National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Samsung Electronics Co., Ltd.
Knox File Encryption 1.6.0 – Fall

Report Number: **CCEVS-VR-VID11540-2024**

Dated: **November 27, 2024**

Version: **1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Ph.D.
Meredith Martinez
Mike Quintos
The Aerospace Corporation

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Gossamer Security Solutions, Inc.
Columbia, 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 Knox File Encryption 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 (TOE) 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 Columbia, MD, United States of America, and was completed in November 2024. 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 compliant with both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) with the PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10).

The Target of Evaluation is the Samsung Knox File Encryption 1.6.0.

The 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 (CCEVS) 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 Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.6.0 - Fall Security Target, Version 0.3, November 13, 2024 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	Samsung Knox File Encryption 1.6.0 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Application Software and File Encryption, Version 1.1, 07 April 2022 (CFG_APP-FE_v1.1) which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) with the PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10)
ST	Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.6.0 - Fall Security Target, Version 0.3, November 13, 2024
Evaluation Technical Report	Evaluation Technical Report for Samsung Knox File Encryption 1.6.0, Version 0.2, November 13, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome Myers, Ph.D. Meredith Martinez Mike Quintos

3 Architectural Information

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

The Target of Evaluation (TOE) is Samsung Knox File Encryption 1.6.0. The TOE is a service built into Samsung Knox that can provide an additional layer of file encryption when configured. This is available on devices with Android 14 and Knox 3.10.

3.1 TOE Description

The TOE is a software service built into Samsung Android 14 with Knox 3.10 to provide file encryption. Samsung Knox File Encryption is designed to provide a second encryption layer similar to and on top of the file-based encryption (FBE) layer for the entire device. The Knox File Encryption service runs in the background and utilizes Samsung Android cryptographic modules to provide file encryption services. The service is designed to run without any user intervention as all files will be encrypted automatically.

Knox File Encryption can be configured to encrypt files only in a Knox work profile or it can alternately be configured to encrypt the entire device. When configured as part of a Knox work profile, the service relies on the Knox work profile to provide the user's password for authentication (the password entered for the work profile), and then encrypts all files stored in the Knox work profile. When configured to encrypt all contents of the device, Knox File Encryption provides an authentication prompt (separate from the device lock screen). In this configuration all files stored on the device will be encrypted.

The Master Key (MKDD) is protected by a Trusted App inside TrustZone by the user's password. Each encrypted file is protected by a uniquely generated FEK which is encrypted by the Master Key as a KEK. The administrator can specify a period of inactivity after which the Master Key and all FEKs are wiped from memory to fully lock the encrypted files.

3.2 TOE Evaluated Platforms

Details regarding the evaluated configuration is provided in Section 8 of this document.

3.3 TOE Architecture

The TOE is software built into Samsung Knox. The TOE is designed as a framework for providing file encryption for files on the device. The software is comprised of four major components: the DualDAR Service, the DualDAR Client, the DualDAR Driver and cryptographic modules. Management of the TOE is provided through normal device administration functions; the TOE does not provide any configuration or management capabilities itself but relies on the platform to provide a User Interface (UI) (such as for password entry or management) and Mobile Device Management (MDM) control. Administration is limited to enabling the File Encryption feature.

The boundary of files being encrypted is called the File Encryption Boundary (FEB). Once the FEB has been set, by creating a File Encryption-enabled work profile, the service for encrypting/decrypting files is the same. The specific version listed for DualDAR denotes the FEB that can be set.

The components provide the following functions within the TOE:

- DualDAR Service: manages the implementation of the configuration and monitoring system status for the lock state
- DualDAR Client: handles access to the Master Key (unlock and wipe)
- DualDAR Driver: handles the encryption/decryption I/O of files with the Master Key unlocked by the DualDAR Client
- Cryptographic Modules: handle the cryptographic operations of the TOE (Samsung Kernel Cryptographic Module and Samsung SCrypto)

Depending on the FEB configuration, the TOE either utilizes the Knox work profile authentication or provides its own authentication to unlock the 256-bit Master Key. Once the Master Key is unlocked the DualDAR Driver can read an encrypted file to unlock the individual 256-bit FEK. The unlocked FEK is then used to decrypt the contents. When using a Knox work profile, all open files will be closed and all unlocked FEKs and the Master Key will be cleared from memory (this is handled by the DualDAR Service) when the profile becomes locked. When not using a Knox work profile, the administrator can specify an inactivity period to force a device restart to close all open files and clear all FEKs and the Master Key.

By default (and in this configuration), the DualDAR Driver utilizes the Samsung Kernel Cryptographic Module of the device for AES-CBC-256 to decrypt/encrypt the contents of the file. The FEK is encrypted with AES-GCM using the 256-bit Master Key. All keys are generated using platform-provided Deterministic Random Bit Generator (DRBG) functions and are 256-bit.

The TOE does not provide or utilize any communications services, nor does the TOE transmit or receive data or keys from remote systems.

Samsung provides a Software Development Kit (SDK) which can be used to integrate a third-party encryption library to be used by the DualDAR Service and Driver but this configuration is not included as part of this evaluation.

3.4 Physical Boundaries

The TOE is a software application running on a mobile device. The mobile device platform provides a host Operating System and a Trusted Execution Environment.

