SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*
SERTIT er en del av Nasjonal sikkerhetsmyndighet *SERTIT is a part of Norwegian National Security Authority*

SERTIT-092 MR Maintenance Report

Issue 2.0 25.05.2022

XOmail version 21.1.3

MAINTENANCE REPORT - SERTIT STANDARD REPORT TEMPLATE ST 010E VERSION 1.0 12.04.2021

Contents

1 Introduction

The TOE identified in this Maintenance Report was assessed according to the Assurance Continuity Requirements [1] set out by the CCRA and the Impact Analysis Report (IAR) [2] from the Security Developer Analyst at Thales Norway AS. In accordance with those requirements, the IAR [2] describes the changes made to the TOE.

The baseline for this Assurance Continuity Assessment was the certified TOE with Certification Report number SERTIT-092 CR [5], and the belonging Security Target and the Evaluation Technical Report.

The changes in the TOE is analysed [6] by the ITSEF Norconsult AS.

After examining all documents and evidences provided to SERTIT, the overall conclusion is that the changes made to the TOE is categorized as minor. Therefore, Certificate Maintenance is granted.

This Maintenance Report for the XOmail version 21.1.3 is an addendum to the Certification Report [5].

2 Description of Changes

Maintained TOE identification:

Name:	XOmail
Identity:	712 27734
Variant:	AFAA 53
Version:	21.1.3

The XOmail 21.1.x version branch is subjected to tight configuration control while in a Common Criteria assurance maintenance phase. The process is documented in the XOmail software Development Plan. The main adaptions are:

- Work Package Managers and Software Engineers are made aware of limitations on allowed changes on the TOE. Both Work Packages and Change and Problem Reports are reviewed prior to starting work, with only required changes being allowed to the TOE on the 21.1 branch.
- All Change and Problem Reports are inspected and approved by the Software Change and Control board after implementation.
- A designated person from the Code Review Board is responsible for all QA on source code modifications.

The IAR [2] chapter 2 lists the changes to the certified TOE. Each change is identified and clearly and adequately described. This report lists a condensed list of changes suitable for publication. A complete list of the changes relevant to the TOE can be found in the IAR [2]. The IAR [2] also lists changes that are handled according to the ALC_FLR Flaw Remediation process and changes to non-TOE XOmail components.

There are no changes to the security objectives for the TOE [4].

2.1 Hardware related changes:

None

2.2 Software related changes

New functionality Category	Description
Address directory management	LDIF based address import: New utility for import of addresses from a RFC 2849 LDIF file (WP236, ER-20398, ER-20401, ER-20402). Improved address synchronization to clients (ER-20238)
Audit and logging	Improved alarms and error messages related to low-level I/O channel monitoring (ER-20243), and improved filtering (ER-20318). Support logging of SNMPv3 messages (ER-20323)
Authentication	Extend existing Kerberos single sign-on to Admin client (ER-20087)
Configuration	Added new option for disabling an external connection temporarily (ER-18696) Number of originators for departments increased to 25 (ER-20358)
Hardware	Added support for Sunhillo PCE335 X.25 NIC (ER-20271)
Message processing	Improvements for tactical messaging scenarios (ER-20124, ER-20392, ER-20272). Improved folder organization support for shared message storages (ER-20196) New minor configuration options for specialized usage scenarios (ER-20362, ER-20382) and Special Handling messages (ER-20187)
Messaging protocols	Improved configurability and monitoring for ACP127 channels (ER-20222, ER-20374, ER-20375) Improvements in SMTP E-mail processing (ER-20242)
Reliability	Optional support for more frequent database flushing to disk (ER-20297)
Other	Support for “beta” prerelease version numbers (ER-20417)

Error corrections Category	Description
Authentication	Corrected Kerberos single sign-on for mixed IPv4/IPv6 environments (ER-20559)
Audit and logging	Corrected misleading “Security” reference in “Transmission problem” alarms (ER-13565) Corrections to log attributes and supporting text (ER-20264)

	Corrections for usability issues (ER-20292, ER-20446, ER-20503) Crash while generating SNMPv3 (ER-20276)
Configuration	Fix crash when processing large address lists (ER-20393) Minor usability improvements (ER-20472)
Installation	Misc errors in automatic installation and configuration scripts (ER-20456)
Message presentation	Several minor corrections related to presentation of message attributes (ER-19652, ER-20487).
Message processing and protocol issues	Corrected errors for manual message operations (ER-20186, ER-20262), STANAG 4406 (ER-12254, ER-20063), ACP127 (ER-20240, ER-20269, ER-20304, ER-20492, ER-20523, ER-20525), distribution (ER-20255, ER-20256, ER-20258, ER-20288, ER-20312), SMTP e-mail (ER-20261, ER-20306), address list expansion (ER-20347), archive retrieval (ER-20572), and other messaging and directory shadowing errors (ER-20448, ER-20462, ER-20480, ER-20496, ER-20526, ER-20553).
Network error handling	Improved handling of unexpected user client disconnection (ER-19982)
Printing	Corrected errors in customer specific print format and minor simplifications to print format configuration (ER-20468)
Traffic management	Corrections related to management of message queues (ER-19620)
User interface	Corrected error when updating user profile configuration (ER-20555)

There are no changes to the certified TOE development environment.

3 Affected Developer Evidence

The IAR [2] chapter 3 list all of the affected items of the developer evidence for each change in the certified TOE in a structured and clear manner. All items of the developer evidence that has been modified in order to address the developer action elements are identified. The developer has described the required modifications to the affected items of the developer evidence in chapter 4 of the IAR [2].

4 Conclusion

The IAR [2] provided by the developer clearly presented the changes to the certified TOE scope, and analyzed impacts to all the assurance classes following the requirements described in [1].

The analysis in the IAR [2] is intended to demonstrate that the cumulative impact on assurance is minor.

The TOE's security functionality described by the Security Function Requirements specified in the ST [4] are not affected by these changes.

The nature of the changes to the TOE is classified as minor changes in the IAR [2], and SERTIT finds to support this conclusion.

SERTIT therefore concludes that the XOmail version 21.1.3 is appropriate for Certificate Maintenance.

4.1 Recommendations

The maintained TOE should be used with a number of environmental considerations as outlined in the Security Target [4].

Further, the maintained TOE should be used in accordance with the supporting guidance documentation.

Certificate Maintenance team	Lars Borgos Øystein Hole
Date approved	25.05.2022

5 References

[1] CCRA (2012), *Assurance Continuity: CCRA Requirements*, version 2.1, June 2012, CCRA.

[2] Thales Norway AS (2021), *Impact Analysis Report for XOmail 21.1.3 SERTIT-092*, 739 20819, revision 1, 12.03.2021, Thales Norway AS.

[3] Thales Norway AS (2021), *XOmail 21 Security Target*, 739 20725 AAAA SC, Edition 5.1, 05.03.2021, Thales Norway AS.

[4] Thales Norway AS (2021), *XOmail 21 Security Target,* 739 20725 AAAA SC*,* Edition 5.1-public, 05.03.2021, Thales Norway AS.

[5] SERTIT-092 CR *Certification Report,* Issue 1.0, 14 November 2017, SERTIT.

[6] Norconsult AS (2022), *Evaluation of Impact Analysis Report for XOmail 21.1.3*, issue 1.1, 11.05.2022, Norconsult AS.