National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

PP-Configuration for Application Software and File Encryption

Version 1.0

31 January 2020

Report Number:	**CCEVS-VR-PP-0058**
Dated:	**31 January 2020**
Version:	**1.0**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base Requirements
Gossamer Security Solutions
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Application Software and File Encryption, Version 1.0 (CFG_APP-FE_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Application Software Protection Profile (PP_APP_V1.3) Base-PP and the PP-Module for File Encryption, Version 1.0 (MOD_FE_V1.0). It presents a summary of the CFG_APP-FE_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Catonsville, Maryland, performed the evaluation of the CFG_APP-FE_V1.0 and the MOD_FE_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration. The evaluated product was Samsung Knox File Encryption 1.0.

This evaluation addressed the base security functional requirements of MOD_FE_V1.0 as part of CFG_APP-FE_V1.0 and several of the additional requirements contained in Appendices A and B of the PP-Module.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration and PP-Module as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_APP-FE_V1.0 is both Common Criteria Part 2 extended and Part 3 extended. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5).

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and PP-Configurations that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 work units specific to the technology described by the PP or PP-Configuration.

In order to promote thoroughness and efficiency, the evaluation of the CFG_APP-FE_V1.0 and MOD_FE_V1.0 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Samsung Knox File Encryption 1.0, performed by Gossamer Security Solutions in Catonsville, Maryland, United

This evaluation addressed the base security functional requirements of MOD_FE_V1.0 as part of CFG_APP-FE_V1.0 and several of the additional requirements contained in Appendices A and B of the PP-Module. The security functional requirements for PP_APP_V1.3 were already addressed by a separate VR.

MOD_FE_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the PP-Module. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the MOD_FE_V1.0 were evaluated.

The following identifies the PP-Module evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP-Module.

PP-Configuration	PP-Configuration for Application Software and File Encryption, Version 1.0, 25 July 2019
Module(s) in PP-Configuration	Protection Profile Module for File Encryption, Version 1.0, 25 July 2019
ST (Base)	Samsung Electronics Co., Ltd. Samsung Knox File Encryption (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.5, 06 December 2019
Assurance Activity Report (Base)	Assurance Activity Report (ASPP13/FEM10) for Samsung Electronics Co., Ltd. Samsung Knox File Encryption, Version 0.5, 06 December 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions Catonsville, Maryland 21228

3 CFG_APP-FE_V1.0 Description

CFG_APP-FE_V1.0 is a PP-Configuration that includes the following components:

- Protection Profile for Application Software, Version 1.3 (PP_APP_V1.3)
- Protection Profile Module for File Encryption, Version 1.0 (MOD_FE_V1.0)

The PP-Configuration defines a baseline set of security functional requirements (SFRs) for software applications (defined in PP_APP_V1.3) that specifically implement file encryption (defined in MOD_FE_V1.0).

File encryption is the process of encrypting individual files or sets of files (or volumes, or containers, etc.) on an end user device and permitting access to the encrypted data only after proper authentication is provided. Encryption products that conform to this PP-Module must render information inaccessible to anyone (or, in the case of other software on the machine, anything) that does not have the proper authentication credential. The encrypted files may be on a local machine or may be sent to other devices.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_APP-FE_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_APP_V1.3	
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.
From MOD_FE_V1.0	
A.AUTH_FACTOR	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.
A.EXTERNAL_FEK_PROTECTION	External entities that implement ECC CDH or RSA that are used to encrypt and decrypt a FEK have the following characteristics: - meet national requirements for the cryptographic mechanisms implemented - require authentication via a pin or other mechanisms prior to allowing access to protected information (the decrypted FEK, or the private key) - implement anti-hammer provisions where appropriate (for example, when a pin is the authentication factor).
A.SHUTDOWN	An authorized user will not leave the machine in a mode where sensitive information persists in non-volatile storage.
A.STRONG_OE_CRYPTO	All cryptography implemented in the Operational Environment and used by the TOE will meet the requirements listed in this PP-Module. This includes generation of external token authorization factors by a RBG.
A.FILE_INTEGRITY	When the file is in transit, it is not modified, otherwise if that possibility exists, the appropriate selections in Appendix B are chosen for Data Authentication.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_APP-FE_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_APP_V1.3	

