National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Samsung Electronics Co., Ltd.

416 Maetan-3dong, Yeongtong-gu, Suwon-si, Gyeonggi-do, 443-742 Korea

Samsung Electronics Co., Ltd. Samsung Galaxy S5 with KNOX 2

Report Number: CCEVS-VR-VID10596-2014
Dated: October 31, 2014
Version: 1.0

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

Luke Florer
Meredith Hennan
Jerry Myers
Ken Stutterheim
Aerospace Corporation
Columbia, MD

Sheldon Durrant
MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
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 Samsung Galaxy S5 with KNOX 2 solution provided by Samsung Electronics Co., Ltd. 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 2014. 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) are the Samsung Galaxy S5 with KNOX 2 products.

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 Samsung Electronics Co., Ltd. Samsung Galaxy S5 with KNOX 2 (MDFPP11) Security Target 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) 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:	Samsung Electronics Co., Ltd. Samsung Galaxy S5 with KNOX 2
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 1.1, 12 February 2014
ST:	Samsung Electronics Co., Ltd. Samsung Galaxy S5 with KNOX 2 (MDFPP11) Security Target, Version 0.4, October 14, 2014
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy S5 with KNOX 2.0 (MDFPP11) , Version 3.3, October 31, 2014
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	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Kenneth Elliott, The Aerospace Corporation
	Luke Florer, The Aerospace Corporation
	Meredith Hennan, The Aerospace Corporation

Item	Identifier
	Jerry Myers, The Aerospace Corporation
	Ken Stutterheim, The Aerospace Corporation
	Sheldon Durrant, The MITRE Corporation

3 Architectural Information

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

The TOE is a mobile operating system based on Android 4.4 with modifications made to increase the level of security provided to end users and enterprises. The TOE is intended to be used as part of an enterprise messaging solution providing mobile staff with enterprise connectivity.

The TOE includes a Common Criteria mode (or "CC mode") that an administrator can manage through use of a Mobile Device Management System (MDM). The TOE must be configured as follows in order for an administrator to transition the TOE to CC mode.

- Require a screen lock password (swipe, PIN, pattern, or facial recognition screen locks are not allowed).
- The maximum password failure retry policy should be less than or equal to ten.
- Device encryption must be enabled.
- SD Card encryption must be enabled.

When CC mode has been enabled, the TOE behaves as follows.

- The TOE sets the system wide Android CC mode property to "Enabled".
- The TOE performs FIPS 140-2 power-on self-tests.
- The TOE performs self-tests for the Samsung Key Management Module v2.0.
- The TOE performs secure boot integrity checking of the kernel and key system executables.
- The TOE prevents loading of custom firmware/kernels and requires all updates occur through FOTA (Samsung's Firmware Over The Air firmware update method)
- The TOE uses FIPS 140-2 approved cryptographic ciphers when joining and communicating with wireless networks.
- The TOE utilizes FIPS 140-2 approved cryptographic ciphers for TLS.
- The TOE ensures FOTA updates utilize 2048-bit PKCS #1 RSA-PSS formatted signatures (with SHA-512 hashing).

The TOE includes a containerization capability, KNOX 2. This container provides a way to segment applications and data into two separate areas on the device, such as a personal area and a work area, each with its own separate apps, data and security policies. In this evaluation the KNOX container functionality is enabled, which requires an additional license to be purchased

There are two different models of the TOE, the Samsung Galaxy S5 with KNOX 2. Samsung manufactures the Galaxy S5 hardware in an LTE and 3G cellular radio variant and offers each variant with 16GB or 32GB of internal Flash storage.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy S5 with KNOX 2. The evaluated version of the mobile device is as follows.

- Base Model Number: SM-G900
- Android version: 4.4.2
- Kernel version: 3.4.0
- Build number: KOT49H
- Security software version: MDF v1.0 Release 3.

3.2 TOE Architecture

The TOE combines with a Mobile Device Management solution that enables the enterprise to watch, control and administer all deployed mobile devices, across multiple mobile service providers as well as facilitate secure communications through a VPN. This partnership provides a secure mobile environment that can be managed and controlled by the environment and reduce the risks that can be introduced through a Bring-Your-Own-Device (BYOD) model.

Data on the TOE is protected through the implementation of Samsung On-Device Encryption (ODE) which utilizes a FIPS 140-2 certified cryptographic module to encrypt device and SD card storage. This functionality is combined with a number of on-device policies including local wipe, remote wipe, password complexity, automatic lock and privileged access to security configurations to prevent unauthorized access to the device and stored data.

The Samsung Enterprise Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to more than 390 configurable policies and including additional security functionality such as application whitelisting and blacklisting.

3.3 Physical Boundaries

The TOE is a multi-user operating system based on Android (4.4) that incorporates the Samsung Enterprise SDK. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. The method of use for the TOE is as a mobile messaging and VPN device for use within an enterprise environment where the configuration of the device is managed through a compliant device management solution.

