Swedish Certification Body for IT Security

Certification Report - Protection Profile Encrypted Storage Device

Issue: 1.0, 2012-jun-25

Authorisation: Mikael Åkerholm, Lead Certifier , CSEC

Report Distribution:	FMV/AK Led (Tomas Falkman)
	atsec information security AB (Rasma M Araby)
	ProAvia (Anna-Lena Hallgren)
	FMV/CSEC (Mikael Åkerholm)
	Arkiv

Table of Contents

1 Executive Summary

This report describes a Protection Profile certification done by CSEC, The Swedish Certification Body for IT Security. The Protection Profile describes an Encrypted Storage Device (ESD). The evaluation is based on the requirements of the APE (Protection Profile Evaluation) assurance class of the Common Criteria for Information Security Evaluation.

The Encrypted Storage Device shall be used in a trusted environment by a legitimate user. The ESD is a personal device and it shall only be used for temporary storage of data whilst the data is in transit between two trusted host computers. In the event the ESD is lost or stolen, all confidential information stored in persistent memory in the ESD shall be encrypted to prevent the information from being disclosed to unauthorised parties.

The user shall be required to authenticate to the ESD by providing a user secret before performing any other operation. The user secret shall be input directly on the device, or via an application executing on the trusted host computer. If the user secret is entered into the host computer, then the application in the host is also considered part of the TOE (Target of Evaluation). The user secret shall not be a biometric identifier.

There are four assumptions and two optional assumptions made in the PP regarding the secure usage and environment of the ESD.

There are two architectures for the TOE, type A and type B, depending on if the applications are executed in the ESD or in the host.

The TOE has 20 different Security Function Requirements addressed in the PP.

The assurance package is EAL2+.

EAL2 is applicable in those circumstances where users require a low to moderate level of independently assured security. EAL2 has been augmented with ATE_COV.2 to ensure full test coverage of all TOE Security Function Interfaces (TSFI).

The evaluation of the PP Encrypted Storage Device was conducted by atsec information security AB and completed on April 26, 2012. This certification report is based on the content of the Evaluation Technical Report (ETR) submitted by atsec information security AB. The evaluation was conducted by applying CEM, and the certification process has verified that the PP satisfies all APE requirements according to Common Criteria.

The certificate applies only to the specific version and release of the protection profile listed in this certification report.

The certificate is not an endorsement of the protection profile by CSEC or by any other organisation that recognises or gives effect to this certificate, and no warranty of the protection profile by CSEC or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC 2012001
Identification of the certified PP	PP Encrypted Storage Device
Assurance Package	EAL 2, augmented by ATE_COV.2
Sponsor	FMV Ak Led, Banérgatan 62, 115 88 Stockholm
PoC	Tomas Falkman
ITSEF	atsec information security AB Svärdvägen 11 182 33 Danderyd
Common Criteria version	3.1, Revision 3, Final

3 Security Related Qualities

3.1 Security Policy

Organisational Cryptographic and Entropy policies are summarized in [PP] section 3.5, Organisational Security Policy.

3.2 Assumptions

There are four assumptions and two optional assumptions made in the PP regarding the secure usage and environment of the ESD. The TOE only relies on these being met to counter the five threats and one optional threat to fulfill the organizational security policies (OSP) in the PP. The assumptions, the threats and the organizational security policies are described in chapter 3 in [PP].

3.3 Clarification of Scope

To address the need for vulnerability analysis of the cryptographic functions, refinements have been made to ensure that ADV_TDS.1 provides additional information of the design and implementation representation of the cryptographic functions. This information will be used when performing AVA_VAN.2, which also has been refined to specify specific testing.

3.4 Architectural Information

There are two architectures for the ESD, type A and type B.

In architecture type A, the Application for initialization and the Application for authentication are stored on and executed by the ESD. The user secret is input directly into the ESD.

In architecture type B, the Application for initialization and the Application for authentication are executed on the host. The user secret is input to the ESD via the host. The applications may either be installed on the host or be stored on the ESD. In both cases, both applications are included in the TOE. For further details see [PP] section 1.2.3, TOE components.

The TOE has 21 different Security Function Requirements addressed in the PP (see [PP] section 6.2). The areas are:

- Cryptographic support
- User Data Protection
- Identification and Authentication
- Security Management

There are also Information Flow Control Policies and requirements regarding Random Number Generation.

The ESD may have an onboard upgradable firmware. If the firmware is upgradable, the firmware upgrade package shall be signed by a trusted party, and the authenticity of the signed package shall be verified by the ESD before performing any other action with respect to the upgrade package. The public key used for signature verification shall be generated and stored in the ESD at production.

Further details in [PP] section 1.2.6, Optional security features.

4 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Family Name	Assurance Components	Verdict
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

Summarizing the results of all assurance components, the final evaluation result is PASS.

5 Glossary

ADV_TDS	Assurance Development - TOE Design
ATE_COV	Assurance Test - Coverage
AVA_VAN	Assurance Vulnerability Assessment - Vulnerability Analysis
CC	Common Criteria
CEM	Common Methodology for Information Security Evaluation
EAL	Evaluation Assurance Level
ESD	Encrypted Storage Device
ETR	Evaluation Technical Report
ITSEF	IT Security Evaluation Facility
PP	Protection Profile
TOE	Target of Evaluation
TSFI	TOE Security Functional Interface

6 Bibliography

PP	Protection Profile Encrypted Storage Device, v2.1, 2012.04-26, 11FMV10216-23.
CC	Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3, Final, July 2009.
CEM	Common Methodology for Information Security Evaluation, v3.1, Revision 3, Final, July 2009.