SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-092 CR Certification Report

Issue 1.0 14 November 2017

XOmail 21.1.1, product id 712 27734 AFAA 50

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009E VERSION 1.1 01.07.2015

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

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. [*]

* Mutual Recognition under the CC recognition arrangement applies to EAL 2 and ALC_FLR.3

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 the SOGIS MRA recognition agreement applies to EAL 4 but not to ALC_FLR.3

Contents

1 Certification Statement

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 21.1.1 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL4 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Jørn Arnesen Head of SERTIT
Date approved	14 November 2017

2 Abbreviations

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
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target, Thales XOmail Security Target, 739 20725 AAAA SC Ed. 4, 2 May 2017.

[2] Security Target, Thales XOmail Security Target, 739 20725 AAAA SC Ed. 4-public, 8 May 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[5] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[6] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[8] Evaluation Technical Report for the Common Criteria EAL4 Evaluation of XOmail 21, version 1.2, 10 November 2017.

[9] SERTIT-092 Review Form no1, version 1.2

[10] Administrator’s guide XOmail 21.1, 739 20561 ABAA EO, v 24.1

[11] Installation and Configuration Guide 712 27734 AABA EO, v 31.2

[12] User's Guide 739_20529_abaa_eo_ed23, v 23

[13] SOGIS MRA, Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3.0, January 8th 2010.

[14] ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of XOmail software version 21.1.1 to the Sponsor, Forsvarsmateriell, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1][2] which specifies the functional, environmental and assurance evaluation requirements and components.

4.2 Evaluated Product

The versions of the product evaluated was XOmail software version 21.1.1.

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

The TOE is the server component in a military messaging system that provides the following functionality:

- Secure message transfer between the various components in the XOmail messaging system or connected systems
- Enforce mandatory access control when handling messages from domains with different security policies

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

XOmail Server is available in multiple configurations, each of which is deployable as components of the XOmail product family. Each component contains a shared security core provided by the TOE. All components except the ACP 145 Gateway may be configured in parallel on a TOE installation.

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.
- A limited ACP133 Ed. D Directory Service and the ability to interact with an external master Directory Service or act as a standalone or intermediate Directory Service. Optimized tactical directory shadowing protocol for low-bandwidth unreliable networks.

- Supports antivirus integration
- Message integrity protection using S/MIME over STANAG 4406 Ed 2 and Internet Mail networks. Integration with third-party Public Key Infrastructures to support certificate validation, including revocation lists and validation of certificate chains.
- Support for automated installation
- Automated printing of messages.
- Clustering support for enhanced availability and reliability.

4.4 Protection Profile Conformance

The Security Target[1][2] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1][2] specified the assurance components for the evaluation. The assurance incorporated predefined evaluation assurance level EAL4, augmented with ALC_FLR.3. Common Criteria Part 3[5] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[3].

4.6 Security Policy

The TOE security policies are detailed in the ST[1][2]

4.7 Security Claims

The Security Target[1][2] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[4]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- **TT.ADM_ERROR**
  Improper administration results in a security policy violation
- **TT.AUDIT_FAILURE**
  An attacker may cause audit records to be lost or modified. Attackers may also cause audit overflow, so that important audit records seemingly disappear
- **TT.COM_INTEGRITY**
  The integrity of transmitted information may be compromised due to deliberate or accidental insertion or modification. New information may be inserted onto the network, or existing traffic modified in transit. An attacker may modify the security label, priority, recipients, originators or other attributes of the message and its data

- **TT.DOS**
  An attacker may cause system resource exhaustion, resulting in delayed message handling or the inability of authorized users to access system resources
- **TT.FAULTS**
  The TOE crashes or deadlocks due to software or hardware errors
- **TT.MASQUERADE**
  An attacker tries to masquerade as a trusted entity in order to by mistake be trusted with classified information
- **TT.MONITORING**
  An attacker monitors activities and actions performed on classified information. Such activities and actions include authentication and creating, viewing, modifying and deleting classified information. The monitoring activities can be performed at multiple levels, like screen monitoring or network monitoring
- **TT.REPLAY**
  A malicious process or user gains access by replaying authentication data
- **TT.UNATTENDED**
  A malicious user may gain unauthorized access to an unattended session
- **TT.UNAUTH_ACCESS**
  Unauthorized access to identified assets may occur. Methods of attack covered by this threat are brute force attacks, session hijacking, authentication data cracking, privilege escalation and social engineering

