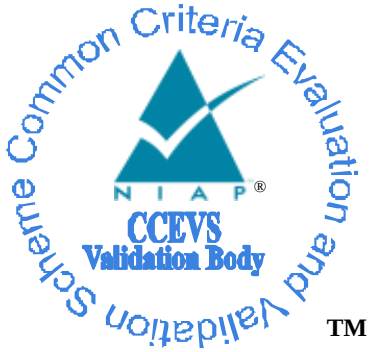
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Trivalent

180 Admiral Cochrane Drive, Suite 410

Annapolis, MD 21401 USA

Trivalent Protect (for Android) 2.6

Report Number: CCEVS-VR-10856-2018
Dated: June 13, 2018
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
Jerome Myers
The Aerospace Corporation
Columbia, MD

Michelle Carlson
Stelios Melachrinoudis
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 1
2 Identification 1
3 Architectural Information 3
3.1 TOE Evaluated Platforms 3
3.2 TOE Architecture 3
3.3 Physical Boundaries 4
4 Security Policy 4
4.1 Cryptographic support 4
4.2 User data protection 5
4.3 Identification and authentication 5
4.4 Security management 5
4.5 Privacy 5
4.6 Protection of the TSF 5
4.7 Trusted path/channels 5
5 Assumptions 6
6 Clarification of Scope 6
7 Documentation 6
8 IT Product Testing 7
8.1 Developer Testing 7
8.2 Evaluation Team Independent Testing 7
9 Evaluated Configuration 7
10 Results of the Evaluation 7
10.1 Evaluation of the Security Target (ASE) 8
10.2 Evaluation of the Development (ADV) 8
10.3 Evaluation of the Guidance Documents (AGD) 8
10.4 Evaluation of the Life Cycle Support Activities (ALC) 8
10.5 Evaluation of the Test Documentation and the Test Activity (ATE) 9
10.6 Vulnerability Assessment Activity (VAN) 9
10.7 Summary of Evaluation Results 9
11 Validator Comments/Recommendations 9
12 Annexes 11
13 Security Target 11
14 Glossary 11
15 Bibliography 13

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Trivalent Protect (for Android) solution provided by 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 June 2018. 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 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).

The Target of Evaluation (TOE) is the Trivalent Protect (for Android) 2.6.

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 Trivalent Protect (for Android) (ASPP12/ASFEEP10) Security Target, Version 0.8, June 4, 2018 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Trivalent Protect (for Android) 2.6 (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 Protect (for Android) 2.6 Security Target, Version 0.8, June 4, 2018
Evaluation Technical Report	Evaluation Technical Report for Trivalent Protect (for Android) 2.6, version 0.4, June 4, 2018
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, Aerospace Corporation
	Jerome Myers, The Aerospace Corporation
	Michelle Carlson, The MITRE Corporation
	Stelios Melachrinoudis, The MITRE 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 Trivalent Protect (for Android) Version 1.2.0 software application package residing on evaluated Getac MX50 mobile devices running Android 5.1.1. The TOE is a privileged application built-in to the Getac MX50 ruggedized table that provides the capability to handle file encryption. The Getac MX50 utilizes the Intel Atom Z8350 processor.

Trivalent Protect (for Android) provides file level encryption through a privileged software that is built into the Getac MX50 mobile device. The Trivalent Protect (for Android) software uses encryption, to protect data from unauthorized users. Trivalent Protect (for Android) enhances the level of encryption for secure data-at-rest by providing additional encryption distinct from the data-at-rest protection provided by the platform.

Trivalent Protect (for Android) runs in the background and uses both Android and BouncyCastle keystore to protect the File Encryption Key Encryption Key (FEKEK) that is used for encryption of user data. The FEKEK is a 256-bit AES key that is used by Trivalent Protect (for Android) for file level encryption, transparently to all Android applications, for the internal public app storage ("/sdcard"). Note that the applications' sandbox storage "/data/data/<app>" is not applicable. Encryption using the FEKEK by Trivalent Protect (for Android) is provided by the SPX Core (Security First, Secure Parser Library).

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the Trivalent Protect (for Android) Version 2.6 software application package residing on evaluated Getac MX50 mobile devices running Android 5.1.1.

