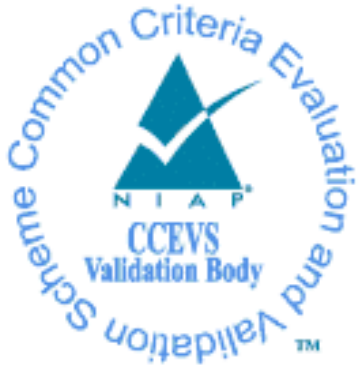
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
Galleon Embedded Computing AS
Embedded Computing XSR and G1 Software Encryption Layer

Report Number: CCEVS-VR-11273-2022
Dated: July 28, 2022
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
Lisa Mitchell
Clare Parran
Chris Thorpe

Common Criteria Testing Laboratory

Kevin Cummins
Douglas Kalmus
Allison Keenan
John Messiha
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) evaluation of Galleon Embedded Computing XSR and G1 Software 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 July 2022. 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 collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 and the collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019.

The TOE is the Galleon Embedded Computing XSR and G1 Software Encryption Layer. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 (CCEVS) 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Galleon Embedded Computing XSR and G1 Software Encryption Layer Security Target, version 1.5, July 14, 2022 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Galleon Embedded Computing XSR and G1 Software Encryption Layer (Specific models identified in Section 4.1)
Protection Profile	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 and collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019
ST	Galleon Embedded Computing XSR and G1 Software Encryption Layer Security Target, version 1.5, July 14, 2022
Evaluation Technical Report	Evaluation Technical Report for Galleon Embedded Computing XSR and G1 Software Encryption Layer, Version 0.4, July 14, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
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

Item	Identifier
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Clare Parran, Chris Thorpe

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

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 and the CPP_FDE_AA_V2.0E/CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the CPP_FDE_AA_V2.0E/CPP_FDE_EE_V2.0E and applicable Technical Decisions 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 the Full Drive Encryption Protection Profiles 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.

4 Architectural Information

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

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

The TOE provides software Full Drive Encryption of removable drives and can be installed on Galleon's XSR or G1 models. All models use Intel 64-bit CPUs, and Galleon offers the G1 with a single CPU model while offering the XSR with a range of CPUs to allow customers to tailor the system to their needs.

The XSR and G1 (hereafter referred to as the Products) 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 XSR model supports encryption of one RDM (at a time), up to 4 internal SSDs, and its internal, non-removable mSATA SSD. The G1 model also supports encryption of one RDM (at a time) and up to 2 internal SSDs. Both securely encrypt all user data stored within either model.

The Products run the Red Hat Enterprise Linux (RHEL) Release 8.4 operating system. The Products provide a software-based Full Disk Encryption (FDE) of the removable drive within each RDM. In addition to the software-based FDE layer, the TOE also provides a hardware-based Full Drive Encryption (FDE) layer to encrypt the drive within each RDM. The hardware-based FDE layer is addressed in a separate evaluation.

The TOE, whether operating as a NAS or a more general server, supports encrypting the data of additional software running on the TOE's operating system. The TOE might include software to support protocols including CIFS and NFS or might include the vendor's data recording software or even include customer provided software applications. The RHEL administrator can enable, disable, or install additional (accessing the system directly) desired protocols and software applications to support their use-case and application.

4.1 TOE Evaluated Platforms

The following table summarizes the CPU options available (bold denotes the models used during evaluation testing, while italics denotes equivalent models).

Model	Processor
XSR	**Intel Xeon E3-1505Lv6 (Kaby Lake)**
XSR	*Intel Xeon E3-1505Mv6 (Kaby Lake)*
XSR	*Intel Xeon E-2276ME (Coffee Lake)*
XSR	*Intel Xeon E-2276ML (Coffee Lake)*
G1	**Intel Atom C2758 (Rangeley)**

4.2 TOE Architecture

The TOE provides a software Full Drive Encryption solution that can encrypt a Removable Data Module (RDM) which contain a data drive within as well as additional internal SSDs.

4.3 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).

5 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

5.1 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.

5.2 User data protection

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

5.3 Security management

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

5.4 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.

6 Documentation

The following documents were available with the TOE for evaluation:

- SW Encryption Layer Certifiable Encryption, Version 1.0.7, July 14, 2022

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 Software Encryption Layer, Version 0.4, July 14, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (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_V2.0E/CPP_FDE_EE_V2.0E including the tests associated with optional requirements. The DTR, in Section 2, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary 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 Embedded Computing XSR and G1 Software Encryption Layer TOE to be Part 2 extended, and to meet the SARs contained in the CPP_FDE_AA_V2.0E/CPP_FDE_EE_V2.0E.

8.1 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 Software 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.

8.2 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 ST and Guidance document. Additionally, the evaluator performed the assurance activities specified in the CPP_FDE_AA_V2.0E/ CPP_FDE_EE_V2.0E related to the examination of the information contained in the 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.

8.3 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.

8.4 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 identified.

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.

8.5 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 CPP_FDE_AA_V2.0E/ CPP_FDE_EE_V2.0E and recorded the results in the DTR, 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.

8.6 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 did not uncover any residual vulnerability.

The evaluation team searched the following databases:

- National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)

The search was performed on 7/12/2022. The search was conducted with the following search terms: "disk encryption", "drive encryption", "key destruction", "key sanitization", "Password caching", "Key caching", "Galleon", "G1", "XSR", "Intel Atom CPU C2758", "Intel Xeon CPU E3-1505L v6", "Opal management software", "SED management software", "LUKS", "Linux Unified Key Setup", "kernel cryptography", "openssl", "libcrypt", "RHEL 8.4", "Intel Xeon E3-1505Mv6", "Intel Xeon E-2276ME", "Intel Xeon E-2276ML".

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.

8.7 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 correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the SW Encryption Layer Certfiable Encryption, 1.0.7, July 14, 2022. No other versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, would need to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable

11 Security Target

The ST is identified as: *Galleon Embedded Computing XSR and G1 Software Encryption Layer Security Target, Version 1.5, July 14, 2022.*

12 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 2: Glossary

13 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 Software Encryption Layer Security Target, Version 1.5, July 14, 2022 (ST).

[7] Assurance Activity Report for Galleon Embedded Computing XSR and G1 Software Encryption Layer, Version 0.4, July 14, 2022 (AAR).

[8] Detailed Test Report for Galleon Embedded Computing XSR and G1 Software Encryption Layer, Version 0.4, July 14, 2022 (DTR).

[9] Evaluation Technical Report for Galleon Embedded Computing XSR and G1 Software Encryption Layer, Version 0.4, July 14, 2022 (ETR)

[10] SW Encryption Layer Certfiable Encryption, 1.0.7, July 14, 2022 (AGD)