Certification Report

Marvell LS2 HSM

Hardware version: **CN9310410-03 C**
Firmware version: **MARVELL-LS2-FW-10.24-0780**
Bootloader version: **MARVELL-LS2-UBOOT-10.24-0702-R01-SB or MARVELL-LS2-UBOOT-10.24-0702-R02-SB**

Sponsor and developer:	***Marvell Semiconductor, Inc*** **5488 Marvell Lane** **Santa Clara, CA 95054** **U.S.A.**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400151-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400151-01**
Author(s):	**Haico Haak**
Date:	**23 February 2026**
Number of pages:	**15**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Marvell LS2 HSM. The developer of the Marvell LS2 HSM is Marvell Semiconductor, Inc located in Santa Clara, U.S.A. and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Hardware Security Module (HSM) in the form of a PCI-e card, composed by hardware, firmware and software. The TOE is suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services (including support of authentication of client applications or authorized users of secret keys, and support of authentication for electronic identification), as identified by the (EU) No 910/2014 regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS). The TOE may also support protected backup of keys.

The TOE provides the following major security features:

- Cryptographic functions including symmetric and asymmetric algorithms approved by [SOG IS-Crypto] and for use in TSP environments for encryption, decryption, digital signature, verification and hash generation.
- Key management intended as key generation, key import and export and key derivation.
- Backup of the critical user data.
- Audit of the security relevant events of the TOE, to be stored within the TOE and securely exported to a third-party application located on the host.
- Self-protection, which includes self-tests and physical protection.
- Secure communication channels for remote management operations.
- Information and functionality isolation provided by HSM partitions.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 23 February 2026 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Marvell LS2 HSM, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Marvell LS2 HSM are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_FLR.3 (Systematic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

The TOE is stated as a Qualified Signature Creation Device and Qualified Seal Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight BV included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Marvell LS2 HSM from Marvell Semiconductor, Inc located in Santa Clara, U.S.A..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	LS2-B0	CN9310410-03 C
Software	Firmware	MARVELL-LS2-FW 10.24-0780
	Bootloader	One of the following two versions: MARVELL-LS2-UBOOT-10.24-0702-R01-SB **OR** MARVELL-LS2-UBOOT-10.24-0702-R02-SB

To ensure secure usage a set of guidance documents is provided, together with the Marvell LS2 HSM. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The security functionalities of the TOE are:

Cryptographic functions

The TOE includes cryptographic algorithms to provide the following cryptographic functions:

- Digital signature generation and verification
- Message digest generation
- Message authentication code generation and verification
- Encryption and decryption (symmetric and asymmetric)
- Key generation (symmetric and asymmetric)
- Key agreement and distribution
- Key derivation
- Generation of shared secret values
- Cryptographic support (ability of TOE to be used for doing any operation required as part of an OTP mechanism or PKI infrastructure, and Non-PKI is usually credential mechanisms) for one time password and other non-PKI based authentication mechanisms
- Random number generation.

Key management

The TOE supports the secure management of cryptographic keys for those implemented cryptographic functions which requires them, including:

- Key establishment (including key generation)
- Protection of keys held within the TOE and held externally (for use by the TOE);
- Control of access and use of keys by the cryptographic functions within the TOE
- Deletion of keys within the TOE.

The TOE supports the following techniques for establishing keys:

- Generation of cryptographic keys using a random number generator and implementing the key generation algorithms depending on the intended use of the keys.
- Import of cryptographic keys in encrypted form.
- Key agreement protocols establishing common secrets with external entities.
- Derivation of keys from shared knowledge.

Backup

The TOE supports backup and restoration of the TSF state necessary to re-establish an operational state after failure to specially preserve the security requirements on keys.

Audit

The TOE also logs audit records for its own actions, which can be collected, maintained, and reviewed in a larger system from which the TOE is part.

Self-protection

The module is designed with self-protection capabilities that ensure that it remains in a secure state when facing abnormal conditions.

Secure channels

Remote operation of the TOE is only allowed for TOE Partitions. The end-to-end encryption feature in the module allows an application to initiate a TLSv1.2 connection with the firmware to ensure the confidentiality of the data communicated to the HSM.

Authentication & authorization

The module enforces identity-based authentication.

Partitions

Cryptographic keys are stored and managed inside containers called partitions.

The TOE provides isolated internal paths between the host and the addressed partition to manage each partition request.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that EN 419221-5 Protection Profile [EN419221-5] claims the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance in which it is contained (“OE.Env Protected operating environment”).