3.2 TOE Architecture

The TOE is software that is built-in to the Getac MX50 evaluated ruggedized table. The TOE is composed of three major components: a management service application, the Trivalent system service and the FUSE daemon. The Management Service application is delivered by Trivalent and the Trivalent system service and FUSE daemon are delivered as part of the Getac mobile device.

- The Management Service application is responsible for system configuration, initialization, authentication/de-authentication, FEKEK generation and centralized key management.
- The Trivalent System Service is responsible for communication with the FUSE daemon. It is also responsible for securely passing the FEKEK from the Management Service to the FUSE daemon.
- The FUSE daemon is responsible for file I/O, and file encryption/decryption

The TOE utilizes the platform provided BouncyCastle and Android Key stores.

The Management Service obtains the user's FUSE password (hereafter referred to as the DaR password). An AES key derived from the DaR password unwraps one layer of the double-wrapped FEKEK. The Management Service's RSA private key is then used to unwrap the second layer of the FEKEK. The Management Service then wraps the fully-unwrapped FEKE using the Trivalent System Service's RSA public key and sends it to the service for further processing. The Trivalent System Service uses its RSA private key to unwrap the FEKEK before passing the user's FEKEK down to the FUSE daemon. The Trivalent System Service acts as a secure intermediary for the Management Service to communicate with the FUSE daemon. An Android system service is needed as applications cannot directly communicate with Android daemons.

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 per-file FEK. The Android platform generates the 256-bit AES FEKEK through the KeyGenerator API. The Android platform-based AndroidKeyStore provider is used to generate RSA key pairs.

During evaluation testing, Gossamer tested the Trivalent FUSE on the Getac MX50 running Android 5.1.1.

The TOE is capable of communicating with a Trivalent Configuration Manager (TCM) server. This communication is protected using platform provided TLSv1.2.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Getac MX50) 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 Getac MX50 platform runs Android 5.1.1 operating system. The platform's Android 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. The TOE also uses the Android platform-based AndroidKeyStore provider to generate RSA key pairs.

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. The TOE protects communication with a Trivalent Configuration Manger (TCM) server using a TLS v1.2 communication path.

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.

The Security First's SPX Core and native Android (platform provided) cryptographic libraries provides the TOE's cryptographic services. These cryptographic service providers 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 protects all communication to a TCM server using TLSv1.2. All of the data managed by the TOE resides on the evaluated Getac MX50 platform.

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) 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)

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 with File Encryption Extended Package and performed by the evaluation team). More specifically, the evaluation of platform-provided security functionality already covered by the Mobile Device Fundamentals PP (MDFPP) or Operating Systems (OSPP) is outside the scope of this evaluation.
- 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 ASPP12/ASFEEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. Any non-security related functional capabilities of the TOE were not covered in this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- USER GUIDE Trivalent Protect 2.6 for Android, November 2017

This is the only document that should be trusted by the administrator in setting up the TOE into its evaluated configuration.

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 (ASPP12/ASFEEP10) for Trivalent Protect (for Android) 2.6, Version 0.4, June 4, 2018 (DTR) and summarized in the non-proprietary 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 a Common Criteria Certification document and ran the tests specified in the ASPP12/ASFEEP10 including the tests associated with optional requirements. The non-proprietary AAR provides a list of devices, test tools and diagrams for the test environment in Section 3.4.1 (Independent Testing Conformance (ATE_IND.1)). More detailed results of testing can be found in the proprietary Detailed Test Report (DTR) prepared by the evaluator.

9 Evaluated Configuration

Trivalent Protect (for Android) Version 2.6 software application package residing on evaluated Getac MX50 mobile devices running Android 5.1.1. The products must be configured in accordance with the guidance listed in the Documentation section (Section 7 of this VR).

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 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 4 and CEM version 3.1 rev 4. The evaluation determined the Trivalent Protect (for Android) TOE to be Part 2 extended, and to meet the SARs contained in the ASPP12/ASFEEP10.

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 Protect (for Android) 2.6 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 AAR.

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 vulnerability analysis is in the proprietary 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 vulnerability analysis was performed on June 7, 2018.

