National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cyber Reliant Mobile Data Defender for Android SDK Version 4.0

Report Number: CCEVS-VR-VID11283-2023
Dated: March 21, 2023
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

Paul Bicknell
Sheldon Durrant
Linda Morrison
Clare Parran
Lori Sarem
Ben Schmidt
The MITRE Corporation

Common Criteria Testing Laboratory

Raymond Smoley
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) Validation team of the evaluation of Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 solution provided by Cyber Reliant Corp. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 March 2023. 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 Extended, and meets the assurance requirements of the PP-Configuration for Application Software and File Encryption, Version 1.1, 7 April 2022 [base PP: Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10)].

The Target of Evaluation (TOE) is the Cyber Reliant Mobile Data Defender for Android SDK Version 4.0. TOE identified in this Validation Report 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 Validation Report 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 Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 Security Target, version 0.6, March 16, 2023 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:

- 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	Cyber Reliant Mobile Data Defender for Android SDK Version 4.0
Protection Profile	PP-Configuration for Application Software and File Encryption, Version 1.1, 7 April 2022 [base PP: Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10)]
ST	Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 Security Target, version 0.6, March 16, 2023
Evaluation Technical Report	Evaluation Technical Report for Cyber Reliant Mobile Data Defender for Android SDK Version 4.0, version 0.3, March 16, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor	Cyber Reliant Corp
Developer	Cyber Reliant Corp
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Paul Bicknell, Sheldon Durrant, Linda Morrison, Clare Parran, Lori Sarem, Ben Schmidt

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

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

- Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14)
- PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10)]

That information has not been reproduced here and the ASPP14/FE10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/FE10 as described for this TOE in the Security Target. 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.

Clarification of scope

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 Application Software Protection Profile with File Encryption 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 File Encryption Application 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 the ASPP14/FE10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

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

The Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 provides file level encryption through an Android Package Kit (APK) and a library implementation. The library contains both Java and native (C/C++) interfaces in order to support the majority of Android application storage requirements. The same implementation and functionality for both java and C/C++ are provided by the TOE. The library offers two groups of Application Programming Interface (API): one set to manipulate files and one set to manipulate SQLite databases. These libraries are:

AuthenticationLib	Used by the library to talk to the Management service for key management.
CRCsqlite3	Our new SQLite library that is completely file based and calls the FileEncryptionLib-arm library directly
FileEncryptionLib-arm	This is the actual File encryption library which is called for file I/O by the application. It manages all interface with the application.
DataEncryptionLib-arm	This is our library that does the actual data encryption and splitting. It is our core library.

While the API groups provide different abstractions for the read and write operations, they are ultimately simply reading and writing a single file. The library is providing file level encryption.

The Management Service application is a straight Java Data Protection SDK APK, while the Library is intended to be included into a mobile application (and then the mobile application can use the API libraries). The Management Service Application runs in the background and uses WolfCrypt keystores to provide the File Encryption Key Encryption Key (FEKEK) to each of the applications. The Data Protection SDK uses the Android keystore to generate and store an RSA key pair used by the Management Service. On a per application basis the Android keystore is leveraged to store each application's RSA keypair to double wrap the AES-wrapped FEKEK. The single and double wrapped FEKEKs are then stored in WolfCrypt secure keystores. The Management Service application handles necessary authentication and key management. The file level encryption suite is an API designed to support the use of specialized file level encryption for Android applications. Encryption is provided by the Cyber Reliant Mobile Data Defender for Android SDK with WolfCrypt.

The TOE is the Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 software application package residing on evaluated mobile devices running Android 11. The TOE is a software solution providing the capability to handle file encryption on mobile devices.

4.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.

