

IEEE Standard for a Protection Profile in Operational Environment A

IEEE Computer Society

Sponsored by the
Information Assurance Committee

2600.1™

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

12 June 2009

IEEE Std 2600.1™-2009

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

IEEE Standard for a Protection Profile in Operational Environment A

Sponsor

Information Assurance Committee

of the

IEEE Computer Society

Approved 13 May 2009

IEEE-SA Standards Board

Common Criteria Protection Profile information:

PP Identification: IEEE Std 2600.1-2009
PP Registration: CCEVS-VR-VID10340-2009
Version: 1.0
Date: June 2009
Author: Hardcopy Device and System Security Working Group
Sponsor: IEEE Computer Society Information Assurance (C/IA) Committee
Common Criteria Scheme: US (CCEVS – Common Criteria Evaluation and Validation Scheme)
Common Criteria Testing Lab: atsec information security
Common Criteria conformance: Version 3.1, Revision 2, Part 2 extended and Part 3 conformant
Assurance level: EAL 3 augmented by ALC_FLR.2

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

© 2009 IEEE. Copyright claimed in Clauses 10, 11, 13-17, and 19, exclusive of text from Common Criteria Part 2, Version 3.1, and in Annexes A and B, exclusive of text from Common Criteria Part 1, Version 3.1.

Abstract: This standard is 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.”

Keywords: all-in-one, Common Criteria, copier, disk overwrite, document, document server, document storage and retrieval, facsimile, fax, hardcopy, ISO/IEC 15408, multifunction device (MFD), multifunction product (MFP), network, network interface, nonvolatile storage, office, paper, printer, Protection Profile, residual data, scanner, security target, shared communications medium, temporary data

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 12 June 2009. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-5986-7 STD95938
Print: ISBN 978-0-7381-5987-4 STDPD95938

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

Introduction

This introduction is not part of IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A.

This document is a standard for a Common Criteria Protection Profile for Hardcopy Devices. It is intended to be used by manufacturers of Hardcopy Devices to write conformant Security Target documents for Common Criteria certification of their hardcopy device products. It may also be used to write conformant Protection Profiles for Hardcopy Devices.

This standard is related to IEEE Std 2600™-2008. IEEE Std 2600-2008 is a more general standard for hardcopy device security and contains a large amount of content that is beyond the scope of or is otherwise inappropriate for a Common Criteria Protection Profile. The two standards are related by way of the compliance clause of IEEE Std 2600-2008. With some well-defined exceptions, 8.1.1 of IEEE Std 2600-2008 contains Security Objectives that are technically consistent with the Security Objectives (APE_OBJ) clause of this document. The exceptions to this consistency between IEEE Std 2600-2008 and this standard are distinguished by the use of the word "should" instead of "shall" in IEEE Std 2600-2008 and the absence of those objectives in this standard.

For more information

Further information, including the status and updates of this standard can be found on the Internet at http://grouper.ieee.org/groups/2600/.

Comments or questions regarding this document should be directed to stds-2600-1@ieee.org. The comments should include the title of the document, the page, section, and paragraph numbers, and a detailed comment or recommendation.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

amendments, corrigenda, or errata, visit the IEEE Standards Association Web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this draft standard may require use of subject matter covered by patent rights. By publication of this draft standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this draft standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board, the Hardcopy Device and System Security Working Group had the following membership:

Don Wright, *Chair*
Lee Farrell, *Vice-chair*
Brian Smithson, *Secretary and Lead Editor*
Carmen Aubry, Nancy Chen, Ron Nevo, and **Alan Sukert,** *Editors*

Shah Bhatti
Peter Cybuck
Nick Del Re
Satoshi Fujitani
Tom Haapanen
Akihiko Iwasaki
Harry Lewis
Takanori Masui
Yusuke Ohta
Ken Ota
Glen Petrie
Jerry Thrasher
Hiroki Uchiyama
Shigeru Ueda
Brian Volkoff
Bill Wagner
Sameer Yami

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Carmen Aubry
Matthew Ball
Ying Chen
Keith Chow
Paul Croll
Geoffrey Darnton
Russell Dietz
Lee Farrell
Randall Groves
Mark Henley
Werner Hoelzl
Raj Jain
Piotr Karocki
G. Luri
Michael S. Newman
Nick Del Re
Stephen Schwarm
Steven Smith
Brian Smithson
Thomas Starai
Jerry Thrasher
Thomas Tullia
Paul Work
Forrest Wright
Sameer Yami

Acknowledgments

The following companies have agreed to make financial contributions to underwrite the cost of Common Criteria certification of some or all of the IEEE Std 2600-series Protection Profiles:

Canon
Fuji-Xerox
HP
InfoPrint Solutions
Konica Minolta
Kyocera-Mita
Lexmark
Océ
Oki Data
Ricoh
Samsung
Sharp
Toshiba
Xerox

When the IEEE-SA Standards Board approved this standard on 13 May 2009, it had the following membership:

