SERTIT

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

SERTIT-060 MR Maintenance Report

Issue 1.0, 29 November 2018.

TSF 201
HW: 3AQ 25960 BAAA rev E
SW: 3AQ 25950 AAAA rev 2.5

1. Introduction

The certified TOE was evaluated according to Common Criteria version 3.1 R4 and Evaluation Assurance Level EAL 5 augmented with ALC_FLR.3.

The IT Security Evaluation Facility (ITSEF/EVIT) was NTT Com Security (Norway) AS (Now System Sikkerhet AS).

The sponsor/developer is Thales Norway AS. The Security Developer Analyst at Thales Norway AS for this maintenance process was Odd Arne Samdal.

Thales Norway AS submitted an Impact Analysis Report (IAR) [5] to SERTIT on November 19th 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:

Documents:

[1] Trusted Security Filter TSF 201, Security Target 3AQ 25940 AAAA Revision 2, 14 September 2015.
[2] SERTIT-060 CR Certification Report, Issue 1.0, 01 February 2016
[3] SERTIT-060 C Certificate, Issue 1.0, 01 February 2016
[4] Common Criteria EAL5 Evaluation of Trusted Security Filter (TSF 201) Evaluation Technical Report v 1.1, 29.01.2016

3. Maintained TOE identification

TSF 201 Hardware 3AQ 25960 BAAA E

TSF 201 Software 3AQ 25950 AAAA 2.5

Documents:

[5] Impact Analysis Report for TSF201 3AQ 25940 AAAA rev 1, 9 November 2018
[6] Security Target, Security Target for TSF 201 3AQ 25940 AAAA 377 rev 3, 2 November 2018
[7] SERTIT-060 MR Maintenance Report, Issue 1.0, 29 November 2018 (This document).

4. Description of Changes

Software related changes:

Change id	Change description
TSF-86	**New function: Confiqurable Diode Mode Low to Hiqh** The Diode mode function controls the traffic from black to red side and can be set to "Closed" or “Open". When the Diode mode function is set to "Closed" the TSF 201 will block all traffic from black to red side.

	Associated JIRA: TSF—154.
TSF-142	**New function: NAT Low Source Address** The NAT function controls which IP address that shall be used as source address in the IP packets that come from black side and shall be sent into the network on red side. When the NAT function is set to “Enabled” the TSF 201 will change the source address in the IP packets to the red IP address of the TSF 201.
TSF-150	**Adaptions to the new functions** The name of the default filter for TSF 201 red to black communication is changed from “Diode" to “Closed”. The GUI pages Filter and Profiles are redesigned.
TSF-151	A logical error is found and fixed in the KAT tests.
TSF-153	**TSF 201 NTP restart** The TSF 201 would restart when setting the NTP server IP address during initial configuration.
TSF-96	A traffic stop situation is fixed.
TSF-98 / TSF-101	A restart situation when handling fragmented IP packets is fixed.
TSF-103	**TSF 201 restarted when a multicast group was deleted** When a multicast group was deleted in the GUI, the TSF 201 restarted with error code 73 "Restart caused by software error", and the multicast group was not removed. To remove the multicast group, the TSF 201 had to be erased and reconfigured.

Hardware related changes

Change id	**Change description**
TSF-86	**New function: Confiqurable Diode Mode Low to Hiqh** For description see table above
TSF-91	A logical error is found and fixed in the interpretation of the filter language.

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 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 in the IAR[5] chapter 4.

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].

There are a number of changes between the Certified and maintained TOE versions. 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] are 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
Date approved	29 November 2018