4.9 Threats Countered by the TOE's environment

- **TE.AUDIT_FAILURE**
  An attacker may cause audit records to be lost or modified
- **TE.DELIVERY**
  An attacker may try to replace parts (or the complete) TOE with a malicious version
- **TE.DOS**
  An attacker block authorized users from system resources via a resource exhaustion denial of service attack
- **TE.IMPROPER_INST**
  The TOE is installed and/or configured in a manner that undermines security
- **TE.POOR_DESIGN**
  Unintentional or intentional errors in the design of the TOE may exist. Such design flaws includes: inability to adequately separate information based on SP, HCL or NHC and inability to associate correct security attributes with the users
- **TE.POOR_IMPL**
  The developer has failed in implementing the TOE according to the design or security flaws are present in the TOE
- **TE.UNATTENDED**
  A malicious user may gain unauthorized access to an unattended session

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered nment.

4.11 Environmental Assumptions and Dependencies

The environmental assumptions are described in the ST[1][2], chapter 11.1.3.

4.12 IT Security Objectives

The IT security objectives for the TOE are described in the ST[1][2], chapter 8.1 and 8.2.

4.13 Non-IT Security Objectives

The IT security objectives for the TOE are described in the ST[1][2], chapter 8.3.

4.14 Security Functional components

- FAU_ARP.1 Security alarms
- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAA.1 Potential violation analysis
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.3 Action in case of possible audit data loss
- FAU_STG.4 Prevention of audit data loss
- FCO_NRO.1 Selective proof of origin
- FCO_NRR.1 Non-repudiation of receipt
- FCS_COP.1 Cryptographic operation
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Access control functions
- FDP_ETC.2 Export of user data with security attributes
- FDP_IFC.2 Complete information flow control
- FDP_IFF.2 Hierarchical security attributes
- FDP_ITC.2 Import of user data with security attributes
- FDP_RIP.2 Full residual information protection
- FDP_UIT.1 Data exchange integrity
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_UAU.2 Timing of authentication
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UAU.6 Re-authenticating
- FIA_UID.2 Timing of identification
- FIA_USB.1 User-subject binding
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization

- FMT_MTD.1 Management of TSF data
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_FLS.1 Fail secure
- FPT_RCV.1 Manual Recovery
- FPT_RCV.2 Automated recovery
- FPT_RCV.4 Function recovery
- FPT_TDC.1 Inter-TSF basic TSF data consistency
- FPT_TST.1 TSF testing
- FRU_FLT.2 Limited fault tolerance
- FRU_PRS.1 Limited priority of service
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment

4.15 Security Function Policy

The XOmail Server software (TOE) is built with multi-level security and mandatory access control for all message flows and stored information objects. The TOE provides priority handling for messaging, ensuring flash message traffic is delivered with minimal delay even with heavy traffic or congestion.

The backbone of XOmail is the implementation of the widely accepted NATO STANAG 4406 messaging standard, as well as seamless integration with legacy ACP 127 systems, tactical network protocols, and Internet Mail (SMTP) based systems.

TOE functionality can be extended through the use of APIs, which allow third-party applications access to the messaging infrastructure.

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.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[6]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1][2], which prospective consumers are advised to read. To ensure that the Security Target[1][2] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[5] and the Common Evaluation Methodology (CEM)[7].