Robert M. Grow, *Chair*
Tom A. Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

John Barr
Karen Bartelson
Victor Berman
Ted Burse
Richard DeBlasio
Andrew Drozd
Mark Epstein
Alexander Gelman
James Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Ted Olsen
Glenn Parsons
Ronald C. Petersen
Narayanan Ramachandran
Jon Walter Rosdahl
Sam Sciacca
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*

Michael Janezic, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Michael D. Kipness
IEEE Standards Program Manager, Technical Program Development

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

Contents

1. Overview 1

1.1 Scope 1
1.2 Purpose 1
1.3 Application notes 1
1.4 Notational conventions 2

2. Normative references 2

3. Protection Profile introduction (APE_INT) 3

3.1 Protection Profile usage 3
3.2 Protection Profile reference 3

4. Hardcopy Device overview (APE_INT) 3

4.1 Typical products 3
4.2 Typical usage 4

5. TOE overview (APE_INT) 4

5.1 TOE functions 4
5.2 TOE model 5
5.3 Entity definitions 6
5.4 TOE operational model 8

6. Conformance claims (APE_CCL) 9

6.1 Conformance to Common Criteria 9
6.2 Conformance to other Protection Profiles 9
6.3 Conformance to Packages 9
6.4 Conformance to this Protection Profile 9

7. Security Problem Definition (APE_SPD) 10

7.1 Threats agents 10
7.2 Threats to TOE Assets 10
7.3 Organizational Security Policies for the TOE 10
7.4 Assumptions 11

8. Security Objectives (APE_OBJ) 11

8.1 Security Objectives for the TOE 11
8.2 Security Objectives for the IT environment 11
8.3 Security Objectives for the non-IT environment 12
8.4 Security Objectives rationale 12

9. Extended components definition (APE_ECD) 15

9.1 FPT_CIP_EXP Confidentiality and integrity of stored data 15
9.2 FPT_FDI_EXP Restricted forwarding of data to external interfaces 17

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

10. Common Security Functional Requirements (APE_REQ) 18

10.1 Class FAU: Security audit 18
10.2 Class FCO: Communication 20
10.3 Class FCS: Cryptographic support 20
10.4 Class FDP: User data protection 20
10.5 Class FIA: Identification and authentication 23
10.6 Class FMT: Security management 25
10.7 Class FPR: Privacy 28
10.8 Class FPT: Protection of the TSF 28
10.9 Class FRU: Resource utilization 29
10.10 Class FTA: TOE access 29
10.11 Class FTP: Trusted paths/channels 29
10.12 Common security requirements rationale 29

11. Security assurance requirements (APE_REQ) 32

12. SFR Packages introduction 33

12.1 SFR Packages usage 33
12.2 SFR Packages reference 33
12.3 SFR Package functions 35
12.4 SFR Package attributes 35

13. 2600.1-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment A 35

13.1 PRT SFR Package introduction 35
13.2 Class FDP: User data protection 36
13.3 PRT security requirements rationale 37

14. 2600.1-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment A 37

14.1 SCN SFR package introduction 37
14.2 Class FDP: User data protection 37
14.3 SCN security requirements rationale 39

15. 2600.1-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment A 39

15.1 CPY SFR package introduction 39
15.2 Class FDP: User data protection 39
15.3 CPY security requirements rationale 40

16. 2600.1-FAX SFR Package for Hardcopy Device Fax Functions, Operational Environment A 41

16.1 FAX SFR package introduction 41
16.2 Class FDP: User data protection 41
16.3 FAX security requirements rationale 43

17. 2600.1-DSR SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A 43

17.1 DSR SFR package introduction 43
17.2 Class FDP: User data protection 43
17.3 DSR security requirements rationale 45

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

18. 2600.1-NVS SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A 45

18.1 NVS SFR package introduction 45
18.2 Class FPT: Protection of the TSF 46
18.3 NVS security requirements rationale 46

19. 2600.1-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A 47

19.1 SMI SFR package introduction 47
19.2 Class FAU: Security audit 47
19.3 Class FPT: Protection of the TSF 48
19.4 Class FTP: Trusted paths/channels 48
19.5 SMI security requirements rationale 49

Annex A (normative) Glossary 50

Annex B (normative) Acronyms 53

Annex C (informative) Bibliography 54

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.

IEEE Standard for a Protection Profile in Operational Environment A

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

This standard is 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. The 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."

1.2 Purpose

The purpose of this standard is to create a security Protection Profile (PP) for Hardcopy Devices in Operational Environment A as defined in IEEE Std 2600™-2008.

1.3 Application notes

Application notes are provided where they may contribute to the reader's understanding. These notes, while not part of the formal statement of this Protection Profile, are included as an acknowledgment of the diverse uses of this document and are intended to provide guidance to its users.

Copyright © 2009 IEEE. All rights reserved.

Authorized licensed use limited to: Thomson Techstreet. Downloaded on August 30, 2009 at 14:09 from IEEE Xplore. Restrictions apply.