Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.5 – Fall Security Target

Version: 0.3
10/19/2023

Prepared for:

Samsung Electronics Co., Ltd.

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

Prepared By:

www.gossamersec.com

Table of Contents

List of Tables

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE consists of the Samsung Knox File Encryption 1.5 - Fall provided by Samsung Electronics Co., Ltd.. The TOE is being evaluated as a File Encryption application.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Acronyms and Terminology

AA	Assurance Activity
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
EAR	Entropy Analysis Report
FEB	File Encryption Boundary
FEK	File Encryption Key
GUI	Graphical User Interface
KEK	Key Encryption Key
MDM	Mobile Device Management
MKDD	Master Key DualDAR
PCL	Product Compliant List
PMKEK	Password-based Master Key Encryption Key
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TEE	Trusted Execution Environment (TrustZone)
TOE	Target of Evaluation
U.S.	United States
VR	Validation Report

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example, FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement. In other cases, copied from the Protection Profile or Module, a /NAME is added after a requirement to indicate iteration. For example, FCS_COP.1/SKC.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… all objects …" or "… some big things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.5 – Fall Security Target

ST Version – Version 0.3

ST Date – 10/19/2023

KMD Title – Samsung Electronics Co., Ltd. Samsung Knox File Encryption 1.5 Fall Key Management Description

KMD Version – Version 0.3

KMD Date – 10/19/2023

1.2 TOE Reference

TOE Identification – Samsung Knox File Encryption 1.5- Fall

TOE Developer – Samsung Electronics Co., Ltd.

Evaluation Sponsor – Samsung Electronics Co., Ltd.

1.3 TOE Overview

The Target of Evaluation (TOE) is Samsung Knox File Encryption 1.5. 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 13 and Knox 3.9.

1.4 TOE Description

The TOE is a software service built into Samsung Android 13 with Knox 3.9 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 in a Knox work profile and the entire device except for Galaxy Tab Active 3 device which encrypts only in a Knox work profile. 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.

The following table shows the model numbers of the mobile devices used during evaluation testing of Knox File Encryption 1.5+ (the version is listed as "DualDAR"):

Device Name	Model Number	Chipset Vendor	CPU	Android Version	TEE OS	Knox Version	DualDAR Version
Galaxy Z Flip5 5G	SM-F731	Qualcomm	Snapdragon 8 Gen 2 Mobile Platform	13	QSEE 5.24	3.9	1.5.1
Galaxy XCover6 Pro	SM-G736	Qualcomm	Snapdragon 778G	13	QSEE 5.11	3.9	1.5.1
Galaxy Tab Active3	SM- T575	Samsung	Exynos 9810	13	QSEE 4.1	3.9	1.5.0
Galaxy S23 FE	SM-S711	Samsung	Exynos 2200	13	TEEGRIS 5.24	3.9	1.5.1
Galaxy S23 FE	SM-S711	Qualcomm	Snapdragon 8 Gen 1	13	QSEE 5.16	3.9	1.5.1

Table 1 - 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	CPU	Equivalent Devices	Differences
Galaxy Z Flip5 5G	Snapdragon 8 Gen 2 Mobile Platform	Galaxy Z Fold5 5G Galaxy Tab S9 Ultra Galaxy Tab S9+ Galaxy Tab S9	All devices have same software environments (Android, Kernel, TEE)
Galaxy XCover6 Pro	Snapdragon 778G (SM7325)	Galaxy Tab Active4 Pro	All devices have same software environments (Android, Kernel, TEE)
Galaxy Tab Active3	Exynos 9810	N/A	N/A
Galaxy S23 FE	Exynos 2200	N/A	N/A
Galaxy S23 FE	Snapdragon 8 Gen 1	N/A	N/A

Table 2 - Equivalent Devices

1.4.1 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 both UI (such as for password entry or management and 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, the service for encrypting/decrypting files is the same. The specific version listed for DualDAR denotes the FEB that can be set. Setting the FEB for the whole device requires v1.5.1, while either version can set the FEB to the work profile.

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 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 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.

1.4.1.1 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.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the Samsung Knox File Encryption:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

1.4.1.2.1 Cryptographic Support

The TOE runs as part of Samsung Android 13 with Knox 3.9 and includes several cryptographic libraries for encryption/decryption/cryptographic hashing functions for securing file contents and TOE keys.

1.4.1.2.2 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.

1.4.1.2.3 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.

1.4.1.2.4 Security Management

The services provided by the TOE are not available until either a 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.

1.4.1.2.5 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.

1.4.1.2.6 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 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.

1.4.1.2.7 Trusted Path/Channels

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

1.4.2 TOE Documentation

- Samsung Knox File Encryption 1.5 Administrator Guide, version 1.5, October 19, 2023

2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Extended
- PP-Configuration for Application Software and File Encryption, Version 1.1, 7 April 2022 (CFG_APP-FE_V1.1)
  - The PP-Configuration includes the following components:
    - Base-PP: Protection Profile for Application Software, Version 1.4 (PP_APP_V1.4)
    - PP-Module: PP-Module for File Encryption, Version 1.0 (MOD_FE_V1.0)
- Technical Decisions as of June 23, 2023:

TD No.	PP	Applied	Rationale
0455	MOD_FE_V1.0	Yes	
0472	MOD_FE_V1.0	Yes	
0600	MOD_FE_V1.0	No	Not claiming VPNC
0628	PP_APP_V1.4	Yes	
0644	MOD_FE_V1.0	Yes	
0650	PP_APP_V1.4/ MOD_FE_V1.0	No	Not claiming VPNC
0664	PP_APP_V1.4	No	SFR not claimed
0717	PP_APP_V1.4	Yes	
0719	PP_APP_V1.4	Yes	
0736	PP_APP_V1.4	No	SFR not claimed
0743	PP_APP_V1.4	Yes	
0747	PP_APP_V1.4	Yes	
0756	PP_APP_V1.4	Yes	
0780	PP_APP_V1.4	No	SFR not claimed

Table 3 - Technical Decisions

2.1 Conformance Rationale

The ST conforms to the CFG_APP-FE_V1.1. As explained previously, the security problem definition, security objectives, and security requirements are defined in the PP_APP_V1.4/MOD_FE_V1.0 that make up the CFG_APP-FE_V1.1.