The TOE communicates and interacts with 802.11-2012 Access Points to establish network connectivity, and through that connectivity interacts with MDM servers that allow administrative control of the TOE.

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. TOE access
7. Trusted path/channels

4.1 Cryptographic support

The TOE includes a cryptographic module with FIPS 140-2 certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS and HTTPS and also to encrypt the media (including the generation and protection of data, right, and key encryption keys) used by the TOE. Many if these cryptographic functions are also accessible as services to applications running on the TOE.

4.2 User data protection

The TOE is designed to control access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE is design to protect user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected. The functionality provided by the KNOX container enhances the

security of user data by providing an additional layer of separation between apps and data while the device is in use.

4.3 Identification and authentication

The TOE supports a number of features related to identification and authentication. From a user perspective, except for making phone calls to an emergency number, a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display and the frequency of entering passwords is limited and when a configured number of failures occurs, the TOE will be wiped to protect its contents. Passwords can be constructed using upper and lower cases characters, numbers, and special characters and passwords up to 16 characters are supported. The TOE can also serve as an 802.1X supplicant and can use X509v3 and validate certificates for EAP-TLS and TLS, exchanges.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target as well as other functions commonly found in mobile devices. Many of the available functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled. Once the TOE has been enrolled and then un-enrolled, it removes all MDM policies and disables CC mode.

4.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as cryptographic keys so that they are not accessible or exportable. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). It enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It is also designed to protect itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fail, the TOE will not go into an operational mode. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

4.6 TOE access

The TOE can be locked, obscuring its display, by the user or after a configured interval of inactivity. The TOE also has the capability to display an advisory message (banner) when users unlock the TOE for use. The TOE is also able to attempt to connect to wireless networks as configured.

4.7 Trusted path/channels

The TOE supports the use of 802.11-2012, 802.1X, EAP-TLS, and TLS to secure communications channels between itself and other trusted network devices.

5 Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile For Mobile Device Fundamentals, Version 1.1, 12 February 2014 (MDFPP). That information has not been reproduced here and the MDFPP should be consulted if there is interest in that material.

6 Documentation

The following documentation was used as evidence for the evaluation of the Samsung Galaxy S5 with KNOX 2:

- Samsung Android 4.4 on Galaxy Devices Guidance Documentation, version 1.14, October 30, 2014
- Samsung Android 4.4 on Galaxy Devices User Guidance Documentation, version 1.7, October 28, 2014

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report for Samsung Galaxy S5 with KNOX 2 (MDFPP11), Version 1.2, October 31, 2014. Further details may be found in the Assurance Activity Report [1]. The Detailed Test Report is proprietary.

The following diagrams depict the test environments used by the evaluators.

