ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Senetas Distributed by Thales CN Series Encryptors 5.5.1

Maintenance Update of Senetas Distributed by Thales CN Series Encryptors 5.5.1

Maintenance Report Number: CCEVS-VR-VID11486-2025

Date of Activity: 28 July 2025

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Senetas Distributed by Thales CN Series Encryptors 5.5.1 Security Target, Version 1.0, June 2025
- Senetas Distributed by Thales CN Series Encryptors 5.5.1 Impact Analysis Report, Version 1.0, June 2025

Evaluated TOE

- **VR Title** – Common Criteria Evaluation and Validation Scheme Validation Report Senetas Distributed by Thales CN Series Encryptors 5.5.0
- **VR Report #: CCEVS-VR-VID11485-2024**
- **VR Version** – 1.0
- **VR Date** –December 31, 2024

Current AM TOE Updated

- **ACMR Title** – Common Criteria Evaluation and Validation Scheme Validation Report Senetas Distributed by Thales CN Series Encryptors 5.5.1
- **ACMR Report #: CCEVS-VR-VID11485-2025**
- **ACMR Version** – 1.0
- **ACMR Date** – July 28, 2025

Documentation Updated:

CC Evidence	Evidence Change Summary
Senetas Distributed by Thales CN Series Encryptors 5.5.0 Security Target, Version 1.7, December 2024	Senetas Distributed by Thales CN Series Encryptors 5.5.1 Security Target, Version 1.0, June 2025 Updates include Title page, ST Reference, TOE Reference, TOE embedded software version and build number, Common Criteria guidance documents reference
Guidance Documentation: CN4000/CN6000/CN9000 Series Ethernet Encryptors, Firmware Version 5.5.1 Operational User Guidance (AGD_OPE.1), Version 1.0, June 2025	CN4000/CN6000/CN9000 Series Ethernet Encryptors, Firmware Version 5.5.1 Operational User Guidance (AGD_OPE.1), Version 1.0, July 2025. Updates include Title page, ST Reference, TOE Reference, TOE embedded software version and build number.
Senetas Distributed by Thales CN Series Encryptors 5.5.0 Vulnerability Assessment, Version 1.1, December 2024	Senetas Distributed by Thales CN Series Encryptors 5.5.0 Vulnerability Assessment, Version 1.1, July 2025. Updated AVA search date to July 17, 2025.

Assurance Continuity Maintenance Report:

Senetas Corporation Ltd, Distributed by Thales SA (SafeNet) submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 26 June 2025. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, Administrative Guidance, AVA and the IAR. The ST, Administrative Guidance and AVA documents were updated.

Product Updates

All changes to the product, shown in the following table, were feature enhancements and have been assessed as minor. These enhancements do not affect the security functionality or claims of the previously evaluated TOE.

Feature	Description	Affected Platform	Impact Analysis
CN6110 link settings Note: this model was included in the original evalustion.	Minor updates to improve customer experience for new product (CN6110) introduction. Including: -Added help text for linkspeed -s option	CN6110	Minor — Not SFR related. These changes only affect user interface help text and proper link speed configuration. No modifications to encryption algorithms or security-critical components. Changes improve usability without altering security posture.

	-Modified code to preserve MAX_LINK when protocol changes.		
CSDK Image Loading Prevention	Removed pre-release feature from the upgrade path by adding an error message when unsupported CSDK files are detected.	All platforms	Minor – No impact on SFR claims. Adds an early exit with error message when such files are detected. No changes to core security functionality.
Linux Log Rotation Management	-Changed logrotate invocation fixing file permissions and non-rotating logs -Removed 15MB log size override, reducing to system default of 3MB -Added new hourly timer for logrotate -Fixed log rotate file permissions for CN6140 slot operation	All platforms	Minor – No impact on SFR claims. Improves system stability and maintenance efficiency. Optimizes storage utilization with smaller log files. No impact on core function

TOE Environment

There are no updates to operational environment components identified. The TOE environment is consistent with the validated results from the previous evaluation.

Regression Testing

Senetas has performed regression testing on the CN Series Encryptors running the embedded software v5.5.1. Lightship Security has reviewed the test evidence and confirms that the TOE operates as expected and maintains the same results as the tests conducted during the previous evaluation of v5.5.0.

NIST Certificates:

The updates made to the TOE have not changed the cryptographic modules algorithm implementation nor their tested operational environment, so there is no impact to the CAVP certificates.

Vulnerability Assessment:

An updated vulnerability analysis was performed on June 24, 2025 and again on July 17, 2025 using the original search terms. These results are included in the separate document 'Senetas Distributed by Thales CN Series Encryptors 5.5.1 Vulnerability Assessment, Version 1.1, July 2025. There are no residual vulnerabilities in the new version of the product.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the product changes and vulnerability updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.