SERTIT monitored the evaluation which was carried out by the Norconsult EVIT Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[8] to SERTIT on the 10 November 2017. Following the EVIT response[9] to a request for further information SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1][2] with reference to the assumed operating environment specified by the Security Target[1][2]. The evaluated configuration was that specified in 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.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[5]. 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_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	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

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1][2]. The results of this work were reported in the ETR[8] under the CC Part 3[5] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1][2] chapter 8.3 provided by the developer. The Operational User Guidance and Preparative Procedures [10][11][12] describes all necessary steps to configure the TOE in the certified configuration

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

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE’s security functions.

5.5 Vulnerability Analysis

The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis was done, revealing several potential vulnerabilities based on an attacker with Basic-Enhanced attack potential

- A design and implementation review on the TOE was done to identify weaknesses

- The evaluator identified vulnerabilities that where candidates for further testing
- A vulnerability analysis based on the design and implementation review results and the validation test results of security features, was performed
- The evaluator has devised a penetration test plan, based on the result of the independent vulnerability analysis
- Practical penetration tests are performed according the penetration test plan

The penetration testing effort shows that an attacker with Basic-Enhanced attack potential is unable to breach the TOE security functions.

5.6 Developer's Tests

The developers testing of the TSF's together with the independent testing of the TSF's by the evaluator shows that the TOE behaves as described in the ST and that the developer testing efforts is extensive and that the TSF satisfies the TOE security functional requirements.

Each requirement in the developer's functional specification has a corresponding test. Additionally, a few test procedure documents define additional tests. This is done where supporting tests is required or preferred.

5.7 Evaluators' Tests

The evaluator's responsibility for independent testing is required by the ATE_IND class. Since developer's testing procedures were found to be extensive and thorough, the choice was made to perform the evaluator independent testing by repeating a sample of the developer's tests, using both evaluators and developer's tools, at the premises of the developer. The evaluator employs a sampling strategy to select developer tests to validate the developer's test results.

The Independent tests was performed to verify the core functionality of the TOE. The independent tests were partly based on retests with another stress level of the TOE. And some tests of core functionality with other inputs than the ones done by the developer

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[8], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that XOmail software version 21.1.1 meet the 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.

6.2 Recommendations

Prospective consumers of XOmail software version 21.1.1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1][2]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Type	Name	Version	Identification
Software	XOmail	21.1.1	71227734 AFAA 50
Manuals	Administrator's guide XOmail 21.1	24.2	739 20561 ABAA EO
	Installation and Configuration Guide	31.2	712 27734 AABA EO
	User's Guide	23	739_20529_abaa_eo

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The following configuration was used for testing:

XOmail Client

64-bits operating systems to test the XOmail Client on:

- Microsoft Windows 7
- Microsoft Windows 2012 R2 (CC certified GPOS PP v4.1)

XOmail Server

64-bits operating systems to test the XOmail Server on:

- Microsoft Windows 2012 (not prioritized) 2012 R2 (CC certified GPOS PP v4.1)

XOmail Admin

64-bits operating systems to test the XOmail Administration Client on:

- Microsoft Windows 7
- Microsoft Windows Server 2012 R2 (CC certified GPOS PP v4.1)

Java Runtime Environment

JRE for XOmail Administration Client and XOmail Patch Manager:

- Java Runtime Environment Version 1.8 Update 131

Hardware and firmware items

Required hardware for each tester (for running virtual computers on):

- PCs, minimum 8GB RAM, minimum 300 GB free disk space, B-net LAN connection

Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects 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 of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: THALES Norway AS

Product Name: XOmail software

Type of Product: Messaging system

Version and Release Numbers: 21.1.1, product id 712 27734 AFAA 50

Assurance Package: EAL 4 augmented with ALC_FLR.3

Evaluation Criteria: Common Criteria v. 3.1 R4

Name of IT Security Evaluation Facility: Norconsult EVIT

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-092 CR Issue 1.0, 14. November 2017

Certificate Identifier: SERTIT-092 C

Date Issued: 14. November 2017

K Kvassnes
Kjartan Jæger Kvassnes
Certifier

Lars Borgos
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up EAL 2 and ALC_FLR only.

SOGIS MRA recognition for components up to EAL 4.