3 Security Objectives

The Security Problem Definition may be found in the PP_APP_V1.4/MOD_FE_V1.0 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The PP_APP_V1.4/MOD_FE_V1.0 offers additional information about the identified security objectives, but that has not been reproduced here and the PP_APP_V1.4/MOD_FE_V1.0 should be consulted if there is interest in that material.

In general, the PP_APP_V1.4/MOD_FE_V1.0 has defined Security Objectives appropriate for Mobile Devices and as such are applicable to the Samsung Knox File Encryption TOE.

3.1 Security Objectives for the Operational Environment

- **OE.AUTHORIZATION_FACTOR_STRENGTH** (MOD_FE_V1.0) An authorized user will be responsible for ensuring that all externally derived authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected. This can apply to password or passphrase based, ECC CDH, and RSA authorization factors.
- **OE.PLATFORM** (PP_APP_V1.4) The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
- **OE.POWER_SAVE** (MOD_FE_V1.0) The non-mobile operational environment must be configurable so that there exists at least one mechanism that will cause the system to enter a safe power state (A.SHUTDOWN). Any such mechanism (e.g., sleep, hibernate) that does not conform to this requirement must be capable of being disabled. The mobile operational environment must be configurable such that there exists at least one mechanism that will cause the system to lock upon a period of time.
- **OE.PROPER_USER** (PP_APP_V1.4) The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
- **OE.PROPER_ADMIN** (PP_APP_V1.4) The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
- **OE.STRONG_ENVIRONMENT_ CRYPTO** (MOD_FE_V1.0) The Operating environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE.

4 Extended Components Definition

All of the extended requirements in this ST have been drawn from the PP_APP_V1.4/MOD_FE_V1.0. The PP_APP_V1.4/MOD_FE_V1.0 defines the following extended SFRs and SARs and since they are not redefined in this ST the PP_APP_V1.4/MOD_FE_V1.0 should be consulted for more information concerning those CC extensions.

Requirement Class	Requirement Component
FCS: Cryptographic support	PP_APP_V1.4: FCS_CKM.1.1/SK :Cryptographic Key Generation
	PP_APP_V1.4: FCS_CKM_EXT.1/PBKDF: Password Conditioning
	MOD_FE_V1.0: FCS_CKM_EXT.2: Cryptographic key generation (FEK)
	MOD_FE_V1.0: FCS_CKM_EXT.3: Key Encrypting Key (KEK) Support
	MOD_FE_V1.0: FCS_CKM_EXT.4: Cryptographic Key Destruction
	MOD_FE_V1.0: FCS_CKM_EXT.6: Cryptographic Password/Passphrase Conditioning
	MOD_FE_V1.0: FCS_IV_EXT.1: Initialization Vector Generation
	MOD_FE_V1.0: FCS_KDF_EXT.1 Cryptographic Key Derivation Function
	MOD_FE_V1.0: FCS_KYC_EXT.1: Key Chaining and Key Storage
	PP_APP_V1.4: FCS_RBG_EXT.1: Random Bit Generation Services
	PP_APP_V1.4: FCS_STO_EXT.1(1): Storage of Credentials
	PP_APP_V1.4: FCS_STO_EXT.1(2): Storage of Credentials
	MOD_FE_V1.0: FCS_VAL_EXT.1: Validation
FDP: User data protection	PP_APP_V1.4: FDP_DAR_EXT.1: Encryption of Sensitive Application Data
	PP_APP_V1.4: FDP_DEC_EXT.1: Access to Platform Resources
	PP_APP_V1.4: FDP_NET_EXT.1: Network Communications
	MOD_FE_V1.0: FDP_PM_EXT.1: Protection of Data in Power Managed States
	MOD_FE_V1.0: FDP_PRT_EXT.1: Protection of Selected User Data
	MOD_FE_V1.0: FDP_PRT_EXT.2: Destruction of Plaintext Data
	MOD_FE_V1.0: FDP_PRT_EXT.3: Protection of Third-Party Data
FIA: Identification and authentication	MOD_FE_V1.0: FIA_AUT_EXT.1: User Authorization
FMT: Security management	PP_APP_V1.4: FMT_CFG_EXT.1: Secure by Default Configuration
	PP_APP_V1.4: FMT_MEC_EXT.1: Supported Configuration Mechanism
FPR: Privacy	PP_APP_V1.4: FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	PP_APP_V1.4: FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	PP_APP_V1.4: FPT_API_EXT.1: Use of Supported Services and APIs
	PP_APP_V1.4: FPT_IDV_EXT.1: Software Identification and Versions
	MOD_FE_V1.0: FPT_KYP_EXT.1: Protection of Key and Key Material
	PP_APP_V1.4: FPT_LIB_EXT.1: Use of Third Party Libraries
	PP_APP_V1.4: FPT_TUD_EXT.1: Integrity for Installation and Update
FTP: Trusted Path/Channels	PP_APP_V1.4: FTP_DIT_EXT.1: Protection of Data in Transit
ALC: Life Cycle Support	PP_APP_V1.4: ALC_TSU_EXT.1: Timely Security Updates