T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
From MOD_FE_V1.0	
T.UNAUTHORIZED_DATA_ACCESS	An attacker has access to an account that is not permitted to decrypt files or has no access and uses forensic tools for examination.
T.MANAGEMENT_ACCESS	An authorized user may perform sensitive management functions without authorization or a legitimate user may lack the ability to perform necessary security operations due to a lack of supported management functionality.
T.KEYING_MATERIAL_COMPROMISE	An attacker exploits a weakness in the random number generation, plaintext keys, and other keying material to decrypt an encrypted file.
T.UNSAFE_AUTHFACTOR_VERIFICATION	An attacker exploits a flaw in the validation or conditioning of the authorization factor.
T.KEYSPACE_EXHAUST	An attacker is able to brute force the key space of the algorithms used to force disclosure of sensitive data.
T.PLAINTEXT_COMPROMISE	An attacker is able to uncover plaintext remains with forensic tools.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_APP-FE_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
PP_APP_V1.3 and MOD_FE_V1.0 do not define any organizational security policies.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_APP-FE_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_APP_V1.3	

O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.
From MOD_FE_V1.0	
O.KEY_MATERIAL_PROTECTION	The TOE must ensure that sensitive plaintext key material used in performing its operations is cleared once it is no longer needed. Key material must be identified; its use and intermediate storage areas must also be identified; and then those storage areas must be cleared in a timely manner and without interruptions. For example, authorization factors are only needed until the KEK is formed; at that point, volatile memory areas containing the authorization factors should be cleared.
O.FEK_SECURITY	In order to ensure that brute force attacks are infeasible, the TOE must ensure that the cryptographic strength of the keys and authorization factors used to generate and protect the keys is sufficient to withstand attacks in the near-to-mid-term future. Password/passphrase conditioning requirements are also levied to

	help ensure that a brute force attack against these authorization factors (when used) has a similar level of resistance.
O.WIPE_MEMORY	To address the threat of unencrypted copies of data being left in non-volatile memory or temporary files where it may be accessed by an unauthorized user, the TOE will ensure that plaintext data it creates is securely erased when no longer needed. The TOE's responsibility is to utilize the appropriate TOE platform method for secure erasure, but the TOE is not responsible for verifying that the secure erasure occurred as this will be the responsibility of the TOE platform.
O.PROTECT_DATA	The TOE will encrypt data to protect the data from unauthorized access. Encrypting the file or set of files will protect the user data even when low-level tools that bypass operating system protections such as discretionary and mandatory access controls are available to an attacker. Users that are authorized to access the data must provide authorization factors to the TOE in order for the data to be decrypted and provided to the user. The TOE will also optionally include data authentication functionality to protect data from unauthorized modification.
O.SAFE_AUTHFACTOR_VERIFICATION	In order to avoid exposing information that would allow an attacker to compromise or weaken any factors in the chain keys generated or protected by the authorization factors, the TOE will verify the valid authorization factor prior to the FEK being used to decrypt the data being protected.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_APP-FE_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_APP_V1.3	
OE.PLATFORM	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.PROPER_USER	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	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.
From MOD_FE_V1.0	
OE.AUTHORIZATION_FACTOR_STRENGTH	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.POWER_SAVE	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.STRONG_ENVIRONMENT_CRYPTO	The Operating environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE.

5 Functional Requirements

As indicated above, CFG_APP-FE_V1.0 includes both PP_APP_V1.3 and MOD_FE_V1.0. The functional requirements from PP_APP_V1.3 were evaluated separately so this section applies only to requirements of MOD_FE_V1.0.

