

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

CyberReliant Corp.

175 Admiral Cochrane Drive, Suite 404

Annapolis, MD 21401

CRC Data at Rest (DaR) Service
(Native)
Version 1.0.0 (Version Code 2)

Report Number: CCEVS-VR-10651-2015
Dated: October 29, 2015
Version: 0.3

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Ken Elliott
Herb Ellis
Kelly Hood
Jerome Myers
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Chris Keenan
Cornelius Haley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1	Executive Summary	1
2	Identification	2
3	Architectural Information	3
3.1	TOE Evaluated Platforms	3
3.2	TOE Architecture.....	4
3.3	Physical Boundaries.....	4
4	Security Policy	4
4.1	Cryptographic support	5
4.2	User data protection	5
4.3	Identification and authentication.....	5
4.4	Security management.....	5
4.5	Protection of the TSF.....	5
4.6	Trusted path/channels	6
5	Assumptions.....	6
6	Documentation.....	6
7	IT Product Testing	6
7.1	Developer Testing.....	6
7.2	Evaluation Team Independent Testing	6
8	Evaluated Configuration	7
9	Results of the Evaluation	7
9.1	Evaluation of the Security Target (ASE).....	7
9.2	Evaluation of the Development (ADV).....	7
9.3	Evaluation of the Guidance Documents (AGD).....	8
9.4	Evaluation of the Life Cycle Support Activities (ALC).....	8
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	8
9.6	Vulnerability Assessment Activity (VAN).....	8
9.7	Summary of Evaluation Results.....	9
10	Validator Comments/Recommendations	9
11	Annexes.....	9
12	Security Target.....	9
13	Glossary	9
14	Bibliography	10

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of CRC Data at Rest (DaR) Service (Native) solution provided by CyberReliant 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 Catonsville, MD, United States of America, and was completed in October 2015. 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.

The Target of Evaluation (TOE) is the CRC Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2). The TOE is an application package residing on an evaluated mobile device running Android 4.4. The TOE is a software solution providing the capability to handle file encryption on mobile devices.

CRC's DaR Service (Native) provides file level encryption through an APK and a library implementation. DaR Service (Native) contain Java interfaces in order to support majority of android application storage requirements. The implementation and functionality for java is provided by the TOE.

The Target of Evaluation (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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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 CyberReliant Corp Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target, Version 0.6, 10/21/15 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) for Evaluation Assurance Level (EAL) 1 through 4 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:	CRC Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2) (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Application Software, Version: 1.1, 5 November 2014 (ASPP11) with the following extended package: Extended Package: File Encryption. Version 1.0, 11/10/2014 (ASPP11/FEEP10)
ST:	CyberReliant Corp Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target, Version 0.6, 10/21/15
Evaluation Technical Report	Evaluation Technical Report for CRC CRC Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2), Version 0.3, October 29, 2015.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	CyberReliant Corp.
Developer	CyberReliant Corp.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Ken Elliott Herb Ellis Kelly Hood Jerome Myers Aerospace Corporation

3 Architectural Information

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

The Target of Evaluation (TOE) is CyberReliant Corporation's (CRC) Data at Rest (DaR) Service (Native) software application package residing on an evaluated mobile device running Android 4.4. The TOE is a software solution providing the capability to handle file encryption on mobile devices.

CRC's DaR Service (Native) provides file level encryption through an APK and a library implementation. DaR Service (Native) contain Java interfaces in order to support majority of android application storage requirements. The implementation and functionality for java is provided by the TOE.

The DaR's Management Service implementation is a straight Java DaR Service (Native) APK and a library to be included into one's mobile application (and then one can use the API). The Management Service (Native) runs in the background and uses both Android and BouncyCastle keystores to provide the File Encryption Key Encryption Key (FEKEK) to each of the applications. The DaR Service (Native) also uses the Android keystore to store an RSA key pair used by the Management service, and a per application android keystore to store each application's RSA keypair to wrap the AES-wrapped file encryption key encryption key. The Management Service handles necessary user 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 native Android cryptographic API.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the application package residing on an evaluated mobile device running Android 4.4. During evaluation testing, Gossamer tested the CRC DaR on the Samsung Galaxy Note 3 running Android 4.4.

3.2 TOE Architecture

The TOE is software installed on an evaluated mobile device running Android 4.4. The TOE software is installed as a Management Service as well as a 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 DaR password from the user and double wraps the FEKEK by using RSA-2048 first and then wrapping it again using AES-256.