Table 4 - Extended SFRs and SARs

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the PP_APP_V1.4/MOD_FE_V1.0. The refinements and operations already performed in the PP_APP_V1.4/MOD_FE_V1.0 are not identified (e.g., highlighted) here, rather the requirements have been copied from the PP_APP_V1.4/MOD_FE_V1.0 and any residual operations have been completed herein. Of particular note, the PP_APP_V1.4/MOD_FE_V1.0 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the PP_APP_V1.4/MOD_FE_V1.0, which include all the SARs for Part 3 with ALC_TSU_EXT.1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the PP_APP_V1.4/MOD_FE_V1.0 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the assurance requirements alone. The PP_APP_V1.4/MOD_FE_V1.0 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Samsung Knox File Encryption TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	PP_APP_V1.4: FCS_CKM.1.1/SK :Cryptographic Key Generation
	PP_APP_V1.4: FCS_CKM_EXT.1/PBKDF: Password Conditioning
	PP_APP_V1.4: FCS_CKM_EXT.1:Cryptographic Key Generation Services
	MOD_FE_V1.0: FCS_CKM_EXT.2: Cryptographic key generation (FEK)
	MOD_FE_V1.0: FCS_CKM_EXT.3: Key Encrypting Key (KEK) Support
	MOD_FE_V1.0: FCS_CKM_EXT.4: Cryptographic Key Destruction
	MOD_FE_V1.0: FCS_CKM_EXT.6: Cryptographic Password/Passphrase Conditioning
	PP_APP_V1.4: FCS_COP.1/SKC: Cryptographic Operation – Encryption/Decryption
	PP_APP_V1.4:FCS_COP.1/KeyedHash :Cryptographic Operation - Keyed-Hash Message Authentication
	MOD_FE_V1.0: FCS_COP.1(5): Cryptographic Operation (Key Wrapping)
	MOD_FE_V1.0: FCS_IV_EXT.1: Initialization Vector Generation
	MOD_FE_V1.0: FCS_KDF_EXT.1: Cryptographic Key Derivation Function
	MOD_FE_V1.0: FCS_KYC_EXT.1: Key Chaining and Key Storage
	PP_APP_V1.4: FCS_RBG_EXT.1: Random Bit Generation Services
	PP_APP_V1.4: FCS_STO_EXT.1(1): Storage of Credentials
	PP_APP_V1.4: FCS_STO_EXT.1(2): Storage of Credentials
	MOD_FE_V1.0: FCS_VAL_EXT.1: Validation
FDP: User data protection	PP_APP_V1.4: FDP_DAR_EXT.1: Encryption of Sensitive Application Data

Requirement Class	Requirement Component
	PP_APP_V1.4: FDP_DEC_EXT.1: Access to Platform Resources
	PP_APP_V1.4: FDP_NET_EXT.1: Network Communications
	MOD_FE_V1.0: FDP_PM_EXT.1: Protection of Data in Power Managed States
	MOD_FE_V1.0: FDP_PRT_EXT.1: Protection of Selected User Data
	MOD_FE_V1.0: FDP_PRT_EXT.2: Destruction of Plaintext Data
	MOD_FE_V1.0: FDP_PRT_EXT.3: Protection of Third-Party Data
FIA: Identification and authentication	MOD_FE_V1.0: FIA_AUT_EXT.1: User Authorization
FMT: Security management	PP_APP_V1.4: FMT_CFG_EXT.1: Secure by Default Configuration
	PP_APP_V1.4: FMT_MEC_EXT.1: Supported Configuration Mechanism
	PP_APP_V1.4: FMT_SMF.1: Specification of Management Functions
	MOD_FE_V1.0: FMT_SMF.1(2): Specification of Management Functions
FPR: Privacy	PP_APP_V1.4: FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	PP_APP_V1.4: FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	PP_APP_V1.4: FPT_API_EXT.1: Use of Supported Services and APIs
	PP_APP_V1.4: FPT_IDV_EXT.1: Software Identification and Versions
	MOD_FE_V1.0: FPT_KYP_EXT.1: Protection of Key and Key Material
	PP_APP_V1.4: FPT_LIB_EXT.1: Use of Third Party Libraries
	PP_APP_V1.4: FPT_TUD_EXT.1: Integrity for Installation and Update
FTP: Trusted Path/Channels	PP_APP_V1.4: FTP_DIT_EXT.1: Protection of Data in Transit

Table 5 – TOE Security Functional Requirements

5.1.1 Cryptographic Support (FCS)

5.1.1.1 PP_APP_V1.4: FCS_CKM.1/SK: Cryptographic Symmetric Key Generation

FCS_CKM.1.1/SK

The **application** shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1** and specified cryptographic key sizes [

- ***256 bit***

].

5.1.1.2 PP_APP_V1.4: FCS_CKM.1/PBKDF: Password Conditioning

FCS_CKM_EXT.1.1/PBKDF

A password/passphrase shall perform [**Password-based Key Derivation Function**] in accordance with a specified cryptographic algorithm as specified in FCS_COP.1/KeyedHash, with [**100,000**] iterations, and output cryptographic key sizes [***256***] that meet the following **[NIST SP 800-132]**.

FCS_CKM_EXT.1.2/PBKDF

The TSF shall generate salts using a RBG that meets FCS_RGB_EXT.1 and with entropy corresponding to the security strength selected for PBKDF in

FCS_CKM.1.1/PBKDF.

5.1.1.3 PP_APP_V1.4: FCS_CKM_EXT.1.:Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [

- ***generate no asymmetric cryptographic keys***

].

5.1.1.4 MOD_FE_V1.0: FCS_CKM_EXT.2: Cryptographic key generation (FEK)

FCS_CKM_EXT.2.1

The TSF shall [

- ***generate FEK cryptographic keys [***
  - ***using a Random Bit Generator as specified in FCS_RBG_EXT.1 (from [AppPP]) and with entropy corresponding to the security strength of AES key sizes of [256 bit]***

  ]

].

FCS_CKM_EXT.2.2

The TSF shall use a unique FEK for each file (or set of files) using the mechanism on the client as specified in FCS_CKM_EXT.2.1.

5.1.1.5 MOD_FE_V1.0: FCS_CKM_EXT.3: Key Encrypted Key (KEK) Support

FCS_CKM_EXT.3.1

The TSF shall [

- ***generate KEK cryptographic keys [***
  - ***using a Random Bit Generator as specified in FCS_RBG_EXT.1 (from [AppPP]) and with entropy corresponding to the security strength of AES key sizes of [256 bit]***
  - ***derived from a password/passphrase that is conditioned as defined in FCS_CKM_EXT.6]***

].

5.1.1.6 MOD_FE_V1.0: FCS_CKM_EXT.4: Cryptographic Key Destruction

FCS_CKM_EXT.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For volatile memory, the destruction shall be executed by a [***
  - ***single overwrite consisting of [zeroes]];***
- ***For non-volatile memory, the destruction shall be executed by [***
  - ***the invocation of an interface provided by the underlying platform that [***
    - ***instructs the underlying platform to destroy the abstraction that represents the key]***

].

FCS_CKM_EXT.4.2

The TSF shall destroy all keys and key material when no longer needed.