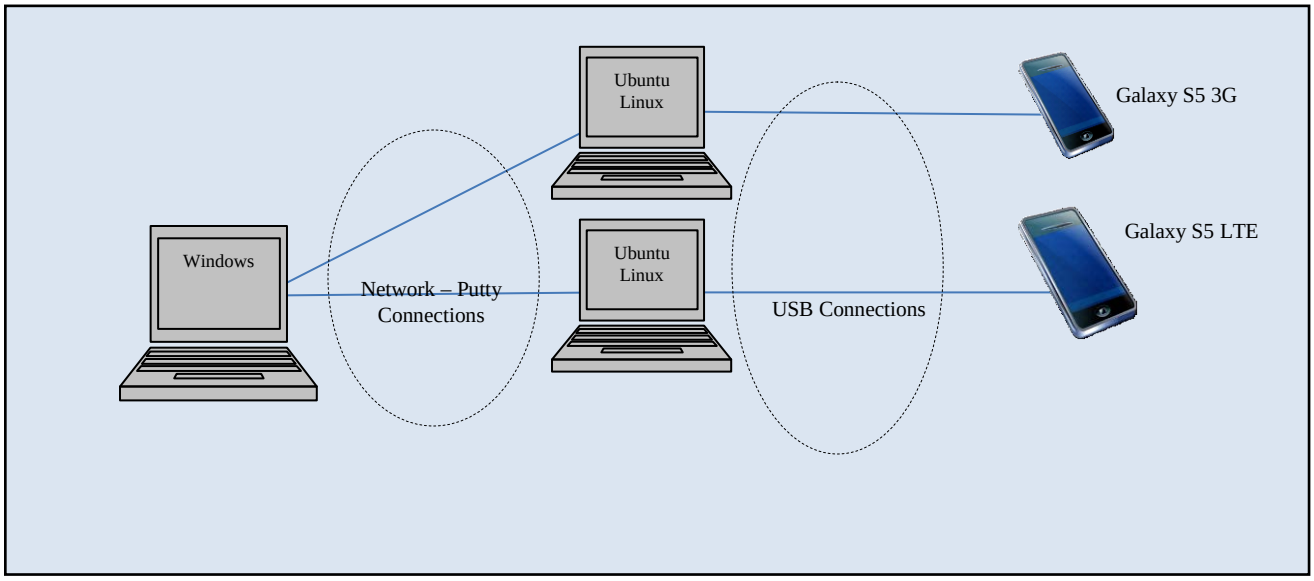

Figure 1 Developer Test Setup

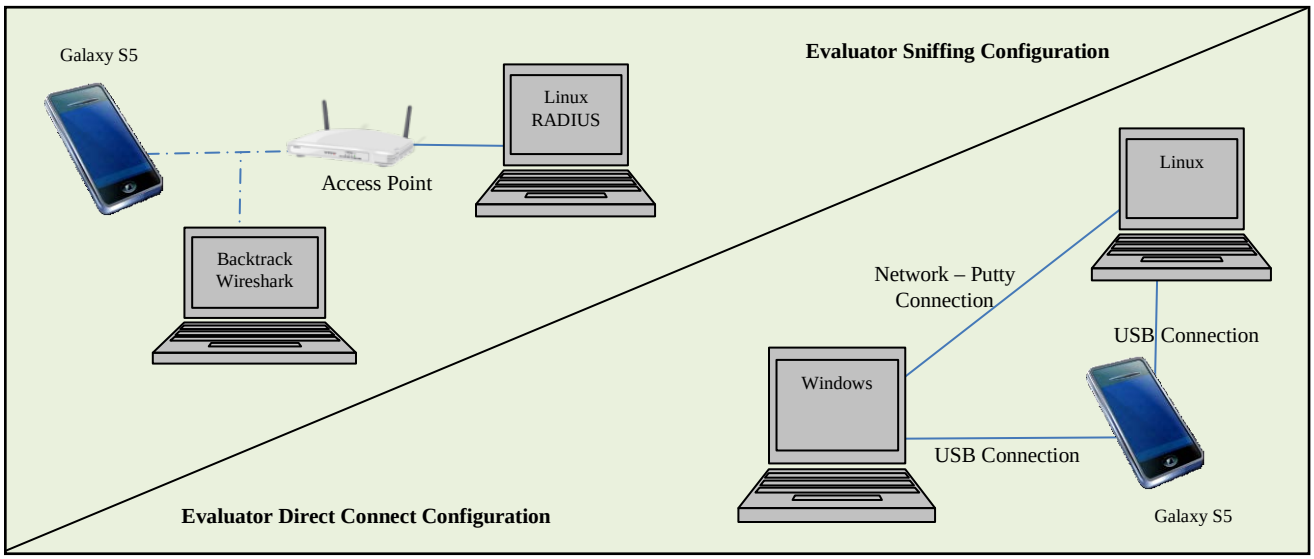

Figure 2 Evaluator Test Setup

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 the Samsung Android 4.4 on Galaxy Devices Guidance Documentation, version 1.14, October 30, 2014 document and ran the tests specified in the MDFPP.

8 Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy S5 with KNOX 2 devices as configured in accordance with CC Configuration Guidance specified in this document.

To use the product in the evaluated configuration, the product must be configured as specified in Samsung Android 4.4 on Galaxy Devices Guidance Documentation, version 1.14, October 30, 2014.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented further in the non-proprietary Assurance Activity Report [1]. The evaluation assurance activities are described in [1] and the proprietary Evaluation Technical Report. Those activities include performance of all EAL1 work units resulting in 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 Samsung Galaxy S5 with KNOX 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 MDFPP 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 MDFPP and recorded the results in a Test Report, summarized in the Assurance Activity Report for Samsung Galaxy S5 with KNOX 2.0 (MDFPP).

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

The analysis and testing for this evaluation relied upon some of the results from a prior evaluation for Samsung Electronics Co., Ltd. Samsung Galaxy S5 & Note 10.1.2014 Edition. The software for the previous evaluation included the same licensed version of KNOX. In that prior evaluation, the KNOX containers were not enabled. Hence, for this evaluation, only the functionality implemented by the SFR's within the Security Target that pertain to the KNOX containers was retested. The validation team deems this acceptable as the evaluated configuration of the TOE did not change.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Samsung Electronics Co., Ltd. Samsung Galaxy S5 with KNOX 2 (MDFPP11) Security Target, Version 0.4, October 14, 2014*.

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.
- **MDFPP.** Protection Profile for Mobile Device Fundamentals.
- **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] Assurance Activity Report for Samsung Galaxy S5 with KNOX 2.0 (MDFPP), Version 4.2, October 31, 2014.

[2] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[5] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

[6] Protection Profile For Mobile Device Fundamentals, Version 1.1, 12 February 2014.

[7] Samsung Android 4.4 on Galaxy Devices Guidance Documentation, Version 1.14, October 30, 2014