National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Galleon Embedded Computing XSR and G1 Hardware Encryption Layer

Report Number: CCEVS-VR-VID11655-2026
Dated: May 21, 2026
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Jaemond Reyes
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Galleon Embedded Computing XSR and G1 Hardware Encryption Layer solution provided by Galleon Embedded Computing AS. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in May 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the:

- *PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine*, Version: 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0) which includes the following components:
    - Base-PP: *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_AA_V2.0E) and
    - Base-PP: *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_EE_V2.0E).

The TOE is the Galleon Embedded Computing XSR and G1 Hardware Encryption Layer.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target*, Version 2.3, May 15, 2026 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Galleon Embedded Computing XSR and G1 Hardware Encryption Layer (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine*, Version: 1.0 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0) which includes the following components: • Base-PP: *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_AA_V2.0E) and • Base-PP: *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_EE_V2.0E).
ST	*Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target*, Version 2.3, May 15, 2026
Evaluation Technical Report	*Evaluation Technical Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5

Item	Identifier
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Galleon Embedded Computing AS
Developer	Galleon Embedded Computing AS
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Jaemond Reyes, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is the Galleon Embedded Computing Encryption Module (EM) running firmware version 4.1.0. The Encryption Module as integrated into Galleon's XSR and G1 products provides their Hardware Encryption Layer, encrypting both internal, non-removable drives as well as a removable drive.

Galleon's HW-layer FDE was evaluated against the FDE collaborative protection profiles, which pertain to data at rest encryption. Network security is outside the scope of an FDE evaluation, and thus only local administration was evaluated.

3.1 TOE Description

The TOE comprises a dedicated hardware solution embedded into Galleon's XSR and G1 products. The TOE (known as the Hardware Encryption Layer or as the Encryption Module) takes the form of either a physically separate card (within the XSR) or directly integrated into the mainboard (of the G1).

The Encryption Module sits between the XSR and G1's mSATA connectors and the mSATA drives themselves (which includes an RDM, internal SSDs, and the non-removable mSATA[only present in the XSR]), providing transparent hardware-based Full Disk Encryption (FDE) of those drives.

The XSR and G1 products into which the TOE integrates can act in multiple different capacities (Network Attached Storage [NAS], data recorder, general server, etc.) and allow for encryption of the Removable Data Module (RDM) attached to the system. The Encryption Module within the XSR model supports encryption of one RDM (at a time), up to 4 internal SSDs, and its internal, non-removable mSATA SSD. Within the G1 model, the Encryption Module supports encryption of one RDM (at a time) and up to 2 internal SSDs. The Encryption Module securely encrypts all user data stored within.

In addition to the hardware-based FDE layer, the XSR and G1 products also possess a software-based Full Drive Encryption (FDE) layer; however, this software-based FDE layer is addressed in a separate evaluation.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The TOE provides a hardware Full Drive Encryption solution that can accept Removable Data Modules (RDMs) which contain data drives within.

3.4 Physical Boundaries

The TOE's physical boundary is the physical perimeter of its enclosure. The TOE provides a ruggedized solution to secure Data at Rest (DAR).

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Security management
4. Protection of the TSF

4.1 Cryptographic support

The TOE includes cryptographic functionality for key management, user authentication, and block-based encryption including: symmetric key generation, encryption/decryption, cryptographic hashing, keyed-hash message authentication, and password-based key derivation. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key destruction. These primitive cryptographic functions are used to encrypt Data-At-Rest (including the generation and protection of keys and key encryption keys) used by the TOE.

4.2 User data protection

The TOE performs Full Drive Encryption on the entirety of each drive (so that no plaintext exists) and does so without user intervention.

4.3 Security management

The TOE provides each of the required management services necessary to manage the full drive encryption using a command line interface.

4.4 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features. It protects key and key material, and includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fail, the TOE will not go into an operational mode.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, 01 February 2019
- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, 01 February 2019

That information has not been reproduced here. CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Full Drive Encryption models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Encryption Module Usage Guidelines*, Version 1.0.9, May 15, 2026

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026 (DTR), as summarized in the evaluation *Assurance Activity Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the CPP_FDE_AA_V20E/CPP_FDE_EE_V20E including the tests associated with optional requirements. The AAR in sections 1.1 and 3.4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The Target of Evaluation (TOE) is the Galleon Embedded Computing Encryption Module (EM) running firmware version 4.1.0. The Encryption Module as integrated into Galleon's XSR and G1 products provides their Hardware Encryption Layer, encrypting both internal, non-removable drives as well as a removable drive.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR).. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Galleon Embedded Computing XSR and G1 Hardware Encryption Layer TOE to be Part 2 extended, and to meet the SARs contained in the CPP_FDE_AA_V20E/CPP_FDE_EE_V20E.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Galleon Embedded Computing XSR and G1 Hardware Encryption Layer products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E related to the examination of the information contained in the TOE Summary Specification (TSS).

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the FDEAA20E/FDEEE20E and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the DTR prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities was conducted on May 12, 2026 and did not uncover any residual vulnerability.

The Evaluation team searched the following databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- MITRE CVE Database ((https://www.cve.org/)
- CVE details https://www.cvedetails.com/vulnerability-search.php),
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)

The evaluator performed the search using the following search terms: "Disk encryption", "Drive encryption", "Key destruction", "Key sanitization", "Password caching", "Key caching", "Galleon", "G1", "XSR", "ARMv7 Processor rev1", "Opal management software", "SED

management software", "SNMP", "SATA", "Microchip ATSAMA5D27C-LD2G", "Enova X-Wall", "Microchip AD220032D", "openssl 3.4.1", "Marvell 88SE9170", and "cryptsetup 2.7.5".

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E and their Supporting Documents, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the configuration instructions in the Guidance document defined in Section 6. No other versions of the TOE software, either earlier or later, were evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST and only that functionality was evaluated. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Validation team strongly recommends that all TOE hardware in the operational environment is kept up to date with patches as they are released. In addition, Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration

11 **Annexes**

Not applicable

12 **Security Target**

The Security Target is identified as: *Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target*, Version 2.3, May 15, 2026.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, 01 February 2019.

[5] *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, 01 February 2019.

[6] *Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target*, Version 2.3, May 15, 2026 (ST). [includes public and proprietary versions]

[7] *Assurance Activity Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026 (AAR).

[8] *Detailed Test Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026 (DTR).

[9] *Evaluation Technical Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer*, Version 0.2, May 15, 2026 (ETR).

[10] *Encryption Module Usage Guidelines*, Version 1.0.9, May 15, 2026 (AGD).