5.1.1.7 MOD_FE_V1.0: FCS_CKM_EXT.6: Cryptographic Password/Passphrase Conditioning

FCS_CKM_EXT.6.1

The TSF shall support a password/passphrase of up to [***maximum value supported by the platform: 256***] characters used to generate a password authorization factor.

FCS_CKM_EXT.6.2

The TSF shall allow passwords to be composed of any combination of upper case characters, lower case characters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”, and [***+ = _ / - ' " : ; , ? ` ~ \ | < > { } [ ]***].

FCS_CKM_EXT.6.3

The TSF shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [**HMAC-**[***SHA-256***]], with [**100,000**] iterations, and output cryptographic key sizes [***256***] that meet the following: [*NIST SP 800-132*].

FCS_CKM_EXT.6.4

The TSF shall not accept passwords less than [***4 characters***] and greater than the maximum password length defined in FCS_CKM_EXT.6.1.

FCS_CKM_EXT.6.5

The TSF shall generate all salts using an RBG that meets FCS_RBG_EXT.1 (**from [AppPP]**) and with entropy corresponding to the security strength selected for PBKDF in FCS_CKM_EXT.6.3

5.1.1.8 PP_APP_V1.4: FCS_COP.1/SKC(: Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC

The **application** shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm [

- ***AES-CBC (as defined in NIST SP 800-38A) mode,***
- ***AES-GCM (as defined in NIST SP 800-38D) mode,***

] and cryptographic key sizes [

- ***256 bit***

].

5.1.1.9 PP_APP_V1.4:FCS_COP.1/KeyedHash Cryptographic Operation - Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash

The **application** shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm

- [***HMAC-SHA-256***]

and [

- ***no other algorithms***

] with key sizes [**256-bits**] and message digest sizes [***256***] and [***no other size***] bits that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

5.1.1.10 MOD_FE_V1.0: FCS_COP.1(5): Cryptographic Operation (Key Wrapping)

FCS_COP.1.1(5)

The TSF shall [***implement functionality to perform Key Wrapping***] in accordance with a specified cryptographic algorithm [*AES*] **in the following modes** [

- ***GCM mode***

] and the cryptographic key size [***256 bits (AES)***] that meet the following: [

- ***"NIST SP 800-38D"***

] **and no other standards**.

5.1.1.11 MOD_FE_V1.0: FCS_IV_EXT.1: Initialization Vector Generation

FCS_IV_EXT.1.1

The TSF shall [

- ***invoke platform-provided functionality to generate IVs***

].

5.1.1.12 MOD_FE_V1.0: FCS_KDF_EXT.1: Cryptographic Key Derivation Function

FCS_KDF_EXT.1.1

The TSF shall [*accept* [***a conditioned password***] to derive an intermediate key, as defined in [

- ***NIST SP 800-132***

] using the keyed-hash functions specified in FCS_COP.1(4)[1] *(**from [AppPP]**), such that the output is at least of equivalent security strength (in number of bits) to the [FEK]*].

5.1.1.13 MOD_FE_V1.0: FCS_KYC_EXT.1: Key Chaining and Key Storage

FCS_KYC_EXT.1.1

The TSF shall maintain a key chain of [

- ***[KEKs] originating from [one or more authorization factors(s)] to [the FEK(s)] using the following method(s): [***
  - ***implementation of key wrapping as specified in FCS_COP.1(5),***
  - ***implementation of key derivation as specified in FCS_KDF_EXT.1***

  ] while maintaining an effective strength of [
  - ***[256 bits] for symmetric keys;***

  ] commensurate with the strength of the FEK]

and [

- ***no supplemental key chains]***

].

[1] Note that the Application Software PP has renamed this requirement FCS_COP.1/KeyedHash

5.1.1.14 PP_APP_V1.4: FCS_RBG_EXT.1: Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [

- ***invoke platform-provided DRBG functionality***

] for its cryptographic operations.

5.1.1.15 PP_APP_V1.4: FCS_STO_EXT.1(1): Storage of Credentials

FCS_STO_EXT.1.1(1)

The application shall [

- ***implement functionality to securely store [MKDD and FEKs] according to [FCS_COP.1/SKC]***

] to non-volatile memory.

5.1.1.16 PP_APP_V1.4: FCS_STO_EXT.1(2): Storage of Credentials

FCS_STO_EXT.1.1(2)

The application shall [

- ***implement functionality to securely store [PMKEK] according to [FCS_CKM.1/PBKDF]***

] to non-volatile memory.

5.1.1.17 MOD_FE_V1.0: FCS_VAL_EXT.1 Validation

FCS_VAL_EXT.1.1

The TSF shall perform validation of the [*user*] by [

- ***receiving assertion of the subject's validity from [Knox work profile]***

].

FCS_VAL_EXT.1.2

The TSF shall require validation of the [*user*] prior to [*decrypting any FEK*].

5.1.2 User Data Protection (FDP)

5.1.2.1 PP_APP_V1.4: FDP_DAR_EXT.1: Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [

- ***implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption;***
- ***protect sensitive data in accordance with FCS_STO_EXT.1***

] in non-volatile memory.

(TD0582 applied)

5.1.2.2 PP_APP_V1.4: FDP_DEC_EXT.1: Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [

- ***no hardware resources***

].

FDP_DEC_EXT.1.2

The application shall restrict its access to [

- ***no sensitive information repositories***

].

5.1.2.3 PP_APP_V1.4: FDP_NET_EXT.1: Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- ***no network communications***

].

5.1.2.4 MOD_FE_V1.0: FDP_PM_EXT.1: Protection of Data in Power Managed States

FDP_PM_EXT.1.1

The TSF shall protect all data selected for encryption during the transition to the [**Data Locked**] state as per FDP_PRT_EXT.1.1.

FDP_PM_EXT.1.2

On the return to a powered-on state from the state(s) indicated in FDP_PM_EXT.1.1, the TSF shall authorize the user in the manner specified in FIA_AUT_EXT.1.1 once before any protected data are decrypted.

FDP_PM_EXT.1.3

The TSF shall destroy all key material and authentication factors stored in plaintext when transitioning to a protected state as defined by FDP_PM_EXT.1.1.

