National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Application Software Protection Profile (APP PP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, November 10, 2014

Report Number: CCEVS-VR-PP-0027
Dated: March 10, 2016
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 and Additional Requirements
Gossamer Security Solutions
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Application Software Protection Profile (APP PP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, November 10, 2014 (pp_app_swfe_ep_v1.0). It presents a summary of the pp_app_swfe_ep_v1.0 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the pp_app_swfe_ep_v1.0 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the CyberReliant Corporation's (CRC) Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2). The evaluation was performed by Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, in the United States and was completed in October 2015. This evaluation addressed the base requirements of the pp_app_swfe_ep_v1.0, as well as a few of the optional, selection-based and objective requirements contained in the Appendices.

The information in this report is largely derived from the Assurance Activity Report (AAR), written by the Gossamer Security Solutions.

The evaluation determined that the pp_app_swfe_ep_v1.0 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the pp_app_swfe_ep_v1.0, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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

The validation team found that the evaluation showed that the pp_app_swfe_ep_v1.0 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the pp_app_swfe_ep_v1.0 was performed concurrent with the first product evaluation against the PP. In this case the

TOE for this first product was the Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2), provided by CyberReliant Corporation's (CRC). Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, in the United States and was completed in October 2015.

The pp_app_swfe_ep_v1.0 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either optional, selection-based, or objective depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because these additional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the pp_app_swfe_ep_v1.0 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional requirements in the pp_app_swfe_ep_v1.0.

Protection Profile	*Application Software Protection Profile (APP PP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, November 10, 2014*
ST (Base)	CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target Version 0.6 October 21, 2015
ST (Additional)	Trivalent Data at Rest (DaR) Service (Inside) (APP PP11/FEEP10) Security Target Version 0.6, December 21, 2015
Assurance Activity Report (Base)	Assurance Activity Report (APP PP11/ASFEEP10) for CRC Data at Rest Service (Native) Version 1.0.0 (Version Code 2) Version 0.4, October 29, 2015
Assurance Activity Report (Additional)	Assurance Activity Report (APP PP11/ASFEEP10) for Trivalent Data at Rest Service (Inside) Version 0.6, December 23, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
CCTL (base and additional)	Gossamer Security Solutions, Catonsville, MD USA
CCEVS Validators (base)	Ken Elliott, Aerospace Corporation Herb Ellis, Aerospace Corporation Kelly Hood, Aerospace Corporation Jerome Meyers, Aerospace Corporation
CCEVS Validators (Additional)	SAME AS ABOVE

3 PP_APP_SWFE_EP_v1.0 Description

This Extended Package (EP) describes security requirements for an encryption product that is configurable for the data it encrypts and is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. However, this EP is not complete in itself, but rather extends the Protection Profile for Application Software (AS PP). This introduction will describe the features of a compliant Target of Evaluation, and will also discuss how this EP is to be used in conjunction with the AS PP.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption Name	Assumption Definition
A.AUTHORIZED_USER	Authorized users of the host machine are well-trained, not actively working against the protection of the data, and will follow all provided guidance.
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 (e.g., power it down or enter a power managed state, such as a "hibernation mode").
A.STRONG_OE_CRYPTO	All cryptography implemented in the Operational Environment and used by the TOE will meet the requirements listed in Appendix C of this EP. This includes generation of external token authorization factors by a RBG.
A.PLATFORM_STATE	The platform on which the TOE resides is free of malware that could interfere with the correct operation of the product.
A.AUTHORIZED_CONFIGURATION	Access and ability to modify the cryptographic configuration files may be done only by authorized users
A.KEK_SECURITY	The KEK will be derived from a strong entropy source, attaining equal or greater bit strength to that of the block cipher it is used in.
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.

Table 1: Assumptions

4.2 Threats

Threat Name	Threat Definition
T.KEYING_MATERIAL_COMPROMISE	Attacks against the encryption product could take several forms; for