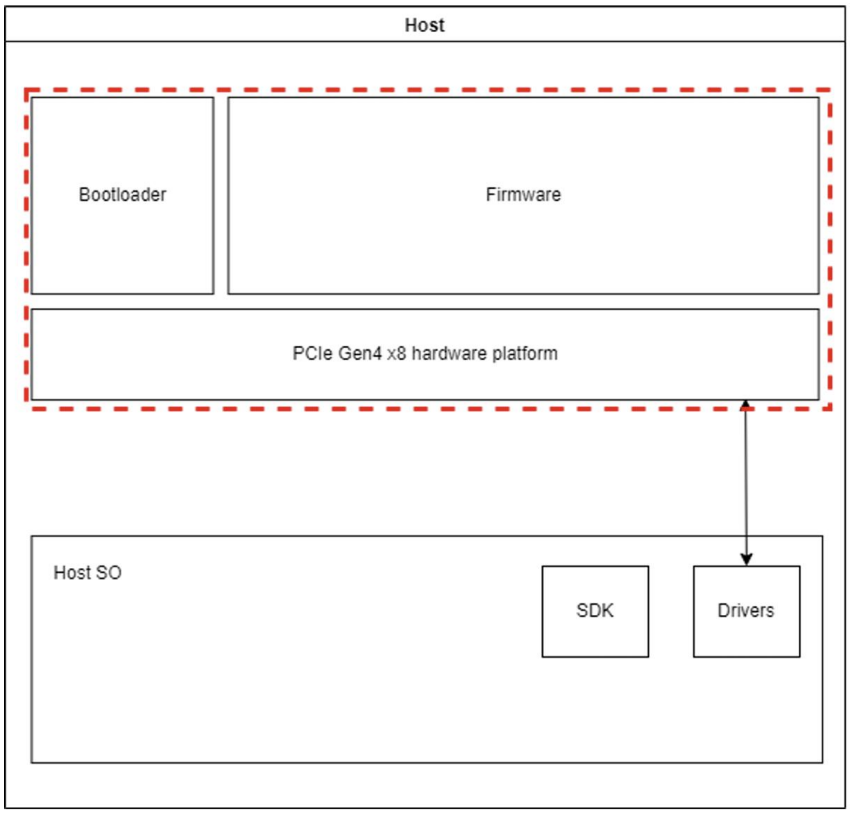
The ST follows the PP and also claims OE.Env, thus the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

2.4 Architectural Information

The TOE is LS2 Hardware Security Module (hereafter referred to as TOE) by Marvell is a high-performance purpose-built security solution for key management and crypto acceleration. The module is deployed in a PCIe slot to provide crypto and protocol acceleration in a secure manner to the system host. It is typically deployed in a server or an appliance to provide crypto offload for the keys stored on the HSM. The module's functions are accessed over the PCIe interface via an API defined by the module.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



The TOE has the following features:

- Cryptographic functions
- Key management
- Backup
- Audit
- Self-protection
- Secure channels
- Authentication & authorization
- Partitions

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Marvell LS2 HSM Hardware Installation Guide	Rev.3
Marvell LS2 HSM Adapter SDK User Guide	Release 10.24-0780 Rev.1.1
Marvell LiquidSecurity 2 SDK API Guide	10.24-0780
Marvell LS2 HSM User Guidance	Version 1.6
Marvell LS2 HSM Preparative Procedures	Version 6.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification and module-to-module level. The testing was largely automated using proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

In addition, fuzz tests are performed. For Fuzz tests, an implementation is applied which traverses all possible paths with a varied set of inputs.

The framework supports three key testing approaches:

- API Testing - Direct interface validation
- Client-Server Model - Distributed testing scenarios
- Driver Model - Functional testing using specific tools

Each test suite includes test plans that detail for each test: Operations TSFI (opcode) Module, subsystems & SFRs Test name and ID Objective Precondition Test Step Description Test Step Expected Result Actual Result Pass/Fail Status.

For the testing performed by the evaluators, the developer made available samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The AVA_VAN.5 assurance class requires the evaluator to conduct a methodical vulnerability analysis based on publicly available source of information and based on structured examination of the evidence while performing previous evaluation activities (ASE, ADV, AGD, ATE). Given the restrictions imposed by the PP (which prevents any physical attack and any side channel attack that requires physical proximity to the TOE), the evaluator focused on vulnerabilities related to design/architectural flaws that would lead intended users to abuse the TOE. For this reason, the evaluator needed to find a methodical approach to scout the TOE implementation searching for such design/architectural flaws.

Step 1: The first step of this type of vulnerability analysis is the identification of areas of concern (as defined in [CEM]).

Step 2: Iteratively, for each SFR, the evaluator formulates security relevant questions for each identified area of concern.

Step 3: the evaluator argues whether a possible vulnerability is removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. If yes, the possible vulnerability is

considered as solved, otherwise it is uniquely labelled as potential vulnerability POT_VUL.xxx.yyy. Potential vulnerabilities are then addressed in the context of penetration tests and further code review.

