National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Trivalent

180 Admiral Cochrane Drive, Suite 410

Annapolis, MD 21401 U.S.A.

Trivalent Android Data Protection SDK version 2.13

Report Number: CCEVS-VR-10786-2017
Dated: April 13, 2017
Version: 0.4

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
Stelios Melachrinoudis

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, 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 Trivalent Android Data Protection SDK solution provided by Cyber Reliant Corporation d.b.a. Trivalent. 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 April 2017. 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 EAL 1.

The Target of Evaluation (TOE) is the Trivalent Android Data Protection SDK 2.0.

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 Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the Trivalent Android Data Protection SDK (ASPP12/ASFEEP10) Security Target, version 1.0, April 10, 2017 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) 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	Trivalent Android Data Protection SDK 2.0 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)
ST	Trivalent Android Data Protection SDK 2.0 Security Target, version 1.0, April 10, 2017
Evaluation Technical Report	Evaluation Technical Report for Trivalent Android Data Protection SDK 2.0, version 0.4, April 11, 2017
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	Trivalent
Developer	Trivalent
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Ken Elliott, Senior Validator
	Stelios Melachrinoudis, Lead Validator

3 Architectural Information

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

Trivalent's Android Data Protection SDK provides file level encryption through an 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 API: one set to manipulate files and one set to manipulate SQLite databases. While the API groups provide different abstractions for the read and write operations, they both 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 one's mobile application (and then the mobile application can use the library's APIs). The Management Service Application 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 Data Protection SDK 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 FEKEK. The Management Service 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 SPX Core (Security First, Secure Parser Library).

The Target of Evaluation (TOE) is Trivalent's Android Data Protection SDK Version 2.13 software application package residing on evaluated mobile devices running Android 5.1 and Android 6.0. The TOE is a software solution providing the capability to handle file encryption on mobile devices.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the application package residing on an evaluated mobile device running Android 5.1 or Android 6.0. During evaluation testing, Gossamer tested the Trivalent Android Data Protection SDK on the Samsung Galaxy S7 running Android 6.0.1 and the Galaxy Note 5 running Android 5.5.1.

Any of the products below utilize the Snapdragon 800 family processor and are appropriate for use with the TOE.

Device Name	Chipset/CPU	Architecture	Android Version
Samsung Galaxy S7 & S7 Edge	Exynos 8890	A64	6.0.1
Samsung Galaxy S7 & S7 Edge	Qualcomm MSM 8996	A64	6.0.1
Galaxy S6 & S6 Edge	Exynos 7420	A64	6.0.1
Galaxy Note 5	Exynos 7420	A64	5.1.1

3.2 TOE Architecture

The TOE is software installed on an evaluated mobile device running Android 5.1 or Android 6.0. 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 Android Data Protection 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.

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 Management Service. Applications registered to the TOE have a unique RSA public/private keypair, so applications pass their RSA public keys to the 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 utilizes Security First's Secure Parser Library (SPX Core) for cryptographic services. The TOE uses the SPX Core for generating 256 bit AES keys.

During evaluation testing, Gossamer tested the Trivalent Android Data Protection SDK on the Samsung Galaxy S7 running Android 6.0.1 and the Galaxy Note 5 running Android 5.5.1.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Android 5.1 or Android 6.0) on which the TOE resides.

4 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

4.1 Cryptographic support

The evaluated platform runs Android 5.1 or Android 6.0 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.

The TOE uses Security First's SPX Core (Security First, Secure Parser Library) for cryptographic algorithms. The SPX Core supports encryption via AES and random number generation via an SP 800-90 AES-256 CTR DRBG. The TOE uses the platform's cryptographic API to perform AES key wrapping and keyed hashing via HMAC.

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 Privacy

The TOE does not transmit Personally Identifiable Information over any network interfaces.

4.6 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, Trivalent shall deliver, via email or other agreed upon method, an updated application. The TOE's software is digitally signed by Trivalent. Each update is accompanied by documentation outlining changes to the overall service, as well as compatible versions of the Trivalent 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 self-tests fail, the TOE will not be able to perform its cryptographic services.

4.7 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 5.1 or Android 6.0).

5 Assumptions

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

- Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12) with the following extended package:
- Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)

That information has not been reproduced here and the ASPP12/ASFEEP10 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 ASPP12/ASFEEP10 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.

6 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 and Application Software Protection Profile Extended Package: 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.
- 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 ASPP and ASFEEP and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Trivalent Android Data Protection SDK Operations & Maintenance Manual, Version 2.13, December 2016

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 Detailed Test Report (ASPP12/ASFEEP10) for Android Data Protection SDK 2.0, Version 0.4, April 11, 2017 (DTR).

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 a Common Criteria Certification document and ran the tests specified in the ASPP12/ASFEEP10 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the Trivalent Android Data Protection SDK Version 2.13 residing on an evaluated mobile device running Android 5.1 or Android 6.0.

10 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).

10.1 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 Trivalent Android Data Protection SDK 2.0 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.

10.2 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 ASPP12 & ASFEEP10 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.

10.3 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 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.

10.4 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 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.

10.5 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 ASPP12 & ASFEEP10 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each 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.

10.7 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.

11 Validator Comments/Recommendations

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the Trivalent Android

Data Protection SDK, to include software or components that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

This was one of the first evaluations performed against the Protection Profile for Application Software, Version 1.2 and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0. As such, there were multiple issues identified by evaluators and validators that needed to be addressed by the appropriate Technical Rapid Response Teams. Generally, issues resulted in formal Technical Decisions published on the NIAP web site. The Technical Decisions that apply to this evaluation are clearly marked in the ST and AAR. For TRRT decisions made for this evaluation that haven't been finalized, they will be published in further TDs and/or are noted in the applicable section of the Assurance Activity Report.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Trivalent Android Data Protection SDK (ASPP12/ASFEEP10) Security Target, Version 1.0, April 10, 2017*.

14 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.

15 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 1.2, 22 April 2016 (ASPP12) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)

[5] Trivalent Android Data Protection SDK (ASPP12/ASFEEP10) Security Target, Version 1.0, April 10, 2017 (ST)

[6] Assurance Activity Report (ASPP12/ASFEEP10) for Android Data Protection SDK 2.0, Version 0.4, April 11, 2017 (AAR)

[7] Detailed Test Report (ASPP12/ASFEEP10) for Android Data Protection SDK 2.0, Version 0.4, April 11, 2017 (DTR)

[8] Evaluation Technical Report for Trivalent Android Data Protection SDK, Version 0.4, April 11, 2017 (ETR)