Threat Name	Threat Definition
	example, if there is a weakness in the random number generation mixing algorithm or the data sources used in random number generation are guessable, then the output may be guessable as well. If an attacker can guess the output of the pseudorandom number generator (PRNG) at the time an encryption key is made, then the output may be used to recreate the keying material and decrypt the protected files. As the encryption program runs, it will store a variety of information in memory. Some of this information, such as random bit generation (RBG) inputs, RBG output, copies of the plaintext file, and other keying material, could be very valuable to an attacker who wishes to decrypt an encrypted file. If the encryption product does not wipe these memory spaces appropriately, an attacker may be able to recreate the encryption key and access encrypted files.
T.KEYSPACE_EXHAUST	The protection of the data involves encrypting said data assuming an attacker may have significant computing resources at their disposal. Several ciphers have already been broken through brute-force attacks because the length of the keys used in those ciphers was too short to provide protection against a concerted computing effort to discover those keys. Because protection of the data may rely on a chaining of keys and encryption mechanisms, there are many opportunities for brute force attacks against each potential key in the chain, such that the weakest link in the chain of factors/keys will determine the overall strength against a brute force attack.
T.PLAINTEXT_COMPROMISE	Unlike full disk encryption, selectable encryption products also need to protect against data leaks to other applications on the machine. Many file creators and editors store temporary files as the user is working on a file, and restore files if the machine experiences an interrupt while a file is open. Any of these files, if not properly protected or deleted, could leak information about a protected file to an attacker. Other applications might also access volatile or non-volatile memory released by the file encryption product, and the software used to create files prior to encryption may retain information about the file even after it has been encrypted. As the user creates and saves a new document, the plaintext will be stored on the machine's hard drive. An attacker could then search for the plaintext of the sensitive, encrypted information. An attacker may not even have to access the encrypted file for the protected information to be compromised. When the user wishes to encrypt the document, this plaintext file should be replaced with the new encrypted version. For non-mobile devices, it is expected that if the volatile and/or non-volatile memory space where the plaintext file was stored is merely released back to the machine without being first wiped clean of the data that was stored there, then the information the user wishes to protect will still be accessible. While protection of the encryption algorithm itself is vital, memory must also be properly managed by the file encryption product or the TOE platform in order for security to remain intact. For mobile devices, it is assumed that the File Encryption product will not be responsible for providing memory management cleanup and the environment's platform has met the Mobile Device Fundamentals Protection Profile.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.
T.UNAUTHORIZED_DATA_ACCESS	The central functionality of the TOE is the protection of resources under its control through encryption. In a shared resource environment, users on a system may have access to administrative-level tools that are

Threat Name	Threat Definition
	capable of over-riding a system's access control protections. Further, if the system were to be lost or the system's storage device stolen, the attacker could then look directly at the storage device using low-level forensic tools in an attempt to access data for which they are not authorized. However, the need to protect the data in these 14 scenarios should not interfere with the data-owner's (or another user that has been granted access to those data) ability to read or manipulate the data.
T.UNSAFE_AUTHFACTOR_VERIFICATION	When a user enters an authorization factor, the TOE is required to ensure that the authorization factor is valid prior to providing any data to the user; the purpose of verification is to ensure the FEK is correctly derived. If the data is decrypted with an incorrectly derived FEK (the FEK is conditioned from the password/passphrase or is decrypted by the KEK), then unpredictable data will be provided to the user. If verification is not performed in a secure manner, keying material or user data may be exposed or weakened.
T.PLAINTEXT_DATA_SPOOFING	For certain modes of encryption, it is possible for a malicious person to modify ciphertext data to force unintended modification to the underlying plaintext data, without the user being notified. There are various failures that may occur on the part of the TOE, to include: failure to verify the integrity of the data prior to decryption, failure to provide integrity on the sensitive data, failure to use a cryptographic or secure hashing code and failure to differentiate the File Authentication Key (FAK) from the FEK; the FAK is any secret value used as input to a keyed hashing function or as part of an asymmetric authentication process.

Table 2: Threats

4.3 Organizational Security Policies

The pp_app_swfe_ep_v1.0 does not define organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

TOE Security Obj.	TOE Security Objective Definition
O.KEY_MATERIAL_PROTECTION	The TOE shall ensure that unencrypted keys or keying material are properly removed from memory after use.
O.FEK_SECURITY	The TOE will encrypt the FEK using a KEK created from one or more authorization factors so that a threat agent who does not have the authorization factor(s) will be unable to gain access to the user data by obtaining the FEK. The size of the FEK will be large enough to make a brute force attack infeasible.
O.WIPE_MEMORY	The TOE shall ensure that non-volatile memory space corresponding to sensitive plaintext material (encryption input) is wiped from the TOE's memory. This includes temporary files that may have been created
O.PROTECT_DATA	The TOE will decrypt/encrypt all user data that is provided to the file encryption program in order to protect it while it is not being activity accessed by the user.
O.AUTHORIZATION	The TOE must enforce the entry of authorization factor(s) by authorized users to be able to encrypt and decrypt user data.
O.SAFE_AUTHFACTOR_VERIFICATION	The TOE shall perform verification of the authorization factors in such a way that the KEK, FEK, or user data are not inadvertently exposed.

TOE Security Obj.	TOE Security Objective Definition
O.DATA_AUTHENTICATION	The TOE shall verify the integrity of the plaintext data using an approved data authentication method.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF in its operational environment
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 3: Security Objectives for the TOE

The following table contains objectives for the Operational Environment.