Most of the possible vulnerabilities were discarded as a result of the evaluator's detailed analysis of the evidence provided by the developer. However, there are several potential vulnerabilities that require further assessment, and where applicable, penetration tests were devised.

The total test effort expended by the evaluators was 8 weeks. During that test campaign, 1% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 0% perturbation attacks, 0% retrieving keys with FA, 0% side-channel attacks, 99% exploitation of test features (logical tests), 0% attacks on RNG, 0% ill-formed Java Card application, 0% software attacks, and 0% application isolation penetration tests.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- Hardware: CN9310410-03 C
- Firmware: MARVELL-LS2-FW-10.24-0780
- Bootloader: MARVELL-LS2-UBOOT-10.24-0702-R00-SB-ES

The bootloader provided is signed by an internal key and it is identical source code used in R01 and R02 bootloader versions. Therefore, all testing results are applicable.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Marvell LS2 HSM, Hardware version: CN9310410-03 C, Firmware version: MARVELL-LS2-FW-10.24-0780. Bootloader version: MARVELL-LS2-UBOOT-10.24-0702-R01-SB **or** MARVELL-LS2-UBOOT-10.24-0702-R02-SB.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the sites in Penang, Malaysia *[STAR-MA], Santa Clara, USA [STAR-SC], Hyderabad, India [STAR-IN] and Reno,*

USA [STAR-DC5] [2]. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Marvell LS2 HSM, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5 and ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[*EN419221-5*]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The Marvell LS2 HSM Security Target, Version 1.18, 20 February 2026 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

API	Application Programming Interface
APT	Adaptative Proportion Test
AU	Appliance user
CCA	CPU Core Access Control
CSP	Critical Security Parameter, Crypto Service Provider, Certification Service Provider
DTBS/R	Data To Be Signed or its unique representation
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PAC	Partition Certificate
PAK	Partition Private Key
PCIe	Peripheral Component Interconnect Express
PCO	Partition Crypto Officer
PCU	Partition Crypto User
POTAC	Partition Owner Trust Anchor Certificate
PP	Protection Profile
SCD	Signature Creation Data
SR-IOV	Single-root input/output virtualization
SVD	Signature Verification Data
TOE	Target of Evaluation
UART	Universal Asynchronous Receiver-Transmitter
UCD	Universal Controller Device
VAD	Verification Authentication Data
VF	Virtual Function

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1
[eIDAS-REP[	Assessment Reporting Sheet eIDAS – Marvell LS2 HSM, Hardware version: CN9310410-03 C, Firmware version: MARVELL-LS2-FW-10.24-0780. Bootloader version: MARVELL-LS2-UBOOT-10.24-0702-R01-SB or MARVELL-LS2-UBOOT10.24-0702-R02-SB, Version 3.0, 20 February 2026
[EN419221-5]	EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020
[ETR]	Evaluation Technical Report “Marvell LS2 HSM, Hardware version: CN9310410-03 C, Firmware version: MARVELL-LS2-FW-10.24-0780. Bootloader version: MARVELL-LS2-UBOOT-10.24-0702-R01-SB or MARVELL-LS2-UBOOT 10.24-0702-R02-SB” – EAL4+, Version 5.0, 20 February 2026
[ETRfC]	Evaluation Technical Report for Composition “Marvell LS2 HSM, Hardware version: CN9310410-03 C, Firmware version: MARVELL-LS2-FW-10.24-0780. Bootloader version: MARVELL-LS2-UBOOT-10.24-0702-R01-SB or MARVELL-LS2UBOOT-10.24-0702-R02-SB” – EAL4+, Version 3.0, 20 February 2026
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, and REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation(EU) No 910/2014 as regards establishing the European Digital Identity Framework
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.1, November 2023
[JIL-AMHD]	Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution
[JIL_QSCD]	Security Evaluation and Certification of Qualified, Electronic Signature/Seal Creation Devices, JIL Interpretations for Security Certification according to eIDAS Regulation 910/2014, Version 1.0, July 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Marvell LS2 HSM Security Target, Version 1.18, 20 February 2026
[STAR-MA]	Site Technical Audit Report – Venture Electronics site for Marvell (Penang – Malaysia), 25-RPT-1570 , Version 3.0, 20 February 2026

[STAR-SC]	Site Technical Audit Report – Marvell LS2 HSM – Santa Clara (USA) 25-RPT-1594 , Version 3.0, 20 February 2026
[STAR-IN]	Site Technical Audit Report – Marvell LS2 HSM – Hyderabad (IN), 25-RPT-1595, Version 3.0, 20 February 2026
[STAR-DC5]	Site Technical Audit Report – Switch Data Center for Marvell (Reno-USA), 25-RPT-1569, Version 3.0, 20 February 2026

(This is the end of this report.)