4.2 TOE Architecture

The TOE is software installed on an evaluated mobile device running Android 11. The TOE software is installed as a Management Service as well as the security functionality (TSF) interface library that is compiled into other applications. References to applications noted in this Security Target are regarded as applications that are compiled with the TSF interface API library. The Management Service is responsible for handling the File Encryption Key Encryption Keys (FEKEKs) necessary to unwrap the FEK. The Management Service obtains the Cyber Reliant Mobile Data Defender for Android SDK password (hereafter referred to as the DaR password) from the user and double wraps the FEKEK by using RSA-2048 first and then wrapping it again using AES-256. Note that the Management Service itself is not responsible for encryption.

The TOE's interface library is compiled into another application's package which allows the other application to invoke the TOE's services (i.e. allows the application to call the TOE's file encryption services once the application is registered with the Management Service). Applications registered to the TOE have a unique RSA public/private keypair to enable the applications to pass their RSA public keys to the Management Service along with an Cyber Reliant Mobile Data Defender for Android SDK's certificate fingerprint; the application uses this as the password to the application's key store. Android's keystore protects keys by storing them in a container with limited access to the keys through Android's keystore API. The TOE allows only a single user at a time.

The TOE stores the double wrapped FEKEKs in the Management Service's WolfCrypt keystore and the single wrapped FEKEKs in the application's specific WolfCrypt keystore. The keys are protected by requiring a password to load both the Management Service and application's keystore. In order for other applications to access its FEK, the application must use the TOE's interface library API to request Management Service functions. The Management Service uses the application's public key to wrap the FEKEK (via RSA-OAEP) so that it can be passed to the application by placing the single wrapped FEKEK into the application's WolfCrypt keystore. The wrapped FEKEKs in each application's WolfCrypt keystore are ephemeral to enable a safeguard as a configurable threshold for consecutive incorrect password attempts. When the password attempt threshold is met, the Cyber Reliant system automatically initiates an authentication timeout.

The TOE uses the WolfCrypt and WolfSSL modules in conjunction with our CRC Encryption and Shredding engine for cryptographic services.

4.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Samsung S20, Samsung Tab Active 3, Panasonic ToughBook FZN1, or equivalent device as identified in section 1.3 of the ST) on which the TOE resides.

5 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

5.1 Cryptographic support

The evaluated platform runs on Android 11 operating system. Android APIs allow generation of keys through Key Generator, and random numbers are generated using Java SecureRandom (256 bits). Keys are used to protect data belonging to the applications that use the TOE.

The TOE uses the Cyber Reliant Mobile Data Defender for Android SDK with the WolfCrypt Module for cryptographic algorithms. The module supports encryption via AES and random number generation via an SP 800-90 AES-256 DRBG. The TOE also performs AES key wrapping and keyed hashing via HMAC.

5.2 User data protection

The TOE protects user data by providing encryption services for applications to encrypt their data. The TOE allows encryption of data using AES-256 bit keys.

5.3 Identification and authentication

The TOE authenticates applications by requiring a PIN/passphrase to unlock the application's file encryption key. A wrong password results in the unsuccessful loading of the application's WolfCrypt keystore. Without the correct keystore, the application cannot load the keys necessary for file encryption/decryption.

5.4 Security management

The TOE's services/options are inaccessible until a configuration has been created. The TOE does not allow invocation of its services without configuration of the TOE's settings upon first start up. The TOE allows password changes for management purposes.

5.5 Privacy

The TOE does not transmit Personally Identifiable Information (PII) over any network.

5.6 Protection of the TSF

The TOE uses the physical boundary of the evaluated platform as well as the Android operating system for the protection of the TOE's application components.

The TOE checks for updates by selecting the check current version option on its menu. If an update is needed, Cyber Reliant shall deliver, via email or other agreed upon method, an updated application. The TOE's software is digitally signed by Cyber Reliant. Each update is accompanied by documentation outlining changes to the overall service, as well as compatible versions of the Cyber Reliant API.