As indicated above, requirements in the MOD_FE_V1.0 are comprised of the "base" requirements and additional requirements that are optional or selection-based. The following table contains the "base" requirements that were validated as part of the Gossamer Security Solutions evaluation activities referenced above.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.2: File Encryption Key (FEK) Generation	Samsung Knox File Encryption 1.0
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Samsung Knox File Encryption 1.0
	FCS_IV_EXT.1: Initialization Vector Generation	Samsung Knox File Encryption 1.0
	FCS_KYC_EXT.1: Key Chaining and Key Storage	Samsung Knox File Encryption 1.0
	FCS_VAL_EXT.1: Validation	Samsung Knox File Encryption 1.0
FDP: User Data Protection	FDP_PRT_EXT.1: Protection of Selected User Data	Samsung Knox File Encryption 1.0
	FDP_PRT_EXT.2: Destruction of Plaintext Data	Samsung Knox File Encryption 1.0
FIA: Identification and Authentication	FIA_AUT_EXT.1: User Authorization	Samsung Knox File Encryption 1.0
FMT: Security Management	FMT_SMF.1(2): Specification of File Encryption Management Functions	Samsung Knox File Encryption 1.0
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Keys and Key Material	Samsung Knox File Encryption 1.0

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 6: Optional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.5: File Authentication Key (FAK) Support	PP-Module Evaluation
	FCS_COP_EXT.1: FAK Encryption/Decryption Support	PP-Module Evaluation
FDP: User Data Protection	FDP_AUT_EXT.1: Authentication of Selected User Data	PP-Module Evaluation
	FDP_AUT_EXT.2: Data Authentication Using Cryptographic Keyed-Hash Functions	PP-Module Evaluation
	FDP_AUT_EXT.3: Data Authentication Using Asymmetric Signing and Verification	PP-Module Evaluation
	FDP_PM_EXT.1: Protection of Data in Power Managed States	Samsung Knox File Encryption 1.0
	FDP_PRT_EXT.3: Protection of Third-Party Data	Samsung Knox File Encryption 1.0
FIA: Identification and Authentication	FIA_FCT_EXT.1: Multi-User Authorization	PP-Module Evaluation
	FIA_FCT_EXT.2: Authorized Key Sharing	PP-Module Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE work units and has indicated its verification through "PP Evaluation."

Table 7: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.3: Key Encrypting Key (KEK) Support	Samsung Knox File Encryption 1.0
	FCS_CKM_EXT.6: Cryptographic Password/Passphrase Conditioning	Samsung Knox File Encryption 1.0
	FCS_COP.1(5): Cryptographic Operation (Key Wrapping)	Samsung Knox File Encryption 1.0
	FCS_COP.1(6): Cryptographic Operation (Key Transport)	PP-Module Evaluation
	FCS_COP.1(7): Cryptographic Operation (Key Encryption)	PP-Module Evaluation
	FCS_KDF_EXT.1: Cryptographic Key Derivation Function	Samsung Knox File Encryption 1.0
	FCS_SMC_EXT.1: Submask Combining	PP-Module Evaluation
	FCS_VAL_EXT.2: Validation Remediation	PP-Module Evaluation

This PP-Module does not define any "**Objective**" requirements.

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_APP_V1.3. The SARs defined in that PP are applicable to MOD_FE_V1.0 as well as CFG_APP-FE_V1.0 as a whole.

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 7: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Samsung Knox File Encryption 1.0
ACE_CCL.1	Pass	Samsung Knox File Encryption 1.0
ACE_SPD.1	Pass	Samsung Knox File Encryption 1.0
ACE_OBJ.1	Pass	Samsung Knox File Encryption 1.0
ACE_ECD.1	Pass	Samsung Knox File Encryption 1.0
ACE_REQ.1	Pass	Samsung Knox File Encryption 1.0
ACE_MCO.1	Pass	Samsung Knox File Encryption 1.0
ACE_CCO.1	Pass	Samsung Knox File Encryption 1.0

8 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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_FE_V1.0 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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 the CCEVS Validation Body uses that leads to the issuance 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.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] PP-Module for File Encryption, Version 1.0, 25 July 2019.

[7] Protection Profile for Application Software, Version 1.3, 01 March 2019.

[8] PP-Configuration for Application Software and File Encryption, Version 1.0, 25 July 2019.

[9] Samsung Electronics Co., Ltd. Samsung Knox File Encryption (PP_APP_V1.3/MOD_FE_V1.0) Security Target, Version 0.5, 06 December 2019

[10] Assurance Activity Report (ASPP13/FEM10) for Samsung Electronics Co., Ltd. Samsung Knox File Encryption, Version 0.5, 06 December 2019