The TOE's interface library is compiled into another application's package. The library allows the other application to invoke the TOE's services. This library allows the application to call the TOE's file encryption services. The application must register itself with the DaR Management Service. Applications registered to the TOE have a unique RSA public/private keypair, so applications pass their RSA public keys to the DaR Management Service along with a certificate fingerprint (which is what the application uses as the password to the application's BouncyCastle 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 BouncyCastle keystore and the single wrapped FEKEKs in the Application's specific BouncyCastle keystore. The keys are protected by requiring a password to load both the Management Service and Application's BouncyCastle keystore. In order for other applications to access its FEK, the application must use the TOE's interface library API in order to request the Management Service's 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 BouncyCastle keystore. The wrapped FEKEKs in each application's BouncyCastle keystore are ephemeral. The Management Service has a configurable timer in which all BouncyCastle keystores will be wiped once the timer expires.

The TOE relies on the evaluated platform's Android API for generating keys as well as performing cryptographic operations. The TOE invokes Android's cryptographic API to generate AES-256 bit keys.

During evaluation testing, Gossamer tested the CRC DaR on the Samsung Galaxy Note 3 running Android 4.4.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Android 4.4) on which the TOE resides.

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 Cryptographic support

The TOE uses the cryptographic services from the evaluated platform. The evaluated platform runs Android 4.4 operating system. Android's APIs allow generation of keys through KeyGenerator, and random numbers are generated using SecureRandom. Keys are used to protect data belonging to the applications that use the TOE.

4.2 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.

4.3 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 BouncyCastle keystore. Without the correct keystore, the application cannot load the keys necessary for file encryption/decryption.

4.4 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 the changing of passwords for management purposes.

4.5 Protection of the TSF

The TOE relies on 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, CRC shall deliver, via email or other agreed upon method, an updated application. The TOE's software is digitally signed by CyberReliant. Each update is accompanied by documentation outlining changes to the overall service, as well as compatible versions of the CRC API.

The native Android cryptographic library, which provides the TOE's cryptographic services, have built-in self-tests that are run at power-up to ensure that the algorithms are correct. If any of the self-tests fail, the TOE will not be able to perform its cryptographic services.

4.6 Trusted path/channels

The TOE does not transmit any data between itself and another product. All of the data managed by the TOE resides on the evaluated platform (Android 4.4).

5 Assumptions

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

- Protection Profile for Application Software, Version: 1.1, 5 November 2014 with the following extended package:
- Extended Package: File Encryption. Version 1.0, 11/10/2014

That information has not been reproduced here and the referenced Protection Profiles should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- [OM] Data at Rest (DaR) Data Encryption/Security Solution, CRC DaR Service Operations & Maintenance Manual, Version 1.0.2, October 27, 2015.

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 Detailed Test Report (ASPP11/FEED10) for CRC Data at Rest Service (Native), Version 0.4, 10/29/2015 .

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 a Common Criteria Certification document and ran the tests specified in the ASPP11 & FEED10 including the tests associated with optional and selection-based requirements.

8 Evaluated Configuration

The evaluated configuration consists of the CRC Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2) running on an evaluated mobile device running Android 4.4.

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 EAL1 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 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

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 Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2) products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 EAL 1 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 ASPP11 & FEED10 related to the examination of the information contained in the TSS.

The validator 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 EAL 1 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 validator 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 EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the ASPP11 & FEPP10 and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator 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 EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator 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

This was one of first evaluations performed against the Protection Profile for Application Software, Version: 1.1 and the first one that had included the File Encryption Extended Package. As a result the evaluators and validators identified multiple issues that needed to be addressed by the appropriate Technical Rapid Response Teams. Some of the issues resulted in formal Technical Decisions that have been published on the NIAP web site. There were some other trrt decisions that were made for this evaluation but that have not yet been finalized as formal Technical Decisions. Those will be published in further TDs and/or are noted in the applicable section of the Assurance Activity report.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: CyberReliant Corp Data at Rest (DaR) Service (Native) (ASPP11/FEED10) Security Target, Version 0.6, 10/21/15.

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 4, September 2012.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.
- [4] Protection Profile for Application Software, Version 1.1, May 2014 (ASPP11)
- [5] Extended Package: File Encryption. Version 1.0, 11/10/2014 (ASPP11/FEEP10)
- [6] CyberReliant Corp Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target, Version 0.6, 10/21/15 (ST)
- [7] Assurance Activity Report (ASPP11/FEEP10) for CRC Data at Rest Service (Native), Version 0.4, October 29, 2015 (AAR)
- [8] Detailed Test Report (ASPP11/FEEP10) for CRC Data at Rest Service (Native), Version 0.4, 10/291/2015 (DTR)