Swedish Certification Body for IT Security

Certification Report

File Encryption PP

Issue: 1.0, 2018-aug-22

Table of Contents

1 Executive Summary

The File Encryption Protection Profile, describes a software TOE, an encryption application for protecting sensitive information in files during transport through unprotected environments. The application provides cryptographic services based on both pre-shared keys and a public key infrastructure. The encryption application provides confidentiality, integrity protection and non-repudiation functionality.

The encryption application is intended to run on a COTS general purpose operating system and a COTS hardware platform in a physically secure environment. Some of the functionality may require access to an X.500 certificate catalougue providing certificate information, CRLs and/or OCSP services. If smart cards are used, smartcard readers will be needed. The application also requires external sources for time and entropy, e.g. in the operating system.

The File Encryption Protection Profile requires demonstrable conformance, and does not claim conformance to any other PP. The product assurance package is EAL3 + ALC_FLR.2.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden and was completed on the 4th of July 2018.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed according to the requirements in assurance class APE.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology.

2 Identification

Certification Identification

Certification ID	CSEC2018001
Name and version of the certified IT product	File Encryption Protection Profile v1.0
Compliance requirement	Demonstrable conformance
Assurance level	Assurance class APE
Product assurance level	EAL3 + ALC_FLR.2
Sponsor	Myndigheten för samhällsskydd och beredskap, MSB
Developer	Myndigheten för samhällsskydd och beredskap, MSB
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2018-08-22

3 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the evaluated PP [FePP] meets the requirements in assurance class APE.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance class and its components are summarised in the following table:

Assurance Class/Component	*Short name*	*Verdict*
Protection Profile Evaluation	APE	PASS
PP Introduction	APE_INT.1	PASS
Conformance Claims	APE_CCL.1	PASS
Security Problem Definition	APE_SPD.1	PASS
Security Objectives	APE_OBJ.2	PASS
Extended Components Definition	APE_ECD.1	PASS
Security Requirements	APE_REQ.2	PASS

4 Evaluator Comments and Recommendations

None.

5 Glossary

PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

6 Bibliography

FePP	File Encryption Protection Profile, MSB, 2018-07-04, document version 1.0
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2018-04-24, document version 29.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2017-04-04, document version 7.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2016-04-03:

QMS 1.21.2 valid from 2018-03-09

QMS 1.21.3 valid from 2018-05-24

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.21.3”.

The certifier concluded that, from QMS 1.21.2 to the current QMS 1.21.3, there are no changes with impact on the result of the certification.