CSEC

Swedish Certification Body for IT Security

Certification Report - PP Information Gateway

Issue: 2.0, 2011-12-14

Report Distribution: FMV/Ak Led (Thomas Dahlbeck)
atsec information security AB (Rasma M. Araby)
Combitech AB (Anders Staaf)
FMV/CSEC(Mikael Åkerholm, Helén Svensson)
Arkiv

Table of Contents

1 Identification

Certification ID	CSEC 2011002
Identification of the certified PP	PP Information Gateway
Assurance Package	EAL 4, augmented by ALC_FLR.1.
Sponsor	FMV Ak Led, Banérgatan 62, 115 88 Stockholm PoC: Thomas Dahlbeck
ITSEF	atsec information security AB, Svärdvägen 11, 182 33 Danderyd
Common Criteria version	3.1, Revision 3, Final
CEM version	3.1, Revision 3, Final
Certification completion date	2011-11-14

2 Executive Summary

This report describes the Protection Profile Evaluation certification by the certification body on the evaluation results applied with requirements of the APE (Protection Profile Evaluation) assurance class of the Common Criteria for information Security Evaluation in relation to PP Information Gateway. This report describes the evaluation results and its soundness and confirmity.

The TOE (TOE is the product described in the PP) is a content filtering device for IP and TCP/UDP traffic between networks.

The TOE is a stand-alone device consisting of hard- and software. The external entities, Log System and Administration Node, are required as to provide support for reception of audit trails from the TOE and to supply an administration interface to the TOE. Neither the log system nor the Administration Node is part of the TOE.

The TOE has four external interfaces:

- Two network interfaces,
- One administration interface to an Administration Node, and
- One Log System interface to an external system for audit trail management.

All external interfaces are Ethernet (IEEE 802.3) compatible. The network interfaces communicate with TCP/IP or UDP/IP (IPv4/IPv6).

There are eight assumptions made in the PP regarding the secure usage and environment of the Information Gateway. The TOE only relies on these being met to counter the six threats, and to fulfill the five organizational security policies (OSP) in the PP. The assumptions, the threats and the organizational security policies are described in chapter 4 in [PP].

The TOE has 30 different Security Function Requirements addressed in the PP within the functional classes. Authentication of users, Non-repudiation within Communications, Encryption of sensitive data, User access control of data with flow control functions, User Authentication and Identification, Security Management functions for the TOE, roles and certificates and finally the protection of the TOE Security Functions that protects the TSF itself.

The Evaluation on the PP Information Gateway was conducted by atsec information security AB and completed on November 14, 2011. Contents of this report have prepared on the basis of the contents of the ETR submitted by atsec information security AB. The evaluation was conducted by applying CEM. This PP satisfies all APE requirements of the Common Criteria, therefore the evaluation results were decided to be suitable.

3 Security Related Qualities

Security Policy

Audit, Audit Transfer, Domain Separation, PKI and Query TOE Status is summarized in [PP] section 3.3, Organizational Security Polices.

Assumptions

Dependencies upon the environment for secure operation of the TOE are described in [PP] section 4.3, Security Objectives for the Operational environment.

Clarification of Scope

Neither the log system nor the Administration Node is part of the TOE. Further details in [PP] section 1.2.8, Available non-TOE hardware/software/firmware.

Architectural Information

The TOE is divided into three separated nodes, two Service Nodes interfacing one network each and a Filter Node interfacing the Service Nodes. User data to be transferred from one network to the other has to pass all three nodes. The Service Nodes are able to receive and format data from the connected networks to an intermediary format that is suitable for control and filtering in the filtering node.
For further details in [PP] section 1.2.2, TOE components.

4 Evaluation Results

Assurance Class 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 classes, the final evaluation result in PASS.

5 Acronyms

The following acronyms have been used in this report.

EAL	Evaluation Assurance Level
TOE	Target of Evaluation
ITSEF	IT security Evaluation Facility
PP	Protection Profile
CC	Common Criteria
CEM	Common Methodology for Information Security Evaluation

6 References

Acronym	Documents used and referenced during the review
PP	Protection Profile Information Gateway v2.0, 2011-11-07, 10FMV8575-24:1
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