5.1.2.5 MOD_FE_V1.0: FDP_PRT_EXT.1: Protection of Selected User Data

FDP_PRT_EXT.1.1

The TSF shall perform encryption and decryption of the user-selected file (or set of files) in accordance with FCS_COP.1(1) (**from [AppPP]**).

FDP_PRT_EXT.1.2

The TSF shall [***implement functionality***] to ensure that all sensitive data created by the TOE when decrypting/encrypting the user-selected file (or set of files) are destroyed in volatile and non-volatile memory when the data is no longer needed according to FCS_CKM_EXT.4.

5.1.2.6 MOD_FE_V1.0: FDP_PRT_EXT.2: Destruction of Plaintext Data

FDP_PRT_EXT.2.1

The TSF shall [***implement functionality***] to ensure that all original plaintext data created when decrypting/encrypting the user-selected file (or set of files) are destroyed in volatile and non-volatile memory according to FCS_CKM_EXT.4 upon completion of the decryption/encryption operation.

5.1.2.7 MOD_FE_V1.0: FDP_PRT_EXT.3: Protection of Third-Party Data

FDP_PRT_EXT.3.1

The TSF shall ensure that all temporary files created by [***all applications***] when decrypting/encrypting the user-selected file (or set of files) are removed or encrypted upon completion of the decryption/encryption operation.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 MOD_FE_V1.0: FIA_AUT_EXT.1: User Authorization

FIA_AUT_EXT.1.1

The TSF shall [***implement platform-provided functionality to provide user authorization, provide user authorization***] based on [

- ***a password authorization factor conditioned as defined in FCS_CKM_EXT.6***

].

5.1.4 Security Management (FMT)

5.1.4.1 PP_APP_V1.4: FMT_CFG_EXT.1: Secure by Default Configuration

FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

5.1.4.2 PP_APP_V1.4: FMT_MEC_EXT.1: Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***].

(TD0437 applied)

5.1.4.3 PP_APP_V1.4: FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- ***For all configurations***
  - ***specify a time period after device lock to enter the Data Lock state***
- ***For whole device configurations***
  - ***specify the minimum password length***
  - ***specify an administrator reset token***

].

5.1.4.4 MOD_FE_V1.0: FMT_SMF.1(2): Specification of Management Functions

FMT_SMF.1.1(2)

The TSF shall be capable of performing the following management functions: [

- ***perform a cryptographic erase of the data by the destruction of FEKs or KEKs protecting the FEKs as described in FCS_CKM_EXT.4.1,***

].

5.1.5 Privacy (FPR)

5.1.5.1 PP_APP_V1.4: FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

The application shall [

- ***not transmit PII over a network***

].

5.1.6 Protection of the TSF (FPT)

5.1.6.1 PP_APP_V1.4: FPT_AEX_EXT.1: Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [**no exceptions**].

FPT_AEX_EXT.1.2

The application shall [

- ***not allocate any memory region with both write and execute permissions***

].

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

5.1.6.2 PP_APP_V1.4: FPT_API_EXT.1: Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

5.1.6.3 PP_APP_V1.4: FPT_IDV_EXT.1: Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [***[an identifier in the Knox version display]***].

5.1.6.4 MOD_FE_V1.0: FPT_KYP_EXT.1: Protection of Key and Key Material

FPT_KYP_EXT.1.1

The TSF shall [

- ***store keys in non-volatile memory only when [***
  - ***wrapped, as specified in FCS_COP.1(5)]***

].

5.1.6.5 PP_APP_V1.4: FPT_LIB_EXT.1: Use of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [**no third party libraries**].

5.1.6.6 PP_APP_V1.4: FPT_TUD_EXT.1: Integrity for Installation and Update

FPT_TUD_EXT.1.1

The application shall [***leverage the platform***] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2

The application shall [***leverage the platform***] to query the current version of the application software.

FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4

Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5

The application is distributed [***with the platform OS***].

(TD0561 applied)

5.1.7 Trusted Path/Channels (FTP)

5.1.7.1 PP_APP_V1.4: FTP_DIT_EXT.1: Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [

- ***not transmit any [data]***

] between itself and another trusted IT product.

5.2 TOE Security Assurance Requirements

The SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

5.2.1 Development (ADV)

5.2.1.1 ADV_FSP.1: Basic Functional Specification

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance Documents (AGD)

5.2.2.1 AGD_OPE.1: Operational User Guidance

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 AGD_PRE.1: Preparative Procedures

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle Support (ALC)

5.2.3.1 ALC_CMC.1: Labelling of the TOE

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 ALC_CMS.1: TOE CM Coverage

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 PP_APP_V1.4: ALC_TSU_EXT.1: Timely Security Updates

ALC_TSU_EXT.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE.

ALC_TSU_EXT.1.2d

The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

ALC_TSU_EXT.1.1c

The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.2c

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.3c

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

ALC_TSU_EXT.1.4c

The description shall include where users can seek information about the availability of new updates including details (e.g. CVE identifiers) of the specific public vulnerabilities corrected by each update.

ALC_TSU_EXT.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 ATE_IND.1: Independent Testing - sample

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability Assessment (AVA)

5.2.5.1 AVA_VAN.1: Vulnerability Survey

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6 TOE Summary Specification

This chapter describes the security functions:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

6.1 Cryptographic Support

PP_APP_V1.4: FCS_CKM.1.1/SK
The TOE generates 256-bit symmetric keys using platform-provided cryptographic modules as described by FCS_RBG_EXT.1. The platform entropy pools are seeded continually from the hardware noise source to ensure sufficient entropy is available for the generation of keys.

PP_APP_V1.4: FCS_CKM_EXT.1/PBKDF /MOD_FE_V1.0: FCS_KDF_EXT.1
The TOE conditions the user password using a PBKDF2 (using HMAC-SHA-256) function that meets NIST SP 800-132 with 100,000 rounds to generate a 256-bit KEK to protect the Master Key (MKDD). All salts are generated using RBGs as specified in FCS_RBG_EXT.1.

PP_APP_V1.4: FCS_CKM_EXT.1.1
The TOE does not generate or use asymmetric keys.

MOD_FE_V1.0: FCS_CKM_EXT.2
The TOE generates FEKs utilizing the Samsung Kernel Cryptographic Module that is part of the platform. The module provides random strings using SHA-256 HMAC_DRBG, seeded from /dev/random with sufficient entropy to generate keys with 256-bit security strength.