5.7 Trusted path/channels

The TOE does not transmit any data between itself and another product. All TOE-managed data resides on the evaluated platform.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cyber Reliant Defender Installation and Use, March 2023

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 Evaluated Configuration

The evaluated configuration consists of the Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 software application package residing on evaluated mobile devices running Android 11. The TOE is a software solution providing the capability to handle file encryption on mobile devices. The TOE is capable of running on Android 11 devices under VID11160, VID11211, or VID11315 with the same application supporting any of the devices. The TOE was tested on the following mobile devices representing one device from each VID.

Device Name	Chipset/CPU	Architecture	Android Version
Samsung S20 (VID11160)	Snapdragon 865	A64	11
Samsung Tab Active 3 (VID11211)	Exynos 9810	A64	11
Panasonic ToughBook FZN1 (VID11315)	Snapdragon 660 (SDM660)	A64	11

The same application runs on all Android devices. Since the TOE is the same for the remaining devices under these evaluations and their behavior was evaluated to be equivalent from a security function standpoint, all other devices from these evaluations are claimed as equivalent.

VID11160

- Samsung S21 (S21 5G / S21+ 5G / S21 Ultra 5G)
- Samsung S21 (S21 5G / S21+ 5G / S21 Ultra 5G / S21 5G FE / Z Fold3 5G / Z Flip3 5G)
- Samsung S20 (S20 5G / S20+ 5G / S20 Ultra 5G / S20 LTE 5G / S20 5G FE / Note20 5G / Note20 LTE / Note20 Ultra LTE / Note20 Ultra 5G)
- Samsung S20 (S20+ 5G / S20 FE / S20 Ultra 5G / Z Flip 5G / Tab S7 / Tab S7+ / Note20 5G / Note20 Ultra 5G / Z Fold2 5G)
- Samsung XCover Pro / Samsung A51
- Samsung Note10 (Note10+ 5G / Note10+ / Note 10 5G / Note 10)
- Samsung S10e (S10+ / S10 5G / S10)
- Samsung S10+_(Note10+ 5G / Note10+ / Note 10 / Tab S6 / S10 5G / S10 / S10e / Fold 5G / Fold / Z Flip)

VID11211

- Samsung A52 5G (A52 5G / A42 5G)
- Samsung A71 5G (A71 5G / A51 5G)
- Samsung Tab Active 3

VID11315

- Panasonic ToughBook FZN1 (FZN1 / FZS1 / FZA3)

8 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 Cyber Reliant Mobile Data Defender for Android SDK Version, Version 0.2, March 9, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/FE10 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices and gives an overview of the testing.

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 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 Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/FE10.

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 Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validators 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 Evaluator performed the assurance activities specified in the ASPP14/FE10 related to the examination of the information contained in the TSS.

The Validators 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 Validators 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 identified.

The Validators 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 ASPP14/FE10 and recorded the results in a Test Report, summarized in the AAR.

The Validators 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 Detailed Test Report (DTR) prepared by the Evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 3/7/2023 with the following search terms: “Trivalent”, “File Encryption”, “Android Encryption”, “Security First”, “SPX Core”, “Secure Parser”, “Cyber Reliant”, and “CRC”.

The Validators 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 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 evaluated configuration instructions in the User Guide Cyber Reliant Defender Installation and Use, March 2023 (AGD). No 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 Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cyber Reliant Mobile Data Defender for Android SDK Version 4.0 Security Target, Version 0.6, March 16, 2023*.

13 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

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] Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14).

[5] PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10).

[6] Cyber Reliant Mobile Data Defender for Android SDK version 4.0 Security Target, Version 0.6, March 16, 2023 (ST).

[7] Cyber Reliant Defender Installation and Use, March 2023, March 2023 (AGD).

[8] Assurance Activity Report for Cyber Reliant Mobile Data Defender for Android SDK Version 4.0, Version 0.3, March 16, 2023 (AAR).

[9] Detailed Test Report for Cyber Reliant Mobile Data Defender for Android SDK Version 4.0, Version 0.2, March 9, 2023 (DTR).

[10] Evaluation Technical Report for Cyber Reliant Mobile Data Defender for Android SDK Version, Version 0.3, March 16, 2023 (ETR)