TOE Security Obj.	TOE Security Objective Definition
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	The non-mobile operational environment must be configurable so that there exists at least one mechanism that will cause the system to power down after a period of time in the same fashion as the user electing to shutdown the system (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.STRONG_ENVIRONMENT_ CRYPTO	The Operating environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE
OE.TRAINED_USERS	Authorized users of the host machine will be trained to follow all provided guidance.

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the pp_app_swfe_ep_v1.0 are comprised of the "base" requirements and additional requirements that are either optional, selection-based, or objective depending on the requirement in question. The following are table contains the "base" requirements that were validated as part of the CyberReliant evaluation activity referenced above.

Requirement Class	Requirement Component
Security Functional Requirements for the File Encryption Application (TOE)	
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Generation (FEK)
FDP: User Data Protection	FDP_PRT_EXT.1: Extended: Protection of Selected User Data
FMT: Security Management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_FEK_EXT.1: File Encryption Key (FEK) Support
	FPT_KYP_EXT.1: Extended: Protection of Key and Key Material
	FPT_TUD_EXT.1: Integrity for Installation and Update

	FPT_LIB_EXT.1: Use of Third Party Libraries
FTP: Trusted path/channels	FTP_DIT_EXT.1: Protection of Data in Transit
Security Functional Requirements for the Software File Encryption Application or Client Platform	
FCS: Cryptographic Support	FCS_CKM_EXT.4: Extended: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic Operation Encryption
	FCS_COP.1(5): Cryptographic Operation (Key Wrapping)
	FCS_IV_EXT.1: Extended: Initialization Vector Generation
	FCS_KYC_EXT.1: Key Chaining and Key Storage
FIA: Identification and Authentication	FIA_AUT_EXT.1: Authentication and Failure Handling
FDP: User Data Protection	FDP_PRT_EXT.1: Extended: Protection of Selected User Data

Table 5: Base Requirements

The following table contains the additional optional requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_COP.1(6): FAK encryption/decryption support	
	FCS_CKM_EXT.5: File Authentication Key (FAK) Support	
	FCS_SMC_EXT.1 Submask Combining	
FDP: User Data Protection	FDP_PRT_EXT.2: Extended: Protection of Selected User Data	
	FDP_PM_EXT.1: Extended: Protection of Data in Power Managed States	
	FDP_AUT_EXT.1: Extended: Authentication of Selected User Data	
	FDP_AUT_EXT.2: Extended: Data Authentication using cryptographic, keyed hash functions	
	FDP_AUT_EXT.3: Extended: Data Authentication using asymmetric signing and verification	

Table 6: Optional Requirements

The following table contains the additional selection-based requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.1(A): Cryptographic key generation (Password/Passphrase conditioning)	CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target Version 0.6 October 21, 2015
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)	CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target Version 0.6 October 21, 2015
	FCS_CKM_EXT.1: Key Encryption Key (KEK) Support	CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target Version 0.6 October 21, 2015
FIA: Identification and Authentication	FIA_FCT_EXT.1(1): Extended: User Authorization with External Entity Authorization Factors	
	FIA_FCT_EXT.1(2): Extended: User Authorization with Password/Passphrase Authorization Factors	CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target Version 0.6 October 21, 2015

Table 7: Selection-Based Requirements

The pp_app_swfe_ep_v1.0 does not contain any objective requirements.

6 Assurance Requirements

The following are the assurance requirements contained in the pp_app_swfe_ep_v1.0:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

Table 8: Assurance Requirements

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass

APE_OBJ.2	Pass
APE_REQ.1	Pass

Table 9: Evaluation Results

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 in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the pp_app_swfe_ep_v1.0 Assurance Activities to determine whether or not 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.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Gossamer Security Solutions, Inc., *CyberReliant Corp. Data at Rest (DaR) Service (Native) (APP PP11/FEEP10) Security Target* Version 0.6 October 21, 2015

[7] Gossamer Security Solutions, Inc., *Trivalent Data at Rest (DaR) Service (Inside) (APP PP11/FEEP10) Security Target* Version 0.6, December 21, 2015

[8] Gossamer Security Solutions, Inc., *CRC Data at Rest (DaR) Service (Native) Validation Report* Version 0.3, October 29th, 2015

[9] Gossamer Security Solutions, Inc., *Trivalent Data at Rest (DaR) Service (Inside)Validation Report* Version 1.0, December 23, 2015

[10] Gossamer Security Solutions, Inc., *Assurance Activity Report (APP PP11/ASFEEP10) for CRC Data at Rest Service (Native) Version 1.0.0 (Version Code 2)* Version 0.4, October 29, 2015

[11] Gossamer Security Solutions, Inc., *Assurance Activity Report (APP PP11/ASFEEP10) for Trivalent Data at Rest Service (Inside)* Version 0.6, December 23, 2015

[12] Application Software Protection Profile (APP PP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, November 10, 2014