National Information Assurance Partnership
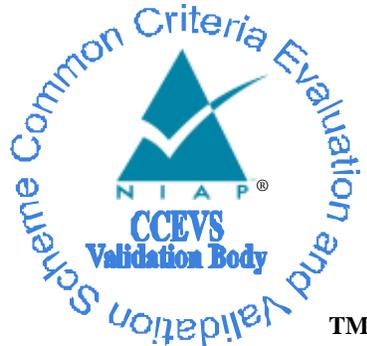

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

IEEE

IEEE 2600.1-2009

Report Number: CCEVS-VR-10340

Dated: 2009-06-09

Version: 2.0

ACKNOWLEDGEMENTS

Validation Team

Mario Tinto

atsec Information Security Corporation

Austin, TX

Table of Contents

1.   EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the evaluation of the IEEE 2600.1-2009 Protection Profile for Hardcopy Devices, Operational Environment A. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by the atsec Information Security Corporation, and was completed during June 2009. atsec Information Security Corporation is an approved NIAP Common Criteria Testing Laboratory (CCTL). The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by the CCTL. The evaluation determined the product to be **compliant to the Protection Profile security assurance requirements of the assurance class APE**.

Standard for a Protection Profile for Hardcopy Devices in a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance, are required. Typical information processed in this environment is trade secret, mission-critical, or subject to legal and regulatory considerations such as for privacy or governance. This environment is not intended to support life-critical or national security applications. This environment will be known as "Operational Environment A."

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 4, and the Conclusions presented in Section 5, of the ETR. The validation team therefore concludes that the evaluation (and its PASS result) for the Protection Profile is complete and correct.

2.   IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) 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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation granted by the National Institute of Standards and Technology (NIST).

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product
- The Protection Profile to which the product is conformant
- The conformance result of the evaluation
- The organizations and individuals participating in the evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	N/A
Protection Profile	IEEE 2600.1-2009
Security Target	N/A
Evaluation Technical Report	*Evaluation Technical Report for a Protection Profile Evaluation: IEEE 2600.1-2009*
Conformance Result	Compliant with APE assurance class
Sponsor	IEEE, Inc.
Developer	IEEE, Inc.
Evaluators	atsec information security corporation
Validators	Mario Tinto

3. SECURITY POLICY

N/A

4. ASSUMPTIONS

4.1. Usage Assumptions

Although there are several assumptions stated in the Protection Profile, the primary conditions are that:

- The TOE is located within monitored facilities and is protected from unmanaged physical access
- Administrators are assumed to be trustworthy

4.2. Clarification of Scope

The Protection Profile covers hard-copy devices with their software and hardware.

5.   ARCHITECTURAL INFORMATION

This Protection Profile explicitly does not mandate any specific architecture.

6.   DOCUMENTATION

N/A

7.   IT PRODUCT TESTING

N/A

8.   EVALUATED CONFIGURATION

N/A

9.   RESULTS OF THE EVALUATION

The evaluation team determined the Protection Profile to be **compliant to the Protection Profile security assurance requirements of the assurance class APE**.

10.   VALIDATOR COMMENTS

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, CEM, and CCEVS practices.

11.   PROTECTION PROFILE

The PP, IEEE Protection Profile for Hardcopy Devices, Operational Environment A, Version 41c is included here by reference.

12. LIST OF ACRYONYMS

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13.   BIBLIOGRAPHY

[1]   Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1.

[2]   Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1.

[3]   Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1.

[4]   Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, Version 3.1.

[5]   Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 3.1.