The TOE automatically generates a new FEK every time a new file is created (as all files within the work profile will be encrypted). The FEK is stored (encrypted by the MKDD with AES-GCM) as part of a metadata header attached to the file. No user interaction is required to generate the FEK or to encrypt any file within the work profile.

MOD_FE_V1.0: FCS_CKM_EXT.3
The TOE generates two KEKs. The first KEK is the PMKEK and the second KEK is the MKDD. The PMKEK is derived, via PBKDF2 (HMAC-SHA-256), from the password entered by the user at successful authentication to either the Knox work profile or Knox File Encryption. The MKDD is generated using AES-256 CTR_DRBG from the SCrypto module, seeded by raw output from the hardware noise source (similar to /dev/random inside the TEE) with sufficient entropy to generate keys with 256-bit strength. The key is then encrypted by the PMKEK to be stored in non-volatile memory. Both KEKs are 256-bit.

MOD_FE_V1.0: FCS_CKM_EXT.4 (KMD)
The TOE relies on the platform for destroying cryptographic keys when they are no longer in use. The platform cryptographic modules provide functionality to automatically overwrite (with zeros) of keys

when they are released. For keys stored in Flash the TOE calls the platform to perform a block erase to the flash controller. The TOE only writes encrypted keys to flash storage

MOD_FE_V1.0: FCS_CKM_EXT.6

Depending on the FEB configuration, the TOE either utilizes the platform authentication services of the Knox work profile to access the user password or provides its own authentication dialog. In either case, the passwords follow common requirements. Passwords can be between 4-256 characters in length. The administrator may choose to require any password length within this range. Passwords may be composed of basic Latin characters (upper and lower case, numbers, and the special characters noted in the selection (see section 5.1.1.7)).

The entered password is conditioned with 100,000 rounds of PBKDF2 (using HMAC-SHA-256) to generate a 256-bit KEK. This KEK is used to encrypt the 256-bit MKDD using AES-GCM.

PP_APP_V1.4: FCS_COP.1.1/SKC / FCS_COP.1.1/KeyedHash / FCS_COP.1(5) (KMD)

The TOE performs cryptographic algorithms in accordance with the following NIST standards and has received the following CAVP algorithm certificates.

The evaluated devices utilize the following kernels for the Samsung Kernel Cryptographic Module (Kernel Crypto).

Device	SoC	Kernel Version	Kernel Crypto Version
Galaxy Z Flip5 5G	Qualcomm Snapdragon 8 Gen 2 Mobile Platform	5.15	2.3
Galaxy Tab Active3	Samsung Exynos 9810	4.9	1.9
Galaxy XCover6 Pro	Qualcomm Snapdragon 778G	5.4	2.2
Galaxy S23 FE	Samsung Exynos 2200	5.10	2.2
Galaxy S23 FE	Snapdragon 8 Gen 1	5.10	2.2

Table 6 - Kernel Versions

The Samsung Kernel Cryptographic (“Kernel Crypto”) Module provides the following algorithms used by the TOE.

Algorithm	NIST Standard	SFR Reference	Cert#
AES 256 CBC	FIPS 197, SP 800-38A	FCS_COP.1/SKC	A3242
			A1456, A1455
			5183, 5184
HMAC SHA-256	FIPS 198-1 & 180-4	FCS_COP.1/KeyedHash	A3242
			A1456, A1455
			3439, 3440

Table 7 - Samsung Kernel Cryptographic Algorithms

The evaluated devices utilize the Samsung SCrypto Cryptographic Module for cryptographic operations within the TEE on each device. The following table lists the TEE operating systems for each device.

Device	SoC	TEE OS Version	SCrypto Version
Galaxy Z Flip5 5G	Snapdragon 8 Gen 2 Mobile Platform	QSEE 5.24	2.7
Galaxy S23 FE	Samsung Exynos 2200	TEEGRIS 4.2.1	2.6
Galaxy S23 FE	Snapdragon 8 Gen 1 Mobile Platform	QSEE 5.16	2.6
Galaxy XCover6 Pro	Qualcomm Snapdragon 778G	QSEE 5.11	2.5

Device	SoC	TEE OS Version	SCrypto Version
Galaxy Tab Active3	Samsung Exynos 9810	TEEGRIS 4.0	2.5

Table 8 - TEE Environments

The Samsung SCrypto TEE library provides the following algorithms.

Algorithm	NIST Standard	SFR Reference	Cert#
AES CBC/GCM 256	FIPS 197, SP 800-38A/D	FCS_COP.1/SKC	A3243, A915 A889, C1360

Table 9 - SCrypto TEE Cryptographic Algorithms

The TOE invokes The Samsung Kernel Cryptographic and the SCrypto modules to perform AES-GCM 256-bit encryption of KEKs and FEKs for key wrapping according to SP 800-38D. The file contents are encrypted using AES-CBC from the Samsung Kernel Cryptographic module. All keys used by the TOE are 256-bit. The key sizes and algorithms used cannot be changed.

MOD_FE_V1.0: FCS_IV_EXT.1
The TOE generates unique IVs for AES-CBC used to encrypt data storage (files). The IVs are generated by using the Samsung Kernel Crypto HMAC_DRBG API when the AES FEK for a file is created.

MOD_FE_V1.0: FCS_KYC_EXT.1 (KMD)
The PMKEK, MKDD and all FEKs are 256-bit AES keys. The MKDD is protected by the PMKEK, which is derived from the password using PBKDF2. The encrypted MKDD is stored in TrustZone as part of the DualDAR Client Trusted App data. The MKDD is used to encrypt the FEK of each file in the FEB (the FEK is stored in the associated file metadata). All keys are encrypted with AES-GCM.

PP_APP_V1.4: FCS_RBG_EXT.1 (KMD)
The TOE utilizes a number of different RBGs included in the platform:

1. An AES-256 CTR_DRBG provided by SCrypto in the TEE OS
2. A SHA-256 HMAC_DRBG provided by Kernel Crypto in the Android Linux kernel

Each of these entropy sources will generate a 256-bit string. The APIs used by the TOE are available to applications that are part of the system services (not general Android applications).