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/) with the following search terms: "Trivalent", "FUSE", "Trivalent Protect", "File Encryption", "Android Encryption", "Security First", "SPX Core", "Secure Parser", “libparser4.so”, “libparser4jni.so”, and” libcryptopp.so.”

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 Protect, 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.

For FDP_PRT_EXT.1, the TSS describes a sophisticated method of encrypting large files, which involves processing threads not invoked when encrypting the small one-line test files used in the test procedures. The test assurance activities do not require large-file testing, thus the test on smaller files is sufficient for this evaluation. The claimed functionality with respect to the M:N shreds was not tested.

11.1 TRRT Requests and Technical Decisions (TDs)

A few TRRT requests were made throughout this evaluation, resulting in TDs. They are described below:

11.1.1 Missing selection in FCS_CKM.1(1)

This issue concerns FCS_CKM.1(1) of the Application Software PP v1.2, which includes an assurance activity stating that either the platform or application can generate asymmetric keys. However, it would be much clearer and correct to also have a selection in the requirement to allow for either the platform or application to generate these keys. The original requirement wording only allows for the application to perform the function which contradicts the corresponding assurance activity.

The Application Software TC agreed with this assessment and has subsequently issued TD0293, which has been superseded by TD0326.

11.1.2 Current or evaluated version [for FPT_AEX_EXT.1.3]?

This issue concerns the assurance activity of FPT_AEX_EXT.1.3 of the Application Software PP v1.2, which states that the application must be able to successfully run on the latest version of Android. However, for this evaluation and others, it would be infeasible to do so if the underlying platform is an earlier version (in this case, Android 5.1.1) than the latest Android version. Moreover, testing the application on the latest version requires taking the supported mobile device out of its evaluated configuration or testing on a non-supported mobile device, which is also not acceptable.

The Application Software TC agreed with this assessment and has subsequently issued TD0295, which supersedes TD0269.

11.1.3 FDP_DAR_EXT.1 and Sensitive Data

This issue concerns the definition of sensitive data and the assurance activity for FDP_DAR_EXT.1. More specifically, FDP_DAR_EXT.1 does not call for the TSS to identify the sensitive data and does not call out FCS_STO_EXT.1 in protecting credentials and keys. A TD was requested to modify the requirement and assurance activity for FDP_DAR_EXT.1.

The Application Software TC agreed with this assessment and has subsequently issued TD0300.

11.1.4 FCS_STO_EXT.1 Android Platform Check

This issue concerns the test assurance activity for FCS_STO_EXT.1, which states that "the evaluator shall verify that the application uses the Android KeyStore or the Android KeyChain to store certificates." It was uncertain as to whether it was sufficient to simply list the contents of the /data/misc/keystore and make the correspondence between the files in that directory and the parts of the TOE with RSA key-pairs associated with them, rather than verify that the relevant keystore calls were made. The Application Software TC stated that it is sufficient to obtain the owner of the /data/misc/keystore and verify that it is the same as the App ID. Thus, it reasonably confirms that the correct libraries are being used. No TD was issued for this TRRT resolution.

11.1.5 FMT_CFG_EXT.1.2 Are Directories Files?

This issue concerns the test assurance activity for FMT_CFG_EXT.1.2 which states that "the command should not print any files". The lab showed that directories were returned as part of traversal but stated that no files were returned in the AAR. The TRRT concluded that per Unix/Linux conventions, directories are considered files but can still be traversed with directory contents listed. The next version of the PP is intended to clarify this point. No TD was issued for this TRRT resolution as of the conclusion of this evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Trivalent Protect (for Android) (ASPP12/ASFEEP10) Security Target, Version 0.8, June 4, 2018*.

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 2012.

[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 Protect (for Android) (ASPP12/ASFEEP10) Security Target, Version 0.8, June 4, 2018 (ST)

[6] Assurance Activity Report (ASPP12/ASFEEP10) for Trivalent Protect (for Android) 2.6, Version 0.4, June 4, 2018 (AAR)

[7] Detailed Test Report (ASPP12/ASFEEP10) for Trivalent Protect (for Android) 2.6, Version 0.4, June 4, 2018 (DTR)

[8] Evaluation Technical Report for Trivalent Protect (for Android), Version 0.4, June 4, 2018 (ETR)