# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


## Validation Report

## KeyW Corporation

# KeyW Protect for Samsung, Version 1.2.1.0

**Report Number:** CCEVS-VR-11061-2020
**Dated:** June 9, 2020
**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

Sheldon Durrant
John Butterworth
Jenn Dotson
Patrick Mallett

### 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 KeyW Protect for Samsung, Version 1.2.1.0 solution provided by KeyW Corporation. 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 2020. 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 1.3, 01 March 2019 (PP_APP_V1.3) with PP-Module for File Encryption, Version 1.0, 25 July 2019 (MOD_FE_V1.0).

The Target of Evaluation (TOE) is the KeyW Protect for Samsung, Version 1.2.1.0.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation Team monitored the activities of the Evaluation Team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation Team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation Team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the KeyW Protect for Samsung, Version 1.2.1.0 (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.4, 06/04/2020 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** | KeyW Protect for Samsung, Version 1.2.1.0<br>(Specific models identified in Section 3.1) |
| **PP-Configuration** | PP-Configuration for Application Software and File Encryption, Version 1.0, 25 July 2019 |
| **ST** | KeyW Protect for Samsung, Version 1.2.1.0 (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.4, 06/04/2020 |
| **Evaluation Technical Report** | Evaluation Technical Report for KeyW Protect for Samsung, Version 1.2.1.0, Version 0.3, June 4, 2020 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 conformant |
| **Sponsor** | United States Special Operations Command (USSOCOM) |
| **Developer** | KeyW Corporation |
| **Common Criteria Testing Lab (CCTL)** | Gossamer Security Solutions, Inc. |
| **CCEVS Validators** | Sheldon Durrant, John Butterworth, Jenn Dotson, Patrick Mallett |

# 3 Architectural Information

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

The KeyW Protect for Samsung application (i.e., the TOE) is a file encryption tool that runs on a Samsung mobile device with Android OS 9.0, Knox 3.3 and DualDAR 1.0. The

Samsung Knox DualDAR API is used to relay all file operations within the Android Enterprise workspace to the TOE, which encrypts or decrypts the file contents automatically. The TOE is a headless Android OS Suite B Data-At-Rest (DAR) encryption application on the Samsung mobile device, which is designed to auto-run and register at mobile device startup for protection of files that reside within the Android Enterprise workspace. Therefore, the Android operating system will ensure that the mobile device features are available only when the TOE is running.

The TOE utilizes the Android OS 9.0 for storage of keys while the TOE includes the *Suite B Cryptographic Algorithms* library, which implements its own random bit generation, AES encryption/decryption, AES key wrapping, keyed-hashing functions, password-based key derivation, key pair generation, key establishment and cryptographic hashing, which have been certified through CAVP.

## 3.1 TOE Evaluated Platforms

The KeyW Protect for Samsung 1.2.1.0 TOE is also known as KEYWprotect. The following table shows the model numbers of the mobile devices used during evaluation testing of KEYWprotect:

| Device Name | Model Number | CPU | Android Version |
|---|---|---|---|
| Samsung Galaxy S10e | SM-G970 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy S10e | SM-G970 | Samsung Exynos 9820 | Android 9.0 |

**Table 1 - Tested Devices**

In addition to the evaluated devices, the following device models are claimed as equivalent since they have the same processors and run the same KEYWprotect software.

| Device Name | Model Number | CPU | Android Version |
|---|---|---|---|
| Samsung Galaxy S10 | SM-G973 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy S10 | SM-G973 | Samsung Exynos 9820 | Android 9.0 |
| Samsung Galaxy S10+ | SM-G975 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy S10+ | SM-G975 | Samsung Exynos 9820 | Android 9.0 |
| Samsung Galaxy S10 5G | SM-G977 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy S10 5G | SM-G977 | Samsung Exynos 9820 | Android 9.0 |
| Samsung Galaxy Note10 | SM-N970 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy Note10 5G | SM-N971 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy Note10+ | SM-N975 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy Note10+ 5G | SM-N976 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy A90 5G | SM-A908 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy Fold | SM-F900 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Galaxy Fold 5G | SM-F907 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Tab S6 (Wi-Fi) | SM-T860 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |
| Samsung Tab S6 (LTE) | SM-T865 | Qualcomm Snapdragon 855 (SDM855) | Android 9.0 |

**Table 2 - Equivalent Devices**

## 3.2 TOE Architecture

The TOE is an application that is installed as a required headless application when the Samsung mobile device is activated for Android Enterprise for use. Being a required application, the Android OS 9.0 platform with Knox 3.3 and DualDAR 1.0 ensures that the TOE is running prior to presenting the home screen to the user, and prevents all actions, which could uninstall the application. The TOE provides its own cryptographic functionality via the existing *Suite B Cryptographic Module*, which has been FIPS-validated through CAVP and CMVP certifications.

When the Android Enterprise workspace is unlocked, all workspace data created by other applications is automatically encrypted by the TOE and stored in the workspace file system via the Samsung Knox DualDAR API. Therefore, no clear text version of the file is ever created on the workspace file system.

## 3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Samsung mobile device with Android OS 9.0, Knox 3.3 and DualDAR 1.0) 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. Privacy
6. Protection of the TSF
7. Trusted path/channels

## 4.1 Cryptographic support

The TOE operates on a Samsung mobile device and uses features provided by the platform for key storage. The TOE includes the *Suite B Cryptographic Algorithms* library, which implements its own algorithms for random bit generation, AES encryption/decryption, AES key wrapping, keyed-hashing functions, password-based Key Derivation, key pair generation, key establishment and cryptographic hashing.

## 4.2 User data protection

The TOE protects user data by providing an integrated file encryption capability that automatically encrypts new files and decrypts files upon user demand. The TOE utilizes 256-bit AES encryption for confidentiality.