PP_APP_V1.4: FCS_STO_EXT.1(1)(2) (KMD)
The TOE uses a TrustZone application to protect the MKDD that is unlocked when the user successfully authenticates. The AES-GCM encrypted key is stored within the TrustZone boundary.

The TOE protects individual FEKs (and IVs) by encrypting them using AES-GCM with the MKDD and placing it in the file metadata.

The PMKEK is conditioned from the password using a PBKDF2 function following NIST SP 800-132.

MOD_FE_V1.0: FCS_VAL_EXT.1
When used with a Knox work profile, the TOE relies on the platform to validate the user credentials via the authentication interface for the Knox work profile. When used to encrypt the entire device, the TOE provides its own authentication interface immediately after the device lock screen. A successful authentication in either case will provide the TOE with access to the entered password to begin the process for accessing the MKDD and hence the protected files.

The MKDD can only be decrypted by the PMKEK, which must be conditioned from the user's authentication credentials. This ensures that the files cannot be accessed without a successful user authentication.

The TOE is a component of the Samsung Knox software package. The TOE is available and can be used only on devices where it is provided from Samsung (i.e. this is not available as a separate application that could be downloaded and installed separately). The operational environments for the TOE are listed as part of Table 1 - Evaluated Devices in the columns: Android Version, TEE OS and Knox Version.

6.2 User Data Protection

PP_APP_V1.4: FDP_DAR_EXT.1 (KMD)
The TOE leverages the platform TrustZone for protection of the MKDD. The TOE includes a Trusted App which leverages an encryption module within TrustZone to encrypt (and decrypt) the MKDD.

To encrypt files, the TOE implements a service which will intercept file requests to encrypt (and decrypt) the files using the included cryptographic modules. All files written inside the Knox work profile boundary, including user data, temporary files or any other type of file created by an application, are considered sensitive data and will be encrypted. When used to encrypt the entire device, all files except a small number of system apps (needed for the device to function properly and specified by Samsung) are encrypted. All other files are automatically considered sensitive data and will be encrypted.

PP_APP_V1.4: FDP_DEC_EXT.1
The TOE is bundled as part of the application package for Knox. This package is bundled as part of the device image and is only updated as part of OS updates. The Knox application is installed automatically as a system service on the first boot. The TOE is only available when specifically activated, and then only intercepts read/write requests for any files within the FEB. The TOE does not access any sensitive information repositories, but will encrypt/decrypt any application and data stored within the defined encryption boundary since it interacts at the file system level (below the concept of whether an application is sensitive or not).

PP_APP_V1.4: FDP_NET_EXT.1
The TOE does not transmit any information over a network.

MOD_FE_V1.0: FDP_PM_EXT.1
The TOE supports three discrete states on the device:

1. Off: the device is powered off (i.e. no power to the device)
2. Data Lock: the device is powered on, not authenticated to the TOE
3. Data Unlock: the device is powered on, authenticated to the TOE

The TOE spends most of its time between states two (Data Lock) and three (Data Unlock). It is not possible to move directly from Off to Data Unlock; the TOE always starts in the Data Lock state on startup.

During the Off state, the MKDD and any unlocked FEKS that may be in use are removed from volatile storage automatically, regardless of whether this state was by user shutdown/restart or by power failure.

On startup, the device places the TOE into the Data Lock state. From the Data Lock state, the user must authenticate successfully to transition to the Data Unlock state. How the TOE came to be in the Data Lock state (i.e. either directly from Off or from Data Unlock), does not change the functionality of the state; in either case successful authentication is required to move to the Data Unlock state. The authentication will allow the MKDD to be decrypted, which in turn will allow the FEKs to be decrypted.

When the TOE transitions to the Data Lock state from the Data Unlock state, the MKDD and any FEKs are cleared from volatile storage and any open files are closed. The transition to the Data Lock state can be initiated by the device being locked or by a timeout period (tied to inactivity in the work profile or by an administrator configuration).

Inactivity settings are controlled by the work profile configuration. These settings are not part of the TOE configuration but are used to determine when the Data Lock transition should occur. The transition itself controlled by the Data Lock setting which specifies the amount of inactive time that can pass before an automatic transition to the Data Lock state. The Data Lock timeout starts after the work profile inactivity period has been reached.

When the FEB configuration is for a Knox work profile, inactivity settings are controlled by the work profile configuration. Similarly, when the FEB configuration is for the whole device, the inactivity settings are controlled by the device configuration. These settings are not part of the TOE configuration but are used to determine when the Data Lock transition should occur. The transition itself controlled by the Data Lock setting which specifies the amount of inactive time that can pass before an automatic transition to the Data Lock state. The Data Lock timeout starts after the device or work profile inactivity period has been reached.

MOD_FE_V1.0: FDP_PRT_EXT.1/ MOD_FE_V1.0: FDP_PRT_EXT.2
The TOE automatically encrypts all files within the FEB, regardless of the point of creation (i.e. a direct user request to create a file vs. an application creating the file on behalf of the user). No temporary files are used during the encryption/decryption process as all file content access is handled through in-place buffers. The TOE only encrypts the file contents; file metadata is not encrypted (the encrypted version of the FEK is considered to be metadata).

The TOE is invoked when the FEB is unlocked by the user entering their credentials. Until successful authentication, all files are encrypted and not accessible. When the FEB enters the Data Lock state, the MKDD and all FEKs are cleared from memory, closing all applications and leaving all data in non-volatile memory encrypted (a Flush Operation is called when a work profile is locked, the device is automatically rebooted when the device is encrypted).

The TOE intercepts all read/write calls from within the FEB and automatically encrypts/decrypts the files utilizing the platform encryption libraries.

MOD_FE_V1.0: FDP_PRT_EXT.3
The TOE automatically intercepts all read/write requests for files contained within the FEB. This ensures that any temporary files created by applications within the FEB are automatically encrypted without the application needing to be made aware.

6.3 Identification and Authentication

PP_APP_V1.4: FIA_AUT_EXT.1
The TOE utilizes the Knox work profile authentication service to acquire the user password so MKDD can be decrypted and the encrypted data unlocked. The platform provides the password directly to the TOE (without modification).

If the TOE is configured to encrypt the whole device, it provides its own authentication dialog to acquire the user password to decrypt the MKDD and unlock encrypted data.

