



SERTIT

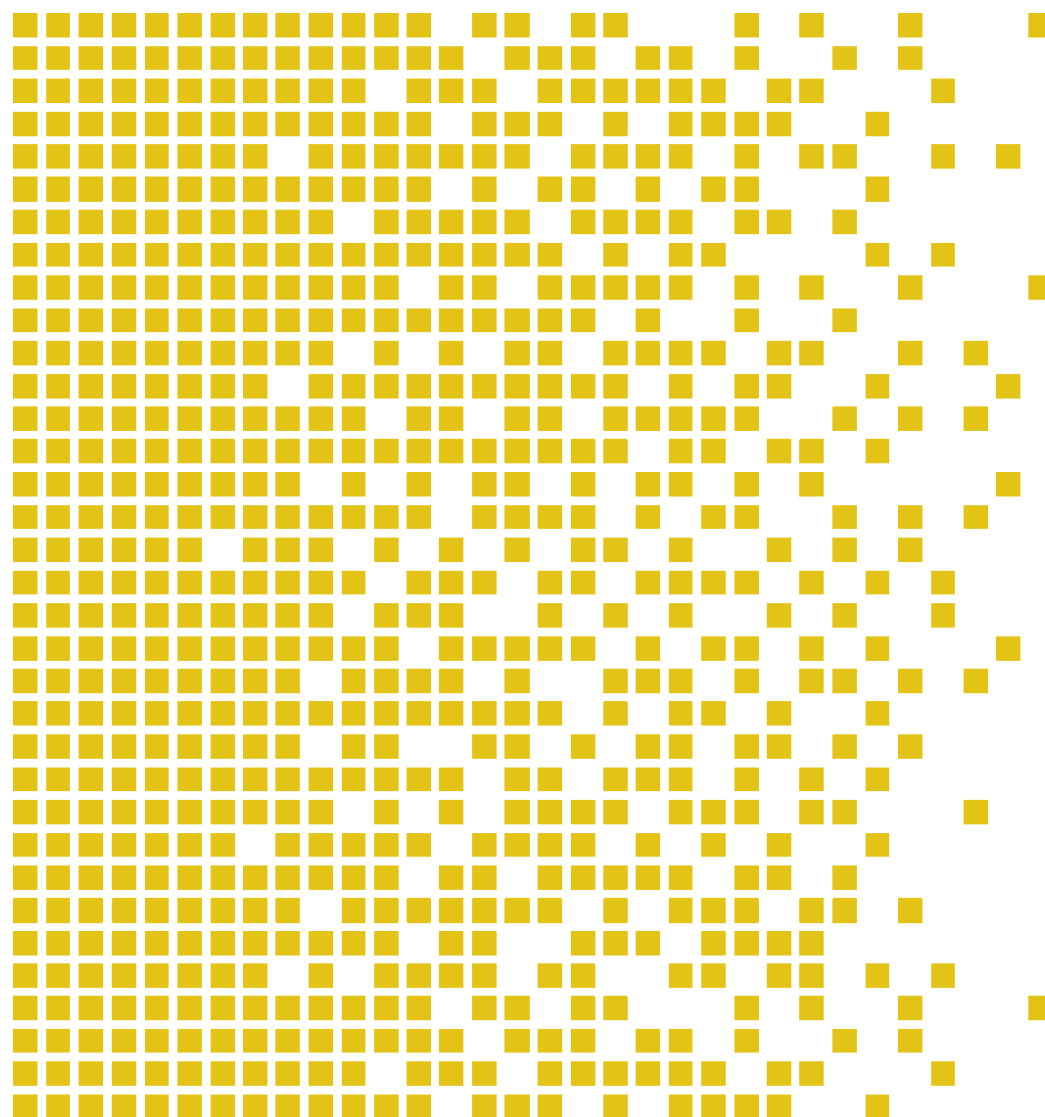
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*
SERTIT er en del av Nasjonal sikkerhetsmyndighet *SERTIT is a part of Norwegian National Security Authority*