### 4.3 Identification and authentication

The TOE authenticates a user by requiring a password before any file data decryption operation is initiated. Without the correct password, the user is unable to decrypt the keys necessary to obtain clear text data from the Android Enterprise workspace file system.

### 4.4 Security management

The TOE does not allow encryption/decryption operations while in the locked state until the user authenticates to the device upon first use of the TOE. The TOE allows the following user management capabilities:

- Change workspace password.
- Reset workspace password using a reset token from the Unified Endpoint Management (UEM) console. Samsung Knox DualDAR by default does not disable reset passwords thereby enabling key recovery. To disable all key recovery mechanisms simply do not set a password using a token, which will prevent a password reset from the IT admin.
- Configure password/passphrase complexity settings including the minimum and maximum lengths.
- Perform a cryptographic erase of the data.
- Configure the corrective behavior (wipe/disable workspace) and number of failed validation attempts required to trigger corrective behavior.

### 4.5 Privacy

The TOE does not transmit Personally Identifiable Information over any network interfaces, nor does it request access to any applications that may contain such information.

### 4.6 Protection of the TSF

The TOE relies on the physical boundary of the evaluated platform as well as the Android 9.0 operating system for the protection of the TOE's application components.

Updates to the TOE are handled via the UEM console.

### 4.7 Trusted path/channels

The TOE does not transmit any data between itself and another network entity. All of the data managed by the TOE resides on the evaluated platform (Samsung mobile device with Android OS 9.0, Knox 3.3, and DualDAR 1.0).

## 5 Assumptions

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

- Protection Profile for Application Software, Version 1.3, 01 March 2019 (PP_APP_V1.3) with PP-Module for File Encryption, Version 1.0, 25 July 2019 (MOD_FE_V1.0)

That information has not been reproduced here and the PP_APP_V1.3/MOD_FE_V1.0 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 PP_APP_V1.3/MOD_FE_V1.0 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 PP_APP_V1.3/MOD_FE_V1.0 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.

# 7 Documentation

The following document was available with the TOE for evaluation:

- Android OS Suite B Data At Rest v1.2.1.0 – User Guide, Document Version 1.3, 05/19/2020

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

# 8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for KeyW Protect for Samsung, Version 0.2, May 19, 2020 (DTR), as summarized in the evaluation Assurance Activity Report.

## 8.1 Developer Testing

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

## 8.2 Evaluation Team Independent Testing

The Evaluation Team verified the product according to a Common Criteria Certification document and ran the tests specified in the PP_APP_V1.3/MOD_FE_V1.0 including the tests associated with optional requirements. The AAR, in sections 1.1 and 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

# 9 Evaluated Configuration

See Section 3.1.

# 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 5 and CEM version 3.1 rev 5. The evaluation determined the KeyW Protect for Samsung TOE to be Part 2 extended, and to meet the SARs contained in the PP_APP_V1.3/MOD_FE_V1.0.

## 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 KeyW Protect for Samsung products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the Evaluation Team, and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

## 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 Evaluation Team performed the assurance activities specified in the

PP_APP_V1.3/MOD_FE_V1.0 related to the examination of the information contained in the TSS.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

## 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 validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

## 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 validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

## 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 PP_APP_V1.3/MOD_FE_V1.0 and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

## 10.6 Vulnerability Assessment Activity (VAN)

The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 5/15/2020 with the following search terms: "KeyW Protect", "KeyWProtect", "KeyW", "libKEYWcrypto", "libKEYWprotect",

"Samsung DualDaR", "DualDaR", "Knox", "containercore", “Suite B Cryptographic Algorithms”. No residual vulnerabilities exist in the TOE.

Additionally, the evaluator installed the Avast Mobile Security antivirus app on each TOE device, checked to ensure the definitions were current, and ran a scan on each device. In each case no issues were identified.

The validators reviewed the work of the Evaluation Team, and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

### 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 validation team suggests that the consumer pay particular attention to the installation guidance to ensure the product is placed into the evaluated configuration.

As was noted in the Clarification of Scope section of this report, the product provides more functionality than was covered by the evaluation. Only the functionality claimed in the SFR’s in the Security Target, on the supported devices described in section 3.1, was evaluated. All other functionality provided by the product needs to be assessed separately and no further conclusions should be drawn as to effectiveness, nor can any claims be made relative to their security based upon this evaluation.

Note: Per the information in Section 2 of the TOE’s guidance documentation (Android OS Suite B Data At Rest v1.2.1.0 – User Guide), the following Blackberry products are required for operating and managing the TOE in the evaluated configuration:

1. Blackberry Unified Endpoint Manager 12.12.1 (Service Pack 12 Maintenance Release 1)
2. Blackberry Unified Endpoint Manager Client 12.36.1.156359

## 12 Annexes

Not applicable

# 13 Security Target

The Security Target is identified as: *KeyW Protect for Samsung, Version 1.2.1.0 (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.4, 06/04/2020.*

# 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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Application Software, Version 1.3, 01 March 2019 (PP_APP_V1.3) with PP-Module for File Encryption, Version 1.0, 25 July 2019 (MOD_FE_V1.0).

[5] KeyW Protect for Samsung, Version 1.2.1.0 (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.4, 06/04/2020 (ST).

[6] Assurance Activity Report (PP_APP_V1.3/MOD_FE_V1.0) for KeyW Protect for Samsung, Version 1.2.1.0, Version 0.3, June 4, 2020 (AAR).

[7] Detailed Test Report for KeyW Protect for Samsung, Version 0.2, May 19, 2020 (DTR).

[8] Evaluation Technical Report for KeyW Protect for Samsung, Version 1.2.1.0, Version 0.3, June 4, 2020 (ETR).