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 TOE runs as part of Samsung Android 14 with Knox 3.10 and includes several cryptographic libraries for encryption/decryption/cryptographic hashing functions for securing file contents and TOE keys.

4.2 User data protection

Depending on the FEB configuration, the TOE either protects all user data within the Knox work profile or the entire device by providing an automatic encryption service for all stored files; applications do not have to be made aware of the Knox File Encryption service to be protected. All keys are AES 256-bit, using AES-GCM for FEK protection and AES-CBC for file content protection.

4.3 Identification and authentication

Depending on the FEB configuration, the TOE either utilizes the authentication services provided by the Knox work profile or its own authentication dialog to unlock the Master Key. Unsuccessful authentication will prevent the Master Key from being unlocked, and hence no encrypted files can be accessed.

4.4 Security management

The services provided by the TOE are not available until Knox File Encryption has been enabled. Authentication management and the work profile lock settings are handled by the Knox work profile management and are generic for all Knox work profile configurations. When the whole device is configured for encryption authentication settings are handled by a combination of the device authentication settings and additional Knox File Encryption settings. In either case, these settings cannot be managed directly on the device but must be configured from the MDM.

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 Samsung Android operating system for the protection of the TOE's components.

The TOE relies on the Samsung Android operating system to provide updates as the software is incorporated as part of the device image. The version of the Knox File Encryption software can be seen in the *About Device* page of the mobile device with the *Knox version* information (as the DualDAR version).

The TOE is a Samsung component, and all code is maintained solely by Samsung. Only documented APIs available in Samsung Android (which includes the Knox work profile and Samsung cryptographic libraries) are used.

4.7 Trusted path/channels

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

5 Assumptions & Clarification of Scope

Assumptions

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

- Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)
- PP-Module for File Encryption, Version 1.0, 25 July 2019 (FE10)

That information has not been reproduced here and the ASPP14/FE10 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 ASPP14/FE10 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.

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 the File Encryption Module 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.
- Apart from the Admin Guide, additional customer documentation for the specific File Encryption Application models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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 ASPP14/FE10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Samsung File Encryption 1.6.0 Administrator Guide, Version 1.6, November 13, 2024

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 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 guide from the NIAP website to ensure the device is configured 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 proprietary Detailed Test Report for Samsung Knox File Encryption, Version 0.2, November 13, 2024 (DTR), as summarized in Section 3.4 of the Assurance Activity Report (AAR).

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 to a Common Criteria Certification document and ran the tests specified in the ASPP14/FE10 including the tests associated with optional requirements. A list of the tested devices is provided in Section 1.2 of the AAR, and a diagram of the test environment with a list of test tools is provided in Section 3.4.

8 Evaluated Configuration

The following table shows the model numbers of the mobile devices tested during the evaluation of Knox File Encryption 1.6.0 (the version is listed as "DualDAR"):

Device Name	Chipset Vendor	SoC	Arch	Kernel	DualDAR Version	Build Number
Galaxy Z Flip6 5G	Qualcomm	Snapdragon 8 Gen 3	ARMv8	6.1	1.6.0	UP1A.231005.007
Galaxy S24 FE	Samsung	Exynos 2400	ARMv8	6.1	1.6.0	UP1A.231005.007

Evaluated Devices

In addition to the evaluated devices, the following device models are claimed as equivalent with a note about the differences between the evaluated device and the equivalent models.

Evaluated Device	SoC	Equivalent Devices	Differences
Galaxy Z Flip6 5G	Snapdragon 8 Gen 3	Galaxy Z Fold6 5G Galaxy Z Fold A	Z Fold6 > Z Flip6 in terms of display size
Galaxy S24 FE	Exynos 2400	N/A	

9 Results of the Evaluation

The results of performing 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 Knox File Encryption TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/FE10.

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 Knox File Encryption 1.6.0 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.

9.2 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 ASPP14/FE10 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 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 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 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the ASPP14/FE10 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.

9.6 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 vulnerability analysis includes a public search for vulnerabilities. The search was performed on November 13, 2024, and a summary is included in Section 3.5 of the AAR. The public search for vulnerabilities did not uncover any residual vulnerability.

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: “Galaxy S24”, “SM-S721”, “Galaxy Z Flip6”, “SM-F741”, “Galaxy Z Fold6”, “SM-F956”, “SM-F958”, “Knox”, “BoringSSL”, “DualDAR”, “containercore”, “Android”, “Exynos”, “Qualcomm Snapdragon”.

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 TOE is an application that functions as a component of a mobile device and is an early participant in NIAP's SBOM evaluation requirement. The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the guidance document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed in other sections of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.6.0 - Fall Security Target, Version 0.3, November 13, 2024*.

13 **Glossary**

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 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 1.4, October 7, 2021 (ASPP14).

[5] PP-Module for File Encryption, Version 1.0, July 25, 2019 (FE10).

[6] Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.6.0 - Fall Security Target, Version 0.3, November 13, 2024 (ST).

[7] Assurance Activity Report for Samsung Knox File Encryption 1.6.0, Version 0.2, November 13, 2024 (AAR).

[8] Detailed Test Report for Samsung Knox File Encryption 1.6.0, Version 0.2, November 13, 2024 (DTR).

[9] Evaluation Technical Report for Samsung Knox File Encryption, Version 0.2, November 13, 2024 (ETR).