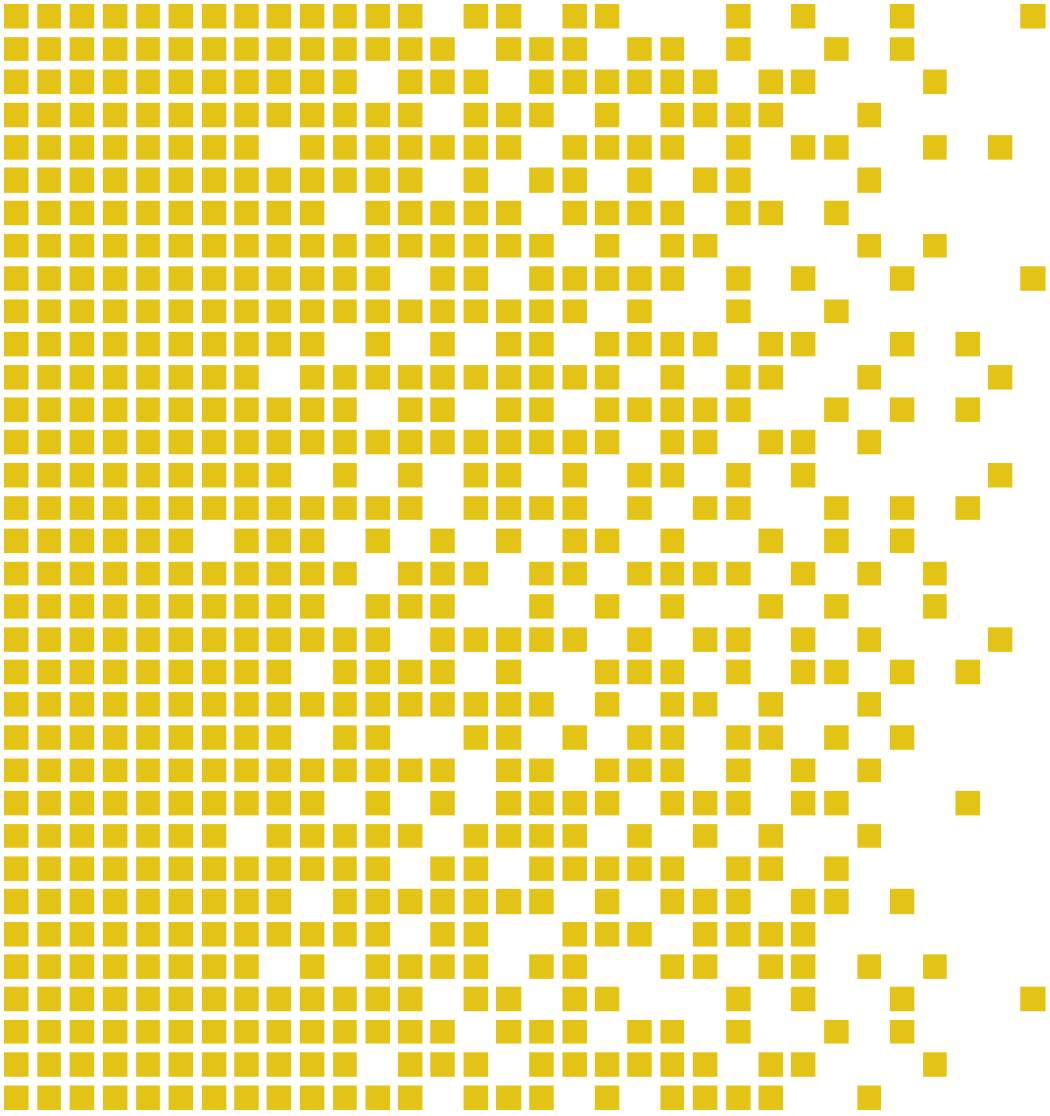
SERTIT-092 MR Maintenance Report

Issue 1.0, 15 November 2018.

XOmail 21.1.1, product id 712 27734 AFAA 52



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

1. Introduction

The certified TOE was evaluated according to Common Criteria version 3.1 R4 and Evaluation Assurance Level EAL 4 augmented with ALC_FLR.3.

The IT Security Evaluation Facility (ITSEF/EVIT) was Norconsult AS.

The sponsor/developer is Thales Norway AS. The Security Developer Analyst at Thales Norway AS for this maintenance process was Christian Tellefsen.

Thales Norway AS submitted an Impact Analysis Report (IAR) [5] to SERTIT on February 2nd 2018. The IAR [5] is intended to satisfy requirements outlined in version 2.1 of the Common Criteria document Assurance Continuity: CCRA Requirements [CCDB-2012-06-01]. In accordance with those requirements, the IAR [5] describes the changes made to the TOE.

2. Certified TOE identification:

XOmail 21.1.1, product id 712 27734 AFAA 50

Documents:

[1] Security Target, Thales XOmail Security Target, 739 20725 AAAA SC Ed. 4, 8 May 2017.
[2] SERTIT-092 CR Certification Report, Issue 1.0, 14 November 2017
[3] SERTIT-092 C Certificate, Issue 1.0, 14 November 2017
[4] Evaluation Technical Report, Common Criteria EAL4 Evaluation of XOmail 21 Issue1.2 10.November 2017

3. Maintained TOE identification

XOmail 21.1.2, product id 712 27734 AFAA 52

Documents:

[5] Impact Analysis Report XOmail 21.1.2 SERTIT-092 8 February 2018
[6] Security Target, Thales XOmail Security Target, 739 20725 AAAA SC Ed. 5, 26 January 2018
[7] SERTIT-092 MR Maintenance Report, Issue 1.0, 15 November 2018 (This document).

4. Description of Changes

The XOmail 21.1.x version branch is subject to tight configuration control while in a Common Criteria assurance maintenance phase. The process is documented in the Thales XOmail Software Development Plan.

The IAR [5] chapter 2 lists a number of changes to the certified TOE. Each change is identified and clearly and adequately described. This report list the changes relevant to the TOE, leaving out flaw remediation and changes to non-TOE XOmail components.

Change ID	Description
WP221	Update XOmail Outlook Add-In for Outlook 2016
WP222	“Set seen” in Transit Log The XOmail Admin and the XOmail Client introduce the ability to mark Transit Log entries with error-status as seen/handled.
WP225	Message tracking New ability for operators to track messages. This function collates information from Transit Log and System Log and presents an overview of where a message has ended up, such as which local storages the messages has been delivered to, if it has been trapped, and processing status for messages towards an ACP 127 domain.
WP226	Intership XOmail introduces the ability to send messages in Transmission Pool on “Intership” format. The “Intership” format uses CallSigns in ACP 127 format lines 2 and 3.
WP227	Network Management improvements The XOmail product introduces several minor updates in the handling of Network Management alarms.
WPT-1570	Message Not Handled alarm improvement (part of WP227) Messages not handled within a specified deadline cause a “message not handled” alarm. The details provided in the alarm are configurable. This CPR provides a new option to display whether the message has been opened.
ER-19922	Admin Guide refers to obsolete configuration file Minor update to guidance documentation.
ER-19941	Removed a workaround for supporting legacy versions of Outlook, where nested message attachments could not be displayed.
ER-19944	Single Sign-On does not work first time after reboot Minor update to guidance documentation.
ER-19971	Correct slow notification to user on reception of specific messages originating from ACP 127.
ER-19981	Reroute from Broadcast Reception did not preserve SCD/TSN.
ER-19990	BRRL matching does not work for nested AIGs Error correction related to expansion of nested address lists on the ACP 127 Gateway.
ER-19992	BRRL matching does not properly handle exempt addresses Error correction related to exempt addresses when expanding address lists on the ACP 127 Gateway.
ER-19997	Alternative recipient on send timeout does not work It is possible to configure the TOE to forward messages automatically if they are not handled within a specified time limit. This change corrects a problem related to this functionality.
ER-20007	ADatP-3 message without valid MSGID not delivered to ACP127 channel ADatP-3 is a text based format, but it is specially handled by some connected systems. The TOE will detect ADatP-3 content and mark these attachments. Invalid ADatP-3 messages would be stopped from being sent on ACP 127 channels. This error correction ensures that ADatP-3 messages, or messages that could be incorrectly identified as ADatP-3, are transferred as text, as they may still have value to the recipient.

ER-20023	No error indication if distribution fails to create DST element As part of debugging an unrelated problem, it was discovered that error logging was not implemented for a specific fault scenario.
ER-20024	VITAL-messages should be explained better in the Martime Gateway manual Minor change to guidance documentation.
ER-20031	Should support configurable alarm visibility This is a minor change to allow filtering of alarms based on a user's associated user template. This allows tailoring of user interfaces.
ER-20033	SMTPGW: Set bodypart content-type to us-ascii if only us-ascii characters are present in text bodypart This minor change ensures that the correct content type is used for SMTP text bodyparts containing only US-ASCII characters.
ER-20037	Missing Section Merge timeout on 64-bit platform Minor error correction to fix problem where some messages could not be joined during reception.
ER-20052	Documented -b option to batch load scripts not supported on Windows Minor change to guidance documentation.
ER-20064	Invalid STANAG 4406 format for CA search response messages Corrected low level protocol error which caused interoperability errors..
ER-20068	TLS improvements Added STARTTLS support for incoming and outgoing traffic, in addition to existing support for TLS over a dedicated port. Existing TLS support and libraries was reused. Additional logging was introduced to aid operational troubleshooting.
ER-20086	Error correction to prevent some SMTP messages to be truncated on reception.
ER-20089	EO 712 27734 Installation and configuration guide: Improved user guidance to avoid common pitfalls in Windows when using software based keys. This should help customers avoid a common problem where keys are incorrectly stored in MS CAPI and cannot be used by the TOE for SHA 256 operations.
ER-20125	List New operation in Remote Delivery Queue fails Minor correction to avoid truncating an integer value.
ER-20129	Support for marking all incoming messages from external STANAG 4406 and SMTP servers as transient Transient messages were only supported for ACP 127 or P_mul connections. Transient messages are used when no delivery reports are required, such as for position updates or short-lived sensor data. This change introduces a new configuration variable which will enable all STANAG 4406 and SMTP messages to be marked with a "Transient" attribute.
ER-20136	Single Sign-On settings missing from site.cfg_ex Improved user guidance.
ER-20142	Minor correction to prevent fault when logging on using single sign-on from an XOmail Client located on the same host as the XOmail Server (TOE).
ER-20162	Removed support for legacy Exchange servers. The change affects new TOE installations only.
ER-20185	False alarm: "DIST: failed to create DST in storage" during delivery Corrected a minor array that would cause holes in journal numbering. The fault occurred when messages was distributed multiple times to the same storage.

There are no changes to the development environment.

5. Affected Developer Evidence

The IAR[5] chapter 3 list all of the affected items of the developer evidence for each change in to the certified TOE 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.

There are no changes to the development environment.

6. Conclusion

The IAR[5] provided by the developer clearly presented the changes to the certified TOE scope, and analysed impacts to all the assurance classes following the requirements described in [CCDB-2012-06-01].

All changes made to the certified TOE are reviewed by the XOmail Software Change Control Board (SCCB) to ensure a minimal impact on assurance state, as required by the defined configuration management process.

Each Change and Problem Report is considered by the SCCB prior to implementation. Each implementation change has been reviewed by a designated Code QA responsible and document changes are reviewed by designated review boards.

Following testing, the SCCB has considered and approved each change.

As no changes have affected the TSF, the analysis document “MHS Security Concept and Design” is unchanged for the updated TOE.

There are a number of changes between the TOE versions 21.1.1 and 21.1.2. The analysis in the IAR[5] 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 [1] is not affected by these changes. Through functional testing of the TOE, assurance gained in the original TOE certification was maintained. As changes to the TOE has been classified as minor, it is the conclusion of SERTIT that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

Certificate Maintenance team	Arne Høye Rage, SERTIT Kjartan Kvassnes, SERTIT
Date approved	15 November 2018