SERTIT-120 MR Maintenance Report

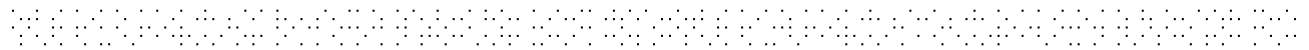
Issue 1.0 13. May 2025

Exp date 12. May 2027

TNOR Guard 1.1.5



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





Contents

1	Introduction	5
2	Description of Changes	6
2.1	Hardware related changes	6
2.2	Software related changes	7
3	Affected Developer Evidence	8
4	Conclusion	9
4.1	Recommendations	9
5	References	10



1 Introduction

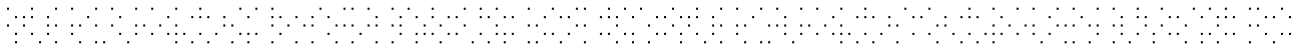
The TOE identified in this Maintenance Report was assessed according to the Assurance Continuity Requirements [1] set out by the CCRA and the Impact Analysis Report (IAR) [2] from the Security Developer Analyst at Thales Norway AS. In accordance with those requirements, the IAR [2] describes the changes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

The baseline for this Assurance Continuity Assessment was the certified TOE with Certification Report number SERTIT-120 CR [5], and the belonging Security Target and the Evaluation Technical Report.

The changes in the TOE are analysed [6] by the ITSEF Nemko System Sikkerhet AS.

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

This Maintenance Report for the TNOR Guard version 1.1.5 is an addendum to the Certification Report [5].



2 Description of Changes

Maintained TOE identification:

Name: TNOR Guard

Identities:

- STANAG 4406 Message Guard – 3AQ 28150
- SMTP Message Guard - 3AQ 28151
- XMPP Chat Guard - 3AQ 28152
- SOAP XML Guard - 3AQ 28153

Variant: B and C

Version: 1.1.5

The TNOR Guard 1.x.x version branch is subjected to tight configuration control while in a Common Criteria assurance maintenance phase. The process is documented in the XMail Software Development Plan. The main adaptations 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.
- 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 components:

- Guard Configuration Tool
- Command Line Tools
- PikeOS
- ElinOS
- Other components

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

2.1 Hardware related changes

There are no hardware related changes.

2.2 Software related changes

Error corrections and improvements

Category	Description
Stability and performance	Corrections for faults and degraded performance during high traffic scenarios.
Audit and logging	Improved scalability for handling very large logs (above 30k entries).
Functional corrections	A number of minor functional corrections to operational use and management.
Configuration	Misc improvements to installation and configuration tools.



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 analysed 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 TNOR Guard version 1.1.5 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	Øystein Hole
Date approved	13. May 2025



5 References

- [1] CCRA (2024), Assurance Continuity: CCRA Requirements, version 3.1, 29.02.2024, CCRA.
- [2] Thales Norway AS (2024), Impact Analysis Report for TNOR Guard 1.1.5 SERTIT-120, 739 20854 AAAA DE, revision 2, 30.10.2024, Thales Norway AS.
- [3] Thales Norway AS (2022), TNOR Guard 1.1.3 Security Target, 739 20726 SC, Edition 10.4, 09.05.2022, Thales Norway AS.
- [4] Thales Norway AS (2022), TNOR Guard 1.1.3 Security Target, 739 20726 SC, Edition 10.4-public, 09.05.2022, Thales Norway AS.
- [5] SERTIT-120 CR Certification Report, Issue 1.0, 12 May 2022, SERTIT.
- [6] Nemko System Sikkerhet AS (2024), Security Audit Report November 2024 TNOR Guard 1.1.5 (SERTIT 120) IAR Thales Norway, issue 1.0, 22.11.2024, Nemko System Sikkerhet AS.