The provided password is conditioned by the TOE with 100,000 rounds of PBKDF2 (using HMAC-SHA-256) to generate a 256-bit KEK.

6.4 Security Management

The TOE is bundled as a component of the Samsung Android operating system on supporting Galaxy devices. The functionality of the TOE is a feature of Knox, and must be enabled via the device management agent; the TOE itself does not provide any management capability but relies on the configuration capabilities of the device and Knox work profile.

PP_APP_V1.4: FMT_CFG_EXT.1
Depending on the FEB configuration, the TOE either relies on the platform to handle authentication credentials or manages them directly.

When the FEB is configured to encrypt a Knox work profile, the TOE relies on the platform to handle authentication credentials. As part of the setup of the Knox work profile for the evaluated configuration the user is required to setup their credentials.

When the FEB is configured to encrypt the device, the TOE provides its own configuration to manage the authentication credentials. The TOE does not provide any default credentials and as part of the setup of this configuration the user is required to enter their credentials. The user cannot complete the setup without entering these credentials.

The TOE relies on Android permissions to restrict access to files created by the TOE.

The TOE is a service bundled as part of the Knox software on the device. The TOE does not have its own data folder but is a feature within the wider Knox software. The configuration of the TOE is maintained and protected within the Knox configuration.

PP_APP_V1.4: FMT_MEC_EXT.1 (KMD)
The TOE configuration is stored as part of the device or the Knox work profile configuration and is not maintained separately.

PP_APP_V1.4: FMT_SMF.1
The TOE configuration has the following common settings:

- TOE functionality is enabled (it cannot be disabled except by removing the Knox work profile or a factory reset depending on the FEB configuration)
- Timeout period for automatically entering the Data Lock state after the device has become locked

When the TOE FEB is configured for the whole device, the password settings for Knox File Encryption are the same as the device password settings. These are automatically used as the parameters for the Knox File Encryption password and cannot be changed individually with the following two exceptions:

- Minimum password length
- Specify an administrator reset token (to allow for the Knox File Encryption password to be reset by the administrator)

The administrator can specify a different minimum password length from the device setting. In addition, the administrator can specify a reset token which can be used to unlock Knox File Encryption so a user can reset their password. The password reset token is only active if a value is provided, so the default configuration is disabled.

These settings are specified by the management agent on the device. There are no other configuration settings for the TOE.

MOD_FE_V1.0: FMT_SMF.1(2)
If the FEB is set for a Knox work profile, when the work profile is removed (such as by unenrollment or by policy by failed login attempts as defined by the work profile management), the MKDD will be erased. If the FEB configuration is for the whole device, the device must be factory reset to erase the MKDD (either by local control or by MDM).

6.5 Privacy

PP_APP_V1.4: FPR_ANO_EXT.1
The TOE does not transmit any information over a network.

6.6 Protection of the TSF

PP_APP_V1.4: FPT_AEX_EXT.1
The TOE components are all compiled with the -fstack-protector option set to enable stack-based buffer overflow protection. The Android Linux kernel provides eight unpredictable bits to the base address of any user-space memory mapping (ASLR) which is supported by the parts of the TOE that run User space. For the components that are kernel modules, the kernel supports KASLR to provide unpredictable bits to the base address of the kernel and all its components at startup. The TOE does not allocate READ and WRITE on memory at the same time.

PP_APP_V1.4: FPT_API_EXT.1 (KMD)
The TOE uses only platform provided APIs as noted below:

- All
  - Android SDK API Level 33
  - Samsung Knox API Level 36
- DualDAR Client
  - Samsung SCrypto Module – AES operations, HMAC-SHA, DRBG
- DualDAR Driver
  - Samsung Kernel Cryptographic Module – AES operations, DRBG

PP_APP_V1.4: FPT_IDV_EXT.1/PP_APP_V1.4: FPT_TUD_EXT.1
The TOE is part of the Knox software contained within the Samsung Android operating system. The TOE relies on the platform for all updates as it is considered a part of the operating system. The platform provides the ability to check for and install updates.

The platform user interface provides a method to query the current version of many components, including the TOE software. The TOE software version can be viewed in the *About Phone/Software information* section in Settings. Under the Knox version section of the display, the software version can be seen as the DualDAR version. The DualDAR Version in Table 1 - Evaluated Devices shows the specific software version evaluated.

MOD_FE_V1.0: FPT_KYP_EXT.1
The TOE stores the MKDD and the FEKs separately in non-volatile memory. The MKDD is stored in the TrustZone where it is wrapped with a key derived from the credentials of the Knox work profile password (using PBKDF2).

The TOE stores a FEK as part of the file metadata. The FEK is encrypted using AES-GCM with the MKDD KEK.

PP_APP_V1.4: FPT_LIB_EXT.1
The TOE runs on Samsung devices that have launched with at least Android 13 and Knox 3.9. The TOE only utilizes the libraries provided with the platform and does not contain any third party libraries as part of the TOE boundary.

PP_APP_V1.4: ALC_TSU_EXT
Samsung utilizes industry best practices to ensure their devices and all components on the device are patched to mitigate security flaws. Samsung provides a web portal for reporting potential security issues (https://security.samsungmobile.com/securityReporting.smsb) with instructions about how to securely contact and communicate with Samsung.

Samsung will create updates and patches to resolve reported issues as quickly as possible, at which point the update is provided to the wireless carriers. The delivery time for resolving an issue depends on the severity, and can be as rapid as a few days before the carrier handoff for high priority cases. The wireless carriers perform additional tests to ensure the updates will not adversely impact their networks and then plan device rollouts once that testing is complete. Carrier updates usually take at least two weeks to as much as two months (depending on the type and severity of the update) to be rolled out to customers. However, the Carriers also release monthly Maintenance Releases in order to address security-critical issues, and Samsung itself maintains a security blog (http://security.samsungmobile.com) in order to disseminate information directly to the public.

Samsung communicates with the reporting party to inform them of the status of the reported issue. Further information about updates is handled through the carrier release notes. Issues reported to Google directly are handled through Google's notification processes.

6.7 Trusted Path/Channels

PP_APP_V1.4: FTP_DIT_EXT.1
The TOE does not transmit any data over a network.