
- NOTIFY
- USR_TRAINING
- TIME_SOURCE
- ARCHIVE_DB
- NETWORK
- OS

For details on these assumptions, the reader is advised to look at chapter 5.3 in the ST Public [10].

4.2 Threats Countered

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

- ADM_ERROR
- AUDIT_FAILURE
- COM_INTEGRITY
- DOS
- FAULTS
- MASQUERADE
- MONITORING
- REPLAY
- UNATTENDED
- UNAUTH_ACCESS

For details on these threats, the reader is advised to look at chapter 3.3.1 in the ST Public [10]. The reader should also have a look at the description of the threat agents in chapter 3.2 in the ST Public [10].

4.3 Threats Countered by the TOE environment

The following seven threats are met by the TOE environment

- AUDIT_FAILURE
- DELIVERY
- DOS

- IMPROPER_INST
- POOR_DESIGN
- POOR_IMPL
- UNATTENDED

For details on these threats, the reader is advised to look at chapter 3.3.2 in the ST Public [10].

4.4 Organisational Security Policies

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

- ACCOUNTABILITY
- CLASSIFICATION
- CLEAR
- DAC
- INTEGRITY
- INTERFACE_CONTROL
- MAC
- MARKING
- PROTECTION

All of the policies are compliant with applicable parts of Norwegian security policy [15] and NATO security policy [16]. The TOE Organizational Security Policies are detailed in Chapter 3.4 of the ST Public [10].

5 Vulnerability Analysis and Testing

5.1 Vulnerability Analysis

The evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The analysis was conducted in the week of 17-21 April 2023. No vulnerabilities were found, but see chapter 8 in this report for recommendations for secure usage of the TOE.

5.2 Developer's Tests

The evaluation showed that the Developer has tested the TOE Security Functionality Interfaces (TSFI) as described in the Design Specifications, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. The developer has tested the TOE Security Functionality (TSF) subsystems against the TOE design and the security architecture description.

5.3 Evaluators' Tests

The evaluators performed independent testing of a subset of the TOE Security Functionality (TSF) and verified that the TOE behaves as specified in the design documentation. Confidence in the developer's test results were gained by performing a sample of the developer's tests.

The evaluators devised penetration tests, based on the independent search for potential vulnerabilities and the security functions from the ST.

The main focus of evaluators' tests was on the new functionality in this version of the TOE.

Testing was conducted in the weeks of 11-21 April 2023.

6 Evaluated Configuration

The evaluated TOE, as described in chapter 1 and Annex A, is a software product. It can run on different hardware and operating systems that satisfies the assumptions and organisational policies described in the ST Public [10].

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 [10], as well as the guidance documents referenced in this chapter.

The TOE relies on authentication mechanisms provided by the Operating System. The responsibility of the TOE is to ensure that authentication is performed before any other operation. The Operating System is responsible for performing the actual authentication and to provide secure storage of the authentication tokens.

The TOE relies on the Operating System to provide an API to the cryptographic functions and Public Key Infrastructure required for S/MIME digital signatures. The TOE depends on the Windows Crypto API (CAPI) standardised interface to third party PKI components:

- X.509 certificate lookup
- X.509 certificate chain validation
- Secure use of cryptographic tokens (private keys).

The TOE does not store cryptographic tokens for S/MIME messaging, but relies on accessing the tokens through the Crypto API. The TOE Environment must ensure appropriate secure storage of cryptographic tokens, e.g. in the CAPI database, on smart cards or HSMs.

7 Evaluation Results

The evaluation addressed the requirements specified in the ST Public [10]. The ITSEF reported the results of this work in the ETR [11] on the 02 June 2023.

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.

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

	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

After due consideration of the ETR [11], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the certification team, SERTIT has determined that XOmail 22.2.0 meets the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 4 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

8 Recommendations

Prospective consumers of XOmail 22.2.0 should understand the specific scope of the certification by reading this report in conjunction with the ST Public [10]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST Public [10].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Chapter 1.

The TOE should be used in accordance with the supporting guidance documentation [12], [13], [14] included in the evaluated configuration.

It should be noticed that unprotected exposure of the TOE might lead to the compromise of information or transmitted information (that could be classified or sensitive).

There are some components that are provided by the XOmail Server that shall not be used in a certified configuration. It is therefore recommended that it is verified that these components are not enabled during installation:

- POP3 client access
  XOmail provides experimental support for the POP3 protocol.
- XOmail Sign & Label Add-In for Outlook
  The Sign & Label Add-In for Outlook provides support for STANAG 4406 Ed 2 compatible security labels and S/MIME digital signatures. The Add-In is intended for use in SMTP-based networks that interface MMHS networks via an XOmail SMTP Gateway and is not directly connected to the XOmail Server.

It is recommended that users read the guidance documentation and user manuals thoroughly before starting using XOmail 22.2.0. The manuals contain notes and warnings that bring attention to important information. Also recommended that the users should have experience with system administration and knowledge of administration of networks and computers. It is regarded essential that administrators of the TOE are trained to operate the TOE correctly. The complexity of the guidance documentation can be an issue. The users and the administrator should attend a course and therefore get a complete overview of the documentation and functionality. It is recommended that all administrators attend a course to gain the necessary knowledge necessary to administer the system.

The TOE is a new version of an existing system. When a new version is installed, the configuration information from the old version is imported to the new version. Therefore, it is recommended that an audit/revision of the configuration of the system/TOE is carried out, after installations of new versions.

9 Security Target

The complete Security Target [9] used for the evaluation performed is sanitised for the purpose of publishing. The Public version (Security Target Public [10]) is provided as a separate document. Sanitisation was performed according to the CCRA framework – ST sanitising for publication [5].

10 Glossary

ACP	Allied Communication Publication
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
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
ITSEF	IT Security Evaluation Facility under the Norwegian Certification Scheme
PP	Protection Profile
SERTIT	Norwegian Certification Authority for IT Security
SMTP	Simple Mail Transfer Protocol
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

11 References

[1] CCRA (2017), *Common Critera 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] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

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

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

[9] Security Target, XOmail 22 Security Target, 739 20802 AAAA SC Ed.4, 14 November 2022.

[10] Security Target Public, XOmail 22 Security Target, 739 20802 SC Ed4-public, 14 November 2022.

[11] Evaluation Technical Report for the Evaluation of XOmail22, version 1.1, 02 June 2023.

[12] XOmail User's Guide, 739_20529_abaa_eo_ed30

[13] XOmail Administrator's Guide, 739_20561_abaa_eo_ed30

[14] XOmail Installation and Configuration Guide, 712_27734_axaa_eo_ed38

[15] Lov om nasjonal sikkerhet (Norwegian Security Act), LOV 2018-06-01 nr 24.

[16] C-M(2002)49, Security Within the North Atlantic Treaty Organisation (NATO), 17 June 2002.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

XOmail 22.2.0 software

The TOE runs on standard 64bit PC platforms, on physical or virtualized environments.

The TOE supports the following operating systems:

Application	Operating systems
XOmail Server	Windows Server 2016 Windows Server 2019 Windows Server 2022

The XOmail Central Archive requires an external DBMS. The following databases are supported:

PostgreSQL 15.0 (recommended)
PostgreSQL 14.5
Oracle Database 19

Refer to the manufacturer’s documentation for additional information.

TOE Documentation

The supporting guidance documents evaluated were:

[a] XOmail User's Guide, 739_20529_abaa_eo_ed30

[b] XOmail Administrator's Guide, 739_20561_abaa_eo_ed30

[c] XOmail Installation and Configuration Guide, 712_27734_axaa_eo_ed38

TOE Configuration

The following configuration was used for testing: