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

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

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

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

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

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

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

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

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

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

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

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

IEEE Standard for a Protection Profile in Operational Environment A

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.

1.4 Notational conventions

The following notational conventions are used throughout this standard:

a) Defined terms in full form are set in title case (for example, "Document Storage and Retrieval").

b) Defined terms in abbreviated form are set in all caps (for example, "DSR").

c) In tables that describe Security Objectives rationale, a checkmark ("✓") placed at the intersection of a row and column indicates that the threat identified in that row is wholly or partially mitigated by the objective in that column.

d) In tables that describe completeness of security requirements, a **bold** typeface letter "P" placed at the intersection of a row and column indicates that the requirement identified in that row performs a principal fulfillment of the objective indicated in that column. A letter "S" in such an intersection indicates that it performs a supporting fulfillment.

e) In tables that describe the sufficiency of security requirements, a **bold** typeface requirement name and purpose indicates that the requirement performs a principal fulfillment of the objective in the same row. Requirement names and purposes set in normal typeface indicate that those requirements perform supporting fulfillments.

f) In specifications of Security Functional Requirements (SFRs):

   1) **Bold** typeface indicates the portion of an SFR that has been completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition.

   2) *Italic* typeface indicates the portion of an SFR that must be completed by the ST Author in a conforming Security Target.

   3) ***Bold italic*** typeface indicates the portion of an SFR that has been partially completed or refined in this Protection Profile, relative to the original SFR definition in Common Criteria Part 2 or an Extended Component Definition, but which also must be completed by the ST Author in a conforming Security Target.

g) The following prefixes in Table 1 are used to indicate different entity types:

Table 1—Notational prefix conventions

Prefix	Type of entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security attribute

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2—Part 2: Security Functional Components.[1]

Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2—Part 3: Security Assurance Components.[2]

IEEE Std 2600™-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security.[3,4]

3. Protection Profile introduction (APE_INT)

3.1 Protection Profile usage

The class of Hardcopy Device (HCD) products encompasses a wide variety of functions and configurations, from small non-networked printers to large networked multifunction devices. To accommodate such a wide variety of products, this Standard for a Protection Profile is structured as a common Protection Profile that applies to all HCDs and a set of named Security Functional Requirements (SFR) packages that may apply to some HCD configurations.

To use this Standard for a Protection Profile, authors compose a Security Target (ST) or Protection Profile which conforms to the Protection Profile identified in 3.2 and which may need to conform to one or more of the SFR packages identified in 12.2. The formal conformance requirements are described in 6.4.

3.2 Protection Profile reference

Title: 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
Version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Sponsor: IEEE Computer Society Information Assurance (C/IA) Committee
Authors: IEEE Hardcopy Device and System Security Working Group
Keywords: Hardcopy, Paper, Document, Printer, Multifunction Device (MFD), Multifunction Product (MFP), All-In-One, Network, Office

PP APPLICATION NOTE 1. This Protection Profile defines two extended components for use in SFR Packages. If a TOE does not need to conform to those SFR Packages, then its ST is Part 2 conformant. Otherwise, a conforming ST is Part 2 extended.

4. Hardcopy Device overview (APE_INT)

4.1 Typical products

The Hardcopy Devices (HCDs) considered in this Protection Profile are used for the purpose of converting hardcopy documents into digital form (scanning), converting digital documents into hardcopy form (printing), transmitting hardcopy documents over telephone lines (faxing), or duplicating hardcopy

[1] Available from http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf.
[2] Available from http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf.
[3] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org).
[4] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

documents (copying). Hardcopy documents are commonly in paper form, but they can also take other forms such as positive or negative transparencies or film.

HCDs can be implemented in many different configurations, depending on their intended purpose or purposes. Simple devices have a single purpose implemented by a single function, such as a printer, scanner, copier, or fax machine. Other devices augment a single primary purpose with additional secondary functions, such as a fax machine that can also be used to make copies, or a copier that can also be used as a printer. Complex multifunction devices fulfill multiple purposes by using multiple functions in different combinations to perform the operations of several single-function devices.

Some HCDs have additional functions that enhance their capabilities, such as hard disk drives or other nonvolatile storage systems, document server functions, or mechanisms for manually or automatically updating the HCD's operating software. All HCDs considered in this Protection Profile are assumed to provide the capability for appropriately authorized users to manage the security features of the HCD.

4.2 Typical usage

HCDs can be used in a wide variety of environments, such as:

- Home use by consumers
- Home or office use by small businesses
- Office use by medium or large organizations
- Self-service use by the public in retail copy shops, libraries, business centers, or educational institutions
- Production use by commercial service providers

HCDs may contain or process valuable or sensitive assets that need to be protected from unauthorized disclosure and alteration. The utility of the device itself may be considered a valuable asset which also needs to be protected. There is also a need to ensure that the HCD cannot be misused in such a way that it causes harm to devices with which it shares network connections.

However, each environment may place a different value on those assets, make different assumptions about security-relevant factors such as physical security and administrator skill, face threats of differing approach and sophistication, and be subject to different external legal, regulatory, or policy requirements. It is not practical to fulfill one set of Security Objectives for all environments, and therefore, IEEE Std 2600-2008 has defined several environments that form the basis for several Protection Profile standards in the IEEE Std 2600 series. A complete description of those environments can be found in IEEE Std 2600-2008.

This Protection Profile and associated SFR Packages address the requirements of Operational Environment A. Operational Environment A is generally characterized as 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.

5. TOE overview (APE_INT)

5.1 TOE functions

To facilitate the creation of Security Targets or Protection Profiles that can be used for many types and configurations of HCDs, this standard is composed of a Protection Profile that describes the generic security problem, objectives, and security functional requirements of all HCDs, and a set of named SFR

Packages whose application depend upon the functions that are performed by a particular conforming Target of Evaluation. Examples of those functions are:

- Printing—producing a hardcopy document from its electronic form
- Scanning—producing an electronic document from its hardcopy form
- Copying—duplicating a hardcopy document
- Faxing—scanning documents in hardcopy form and transmitting them in electronic form over telephone lines and receiving documents in electronic form over telephone lines and printing them in hardcopy form
- Document storage and retrieval—storing an electronic document during one document processing job for access during one or more subsequent document processing jobs, and retrieving an electronic document that was stored during a previous document processing job
- Nonvolatile storage—persistent or temporary storage of User Data or TSF Data on a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel
- Shared-medium Interfaces—transmitting or receiving User Data or TSF Data between the HCD and external devices over communications media which, in conventional practice, is or can be simultaneously accessed by multiple users

These functions can be combined to represent a wide variety of complete Hardcopy Devices.

5.2 TOE model

The Target of Evaluation (TOE) is described using the standard Common Criteria terminology of Users, Subjects, Objects, Operations, and Interfaces. Two additional terms are introduced: Channel describes both data interfaces and hardcopy document input/output mechanisms, and TOE Owner is a person or organizational entity responsible for protecting TOE assets and establishing related security policies.

In the traditional Common Criteria model, Users bind with Subjects through Interfaces to perform Operations on Objects. In this Protection Profile, the distinction between Users and Subjects is not necessary because there is no generic need to distinguish between the security attributes of a User and those of a Subject for this class of IT products, and therefore, it can be assumed that the security attributes of a Subject used in access control decisions are identical to the security attributes of the User that requested access, unless a conforming Security Target or Protection Profile makes a distinction between User and Subjects in its TOE model.

In the traditional Common Criteria model, the TOE Security Functions (TSF) is a subset of the TOE. In this Protection Profile, the distinction between the TOE and TSF is not necessary, and therefore, it can be assumed that the TSF is equivalent to the TOE unless a conforming Security Target or Protection Profile makes a distinction between the TSF and the TOE in its TOE model.

Objects in this Protection Profile are data (which can be created, read, modified, or deleted) and functions (which can be executed). These objects and the communication among them have been defined abstractly so that they do not imply or require any particular architecture or implementation. It is anticipated that Security Target and Protection Profile authors will be able to use this model to describe most common HCD architectures and implementations.

The general TOE model is shown in Figure 1.

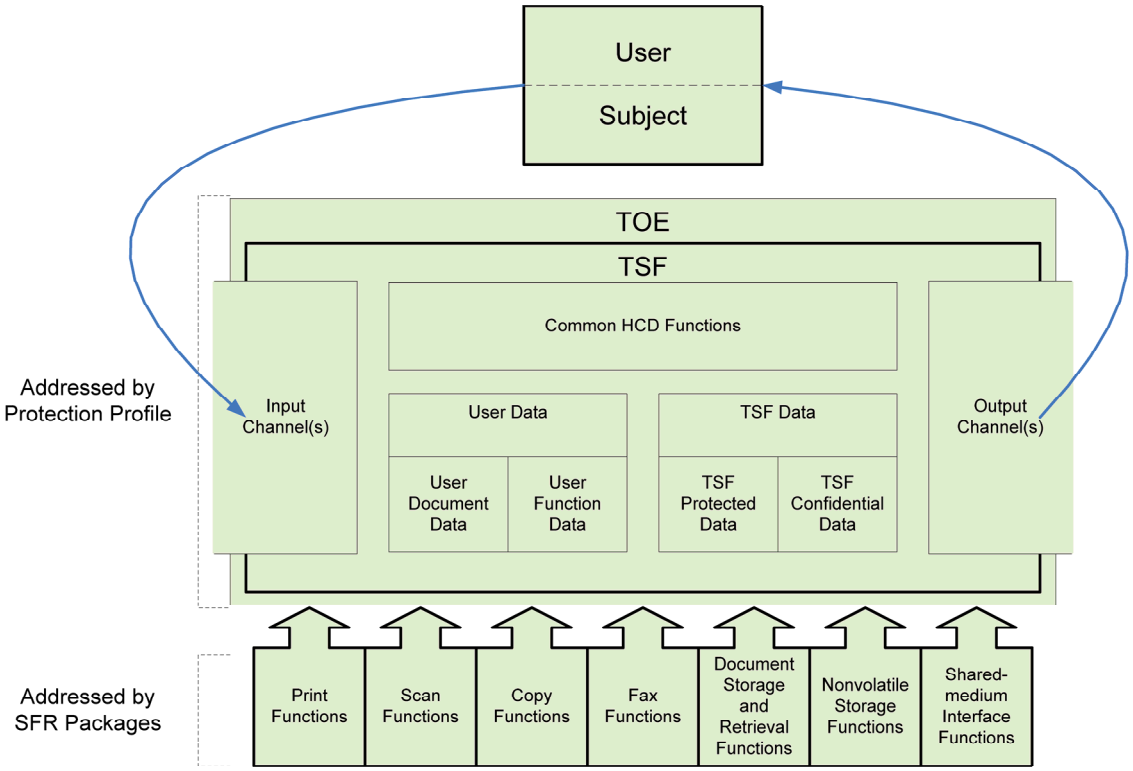


Figure 1—TOE model

PP APPLICATION NOTE 2. There may be cases where User Data and TSF Data are generated outside of the TOE and transmitted to the TOE, as well as cases where User Data and TSF Data are generated and/or processed by the TOE and exported from the TOE. In those cases, it is expected that sufficient security measures exist in the TOE environment that protect these data against unauthorized disclosure and modification. Optionally, the TOE can provide functionality to support this protection.

5.3 Entity definitions

5.3.1 Users

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrator.

Table 2—Users

Designation		Definition
U.USER		Any authorized User.
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

5.3.2 Objects (Assets)

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. In this Protection Profile, Objects are equivalent to TOE Assets. There are three types of Objects: User Data, TSF Data, and Functions.

5.3.2.1 User Data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two objects: User Document Data and User Function Data.

Table 3—User Data

Designation	Definition
D.DOC	User Document Data consist of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

5.3.2.2 TSF Data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data.

Table 4—TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

PP APPLICATION NOTE 3. It is required that ST Authors define the TSF Data assets for their TOEs, and to appropriately categorize those assets according to whether they require protection from unauthorized alteration or protection from both unauthorized disclosure and unauthorized alteration. Examples of some possible categorization of assets are shown in Table 5. These are intended only as examples and are not intended to imply categorization requirements or any requirements of architecture, function, or implementation for conforming products.

Table 5—Examples of TSF Data Categorization

Examples of TSF Protected Data	Examples of TSF Confidential Data
User and Administrator identification data	User and Administrator authentication data
Scan/fax/e-mail destination lists or address books	Credentials for accessing external devices (e.g., e-mail or file servers)
Job status logs	Job details and audit logs
Status of pending or stored jobs and documents	Access control lists
Device and network status information and configuration settings	Device and network management (e.g., Simple Network Management Protocol) authentication data
Device security status	Cryptographic keys

5.3.2.3 Functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. These functions are used by SFR Packages and are identified and defined in 12.3.

5.3.3 Operations

Operations are a specific type of action performed by a Subject on an Object. In this Protection Profile, five types of operations are considered: those that result in disclosure of information (Read), those that result in alteration of information (Create, Modify, Delete), and those that invoke a function (Execute).

5.3.4 Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE. In this Protection Profile, four types of Channels are allowed but not required in any particular conforming Security Target or Protection Profile:

Private-medium Interface: mechanisms for exchanging information that use (1) wired or wireless electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous Users; or (2) Operator Panel and displays that are part of the TOE. It is an input-output channel.

Shared-medium Interface: mechanisms for exchanging information that use wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple Users. It is an input-output channel.

Original Document Handler: mechanisms for transferring User Document Data into the TOE in hardcopy form. It is an input channel.

Hardcopy Output Handler: mechanisms for transferring User Document Data out of the TOE in hardcopy form. It is an output channel.

In practice, at least one input channel and one output channel would be present in any HCD configuration, and at least one of those channels would be either an Original Document Handler or a Hardcopy Output Handler.

5.4 TOE operational model

The TOE is composed of the essential input, output, storage, and processing elements required to perform one or more of the following document processing operations on User Document Data:

- Print a hardcopy document from a document source in electronic form
- Produce an electronic document from a document source in hardcopy form
- Duplicate a hardcopy document
- Transmit and receive facsimiles of hardcopy documents over a telephone line
- Store and retrieve an electronic document

User Function Data (e.g., job status) and TSF Data (e.g., job or audit logs) may be created or modified during the performance of these processes.

The TOE provides the essential elements required to configure the operation of the TOE and may also provide the essential elements required to manage TOE users.

The major security features of the TOE are:

a) All Users are identified and authenticated and are authorized before being granted permission to perform TOE functions.

b) Administrators authorize Users to use the functions of the TOE.

c) User Document Data are protected from unauthorized disclosure or alteration.

d) User Function Data are protected from unauthorized alteration.

e) TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.

f) TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.

g) Document processing and security-relevant system events are recorded, and such records are protected from disclosure or alteration by anyone except for authorized personnel.

6. Conformance claims (APE_CCL)

6.1 Conformance to Common Criteria

This Protection Profile is Common Criteria version 3.1 Revision 2 Part 2 extended and Part 3 conformant.

6.2 Conformance to other Protection Profiles

This Protection Profile is not based on any other Protection Profile.

6.3 Conformance to Packages

This Protection Profile conforms to Common Criteria Evaluation Assurance Level (EAL) 3 augmented by ALC_FLR.2.

6.4 Conformance to this Protection Profile

To claim conformance to this Protection Profile, the conforming Security Target or Protection Profile shall comply with all of the following three rules:

a) It shall claim demonstrable conformance to the Security Problem Definition (APE_SPD), Security Objectives (APE_OBJ), Extended Components Definitions (APE_ECD), and the Common Security Functional Requirements (APE_REQ) of this Protection Profile.

b) If its Target of Evaluation performs any of the functions defined in 12.3, then the Security Target or Protection Profile shall claim demonstrable conformance to the corresponding SFR Package(s) identified in 12.2 (in addition to the Common Security Functional Requirements (APE_REQ) of this Protection Profile).

c) Its Target of Evaluation shall perform at least one of the functions F.PRT, F.SCN, F.CPY, and F.FAX, as defined in 12.3, and claim compliance with the SFR package(s) associated with the function(s).

PP APPLICATION NOTE 4. The ST/PP Author should reference this Protection Profile and SFR Packages by the names defined in 3.2 and 12.2. For example, if an ST conforms to this Protection Profile and the SFR Packages for PRT (Print) and SMI (Shared-medium Interface) functions, then the ST Author would claim conformance to “2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A,” “2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A,” and “2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A.”

7. Security Problem Definition (APE_SPD)

7.1 Threats agents

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE.

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Protection Profile address the threats posed by these threat agents.

7.2 Threats to TOE Assets

This section describes threats to assets described in 5.3.2.

Table 6—Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 7—Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

7.3 Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 8—Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

7.4 Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Protection Profile are based on the condition that all of the assumptions described in this section are satisfied.

Table 9—Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

8. Security Objectives (APE_OBJ)

8.1 Security Objectives for the TOE

This section describes the Security Objectives that the TOE shall fulfill.

Table 10—Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.

8.2 Security Objectives for the IT environment

This section describes the Security Objectives that must be fulfilled by IT methods in the IT environment of the TOE.

Table 11— Security Objectives for the IT environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

PP APPLICATION NOTE 5. If the TOE provides an internal capability to provide access to audit records, then the ST Author should add appropriate objectives (e.g., O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED) and SFRs (e.g., FAU_SAR.1, FAU_SAR.2, FAU_STG.1, and FAU_STG.4) to the ST to describe that capability. Any internal capability for storing and providing access to audit records must perform an equivalent or more restrictive solution to that which is required by OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED.

PP APPLICATION NOTE 6. If both internal and external audit storage capabilities are provided, then the ST Author should express the internal and external capabilities as distinct modes of operation so that each can be evaluated.

8.3 Security Objectives for the non-IT environment

This section describes the Security Objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

Table 12—Security Objectives for the non-IT environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer's guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

8.4 Security Objectives rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 13—Completeness of Security Objectives

Threats. policies, and assumptions	Objectives																		
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYISCAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	✓						✓	✓											
T.DOC.ALT		✓					✓	✓											
T.FUNC.ALT			✓				✓	✓											
T.PROT.ALT				✓			✓	✓											
T.CONF.DIS					✓		✓	✓											
T.CONF.ALT						✓	✓	✓											
P.USER.AUTHORIZATION							✓	✓											
P.SOFTWARE.VERIFICATION									✓										
P.AUDIT.LOGGING										✓	✓	✓	✓						
P.INTERFACE.MANAGEMENT														✓		✓			
A.ACCESS.MANAGED															✓				
A.ADMIN.TRAINING																	✓		
A.ADMIN.TRUST																		✓	
A.USER.TRAINING																			✓

Table 14—Sufficiency of Security Objectives

Threats. policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE.	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.

P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events and prevents unauthorized disclosure or alteration.
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion, and modifications.
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures.	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

9. Extended components definition (APE_ECD)

This Protection Profile defines components that are extensions to Common Criteria 3.1 Revision 2, Part 2. These extended components are defined in the Protection Profile but are used in SFR Packages and, therefore, are employed only in TOEs whose STs conform to those SFR Packages.

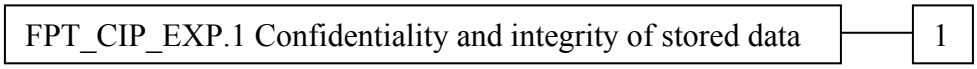
9.1 FPT_CIP_EXP Confidentiality and integrity of stored data

Family behaviour:

This family defines requirements for the TSF to protect the confidentiality and integrity of both TSF and user data.

Confidentiality and integrity of stored data is important security functionality in the case where the storage container is not, or not always, in a protected environment. Confidentiality and integrity of stored data is often provided by functionality that the TSF uses for both TSF and user data in the same way. Examples are full disk encryption functions, where the TSF stores its own data as well as user data on the same disk. Especially when a disk is intended to be removable and therefore may be transported into an unprotected environment, this becomes a very important functionality to achieve the Security Objectives of protection against unauthorized access to information.

Component leveling:



FPT_CIP_EXP.1 Confidentiality and integrity of stored data provides for the protection of user and TSF data stored on a storage container that cannot be assumed to be protected by the TOE environment.

Management: FPT_CIP_EXP.1

The following actions could be considered for the management functions in FMT:

a) Management of the conditions under which the protection function is activated or used

b) Management of potential restrictions on the allowance to use this function

Audit: FPT_CIP_EXP.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

a) Basic: failure condition that prohibits the function to work properly and detected attempts to bypass this functionality (e.g., detected modifications)

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: *media used to store the data*].

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs [assignment: *list of actions*] when it detects alteration of user and TSF data when either is written to [assignment: *media used to store the data*].

Rationale:

The Common Criteria defines the protection of user data in its FDP class and the protection of TSF data in its FPT class. Although both classes contain components that define confidentiality protection and integrity protection, those components are defined differently for user data and TSF data and, therefore, are difficult to use in cases where a TOE provides functionality for the confidentiality and integrity for both types of data in an identical way.

This Protection Profile defines an extended component that combines the confidentiality and integrity protection for both types of data in a single component. The authors of this Protection Profile view this as an approach that simplifies the statement of security functional requirements significantly and therefore enhances the readability and applicability of this Protection Profile. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or FPT class. Since it is intended to protect data that are exported to storage media, and in particular, storage media that might be removable from the TOE, the authors believed that it was most

appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

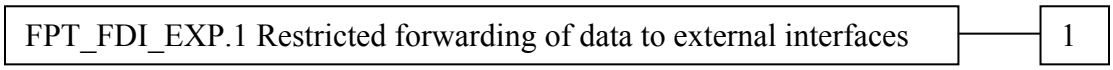
9.2 FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:



FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be allowed by an administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: **No other components**

Dependencies: **FMT_SMF.1 Specification of Management Functions**
FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

10. Common Security Functional Requirements (APE_REQ)

This clause defines the common security functional requirements for the TOE.

10.1 Class FAU: Security audit

PP APPLICATION NOTE 7. If the TOE provides an internal capability to store and provide access to audit records, then the ST Author should add appropriate SFRs (e.g., FAU_SAR.1, FAU_SAR.2, FAU_STG.1, and FAU_STG.4) to the ST, fulfilling any added objectives (see PP APPLICATION NOTE 5 in 8.2), to describe that capability. Any internal capability for storing and providing access to audit records must perform an equivalent or more restrictive solution to that which is required by OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED.

PP APPLICATION NOTE 8. If both internal and external audit storage capabilities are provided, then the ST Author should express the internal and external capabilities as distinct modes of operation so that each can be evaluated.

PP APPLICATION NOTE 9. Additional audit requirements and recommendations may exist in SFR Packages to which a Security Target conforms. Such requirements and recommendations do no supersede the requirements and recommendations in this clause.

FAU_GEN.1 Audit data generation

Hierarchical to: **No other components**

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

— Start-up and shutdown of the audit functions; and

— All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

— **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 15;** [assignment: *other specifically defined auditable events*]

PP APPLICATION NOTE 10. If the ST Author specifies one of the Common Criteria defined audit levels (minimum, basic, or detailed), there may be some conflict among the requirements of that audit level and the requirements listed in Table 15. The ST shall specify the greater of those requirements.

PP APPLICATION NOTE 11. Table 16 lists additional auditable events that are recommended for consideration in FAU_GEN.1.1 in addition to those that are required by Table 15 and by any audit level specified in FAU_GEN.1.1.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

— Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

— For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 15: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*]

Table 15—Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Changes to the time	FPT_STM.1	Minimum	None required
Locking of an interactive session by the session locking mechanism	FTA_SSL.3	Minimum	None required

PP APPLICATION NOTE 12. Table 16 lists additional audit information that is recommended for consideration in FAU_GEN.1.2 in addition to those that are required by Table 15 and by any audit level specified in FAU_GEN.1.1.

Table 16—Audit data recommendations

Auditable event	Relevant SFR	Audit level	Additional information
Job initiation	FDP_ACF.1	Not specified	Type of job

FAU_GEN.1 is a principal SFR to fulfill O.AUDIT.LOGGED and is a dependency of FAU_GEN.2.

FAU_GEN.1 performs audit functions that are recommended for FDP_ACF.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1, FPT_STM.1, and FTA_SSL.3.

FAU_GEN.2 User identity association

Hierarchical to: **No other components**

Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

PP APPLICATION NOTE 13. FAU_GEN.2 is a principal SFR to fulfill O.AUDIT.LOGGED.

PP APPLICATION NOTE 14. FAU_GEN.2 performs audit functions that are recommended for FDP_ACF.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1, FPT_STM.1, and FTA_SSL.3.

10.2 Class FCO: Communication

There are no Class FCO security functional requirements for this Protection Profile.

10.3 Class FCS: Cryptographic support

There are no Class FCS security functional requirements for this Protection Profile.

10.4 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 17 is referenced by the Class FDP SFRs in this clause.

Table 17—Common Access Control SFP

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	attributes from Table 22; see PP APPLICATION NOTE 15	Delete	U.NORMAL	Denied, except for his/her own documents
D.FUNC	attributes from Table 22; see PP APPLICATION NOTE 15	Modify; Delete	U.NORMAL	Denied, except for his/her own function data

PP APPLICATION NOTE 15. These access control rules apply to the specified object if it has any of the attributes listed in Table 22 that are associated with a document processing job. The set of potentially applicable attributes depends on the SFR Packages listed in 12.2 to which a Security Target conforms.

PP APPLICATION NOTE 16. A document is "owned" by a User if that document was created or submitted to the TOE by that User, unless indicated otherwise in one of the named SFR Packages in this standard.

PP APPLICATION NOTE 17. Access control rules for the "Create" Operation are not specified because typically, any authorized U.NORMAL can create his/her own documents and cannot create documents that are owned by another User. The ST Author should consider adding appropriate rules for a conforming TOE.

PP APPLICATION NOTE 18. Conformance to one or more of the named SFR Packages in this standard may expand the rules by adding access controls for additional objects, security attributes, or roles. The User Data access control SFP for a conforming Security Target or Protection Profile is composed of rules defined in Table 17, plus the rules defined in access control SFPs that have been included by conformance with SFR packages.

PP APPLICATION NOTE 19. An ST Author may refine these rules by adding additional security attributes or additional roles, provided that such refinements do not violate the access control policy composed of rules

defined in Table 17 and those defined in all SFPs that have been included by conformance with SFR Packages.

PP APPLICATION NOTE 20. An ST Author may define additional objects and access control rules for those objects as long as this does not violate the access control policy composed of rules defined in Table 17 and those defined in all SFPs that have been included by conformance with SFR Packages.

FDP_ACC.1(a) Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17** on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 17.**

PP APPLICATION NOTE 21. FDP_ACC.1(a) is a principal SFR to fulfill O.DOC.NO_DIS, O.DOC.NO_ALT, and O.FUNC.NO_ALT, and is a dependency of FDP_ACF.1(a) and FMT_MSA.1(a).

FDP_ACC.1(b) Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** on **users as subjects, TOE functions as objects, and the right to use the functions as operations**.

PP APPLICATION NOTE 22. The TOE Function Access Control SFP is composed of the following SFRs: FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b).

PP APPLICATION NOTE 23. The TOE Function Access Control SFP is an access control policy that determines if a Normal User is allowed to use the functions that the TOE offers. The allowed functions are those defined in 12.3 of this standard. The ST Author should include all of the functions that are provided by a conforming TOE. The rules that determine access may be the same or may be different for each function. Such rules are defined in FDP_ACF.1(b).

PP APPLICATION NOTE 24. The TOE Function Access Control SFP may be defined as a policy between users and objects, or between or subjects and objects, depending on if the TOE architecture defines an intermediate subject and specific rules that determine the security attributes of the subject during user-subject binding.

PP APPLICATION NOTE 25. FDP_ACC.1(b) is a principal SFR to fulfill O.USER.AUTHORIZED, and is a dependency of FDP_ACF.1(b) and FMT_MSA.1(b).

FDP_ACF.1(a) Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 17, and for each, the indicated security attributes in Table 17**.

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 17 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 26. FDP_ACF.1(a) is a dependency of FDP_ACC.1(a).

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** to objects based on the following: **users and [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]**.

PP APPLICATION NOTE 27. The TOE Function Access Control SFP is composed of the following SFRs: FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b).

PP APPLICATION NOTE 28. The list of functions should include all of the functions offered by the TOE in the packages. The security attributes may be as simple as an access list assigned to each user indicating the functions the user is allowed to use or an access list assigned to each function indicating the users that are allowed to use the function.

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]**.

PP APPLICATION NOTE 29. This element allows defining the rule that is evaluated to determine if a user is allowed to use a specific function. Depending on which combination of selections are made, the ST Author may specify that all functions are automatically permitted for authorized users, some functions require explicit authorization, all functions require explicit authorization, or permissions are based on other stated conditions.

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **the user acts in the role U.ADMINISTRATOR**: [assignment: ***other*** *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules based on security attributes that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 30. FDP_ACF.1(b) is used to describe the rules that determine if a user is allowed to use a specific function the TOE offers. This PP does not prescribe the rules that determine a user's right to use a function. The author of an ST compliant to this PP may define access control rules common for all functions (in the simplest case, allowing all functions for any user authorized to use the TOE or setting a user

security attribute by an authorized administrator that defines the functions a user is allowed to use), but it also allows for the definition of more complex, function specific rules.

PP APPLICATION NOTE 31. FDP_ACF.1(b) is a dependency of FDP_ACC.1(b).

FDP_RIP.1 Subset residual information protection

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC**, [assignment: *list of objects*].

PP APPLICATION NOTE 32. FDP_RIP.1 is a principal SFR to fulfill O.DOC.NO_DIS.

10.5 Class FIA: Identification and authentication

FIA_ATD.1 User attribute definition

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

PP APPLICATION NOTE 33. FIA_ATD.1 is a dependency of FIA_USB.1.

FIA_UAU.1 Timing of authentication

Hierarchical to: **No other components**

Dependencies: **FIA_UID.1 Timing of identification**

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is authenticated.

PP APPLICATION NOTE 34. If certain functions are desired in the ST's Target of Evaluation which do not require user identification and authorization (e.g., displaying a list of user names at the beginning of the login process), the ST Author should consider allowing the necessary TSF-mediated actions in FIA_UAU.1.1 and FIA_UID.1.1. Such allowances should not be used to circumvent the intended TOE Function Access Control SFP.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

PP APPLICATION NOTE 35. User authentication may be performed internally by the TOE or externally by a trusted IT product in the IT environment.

PP APPLICATION NOTE 36. If user authentication is performed internally, then the ST Author should add appropriate SFRs for authentication handling (e.g., FIA_AFL.1 and FIA_UAU.7).

PP APPLICATION NOTE 37. If user authentication can be performed internally or externally, then the ST Author should express internal authentication and external authentication as distinct modes of operation so that each can be evaluated.

PP APPLICATION NOTE 38. FIA_UAU.1 is a principal SFR to fulfill O.USER.AUTHORIZED and O.INTERFACE.MANAGED.

FIA_UID.1 Timing of identification

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

PP APPLICATION NOTE 39. If certain functions are desired in the ST's Target of Evaluation which do not require user identification and authorization (e.g., displaying a list of usernames at the beginning of the login process), the ST Author should consider allowing the necessary TSF-mediated actions in FIA_UAU.1.1 and FIA_UID.1.1. Such allowances should not be used to circumvent the intended TOE Function Access Control SFP.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

PP APPLICATION NOTE 40. User identification may be performed internally by the TOE or externally by a trusted IT product in the IT environment.

PP APPLICATION NOTE 41. If user identification can be performed internally or externally, then the ST Author should express internal identification and external identification as distinct modes of operation so that each can be evaluated.

PP APPLICATION NOTE 42. FIA_UID.1 is a principal SFR to fulfill O.USER.AUTHORIZED and O.INTERFACE.MANAGED and is a dependency of FIA_UAU.1, FAU_GEN.2, and FMT_SMR.1.

FIA_USB.1 User-subject binding

Hierarchical to: **No other components**

Dependencies: **FIA_ATD.1 User attribute definition**

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].

PP APPLICATION NOTE 43. By default, this Protection Profile assumes that there is no difference between Users and Subjects. See 5.2 for more information.

PP APPLICATION NOTE 44. FIA_USB.1 is a principal SFR to fulfill O.USER.AUTHORIZED.

10.6 Class FMT: Security management

PP APPLICATION NOTE 45. In this Protection Profile, TSF Data have been defined in a general way so as not to imply or require any particular architecture, design, or implementation. The ST Author should identify the specific data that comprise D.CONF and D.PROT in the Target of Evaluation (see also PP APPLICATION NOTE 3 in 5.3.2.2) and define how those data are initialized and managed by iterating and refining FMT_MSA.1(a), FMT_MSA.3(a), FMT_MTD.1(a), and FMT_MTD.1(b).

FMT_MSA.1(a) Management of security attributes

Hierarchical to: **No other components**

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

PP APPLICATION NOTE 46. This Protection Profile does not define any mandatory security attributes, but some may be defined by SFR packages or by the ST Author. The ST Author should define how security attributes are managed. Note that this Protection Profile allows the ST Author to instantiate "Nobody" as an authorized identified role, which makes it possible for the ST Author to state that some management actions (e.g., deleting a security attribute) may not be performed by any User.

PP APPLICATION NOTE 47. FMT_MSA.1(a) is a dependency of FMT_MSA.3(a).

PP APPLICATION NOTE 48. FMT_MSA.1(a) performs management functions that are recommended for FDP_ACF.1(a).

FMT_MSA.1(b) Management of security attributes

Hierarchical to: **No other components**

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

PP APPLICATION NOTE 49. This Protection Profile does not define any mandatory security attributes, but some may be defined by the ST Author. The security attribute(s) that need to be instantiated in this SFR are those used in the access control rules defined in FDP_ACF.1(b). They may be as simple as a list defined per user indicating the functions a user is allowed to use or a list defined per function indicating the users that are allowed to use the function. In the case of complex rules that evaluate more than one security attribute, an ST Author should check if all those security attributes are managed by the same role. If not, he may need to add additional instantiations of FMT_MSA.1(b) for the different security attributes.

PP APPLICATION NOTE 50. If the TOE function access control policy does not allow any body to change a user's ability to execute a function, "Nobody" needs to be instantiated for "the authorized identified roles."

PP APPLICATION NOTE 51. The TOE Function Access Control SFP is composed of the following SFRs: FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b).

PP APPLICATION NOTE 52. FMT_MSA.1(b) is a dependency of FMT_MSA.3(b).

PP APPLICATION NOTE 53. FMT_MSA.1(b) performs management functions that are recommended for FDP_ACF.1(b).

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: **No other components**

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

PP APPLICATION NOTE 54. User and object security attributes are usually initialized when the user or object is created. This Protection Profile does not restrict the way security attributes are initialized, and therefore, the ST Author should describe the policies for security attribute initialization.

PP APPLICATION NOTE 55. FMT_MSA.3(a) is a dependency of FDP_ACF.1(a).

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: **No other components**

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3.1(b) The TSF shall enforce the **TOE Function Access Control Policy**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

PP APPLICATION NOTE 56. The TOE Function Access Control SFP is composed of the following SFRs: FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b).

PP APPLICATION NOTE 57. This SFR is used to define the default values for the access to TOE function assigned to a user when that user is defined. If those default values can be modified by an administrative role, then the role that is allowed to perform this modification should be defined in FMT_MSA.3.2(b). If the default values cannot be modified, then "Nobody" should be instantiated in FMT_MSA.3.2(b) to indicate that the default values are fixed. If the default values are different for each function subject to the access control

policy, this may be expressed in the assignment in FMT_MSA.3.1(b) where the ST Author may define the default values individually for each function.

PP APPLICATION NOTE 58. FMT_MSA.3(b) is a dependency of FDP_ACF.1(b).

FMT_MTD.1 Management of TSF data

Hierarchical to: **No other components**

Dependencies: **FMT_SMR.1 Security roles**
FMT_SMF.1 Specification of Management Functions

PP APPLICATION NOTE 59. In the iterations of FMT_MTD.1.1 below, (a) may be used for TSF Data that are not associated with a Normal User to indicate whether it can be managed by an authorized administrative role or by Nobody, and (b) may be used for TSF Data that are associated with a Normal User, or associated with documents or jobs owned by a Normal User, to indicate whether it can be managed by an authorized administrative role, by that Normal User, or by Nobody.

FMT_MTD.1.1(a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*,** [assignment: *the authorized identified roles* ***except U.NORMAL***]**]]**.

FMT_MTD.1.1(b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data* ***associated with a U.NORMAL or TSF data associated with documents or jobs owned by a U.NORMAL***] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated*]]**.

PP APPLICATION NOTE 60. FMT_MTD.1(a) and FMT_MTD.1(b) are principal SFRs to fulfill O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

PP APPLICATION NOTE 61. The management functions listed in Table 18 are recommended for consideration in FMT_SMF.1. The ST Author should consider specifying other management functions that support administrative functionality of the ST Target of Evaluation.

Table 18—Management function recommendations

Management function	Relevant SFR
Management of the user identities	FIA_UID.1
Management of system time	FPT_STM.1

PP APPLICATION NOTE 62. FMT_SMF.1 is a dependency of FMT_MSA.1 and FMT_MTD.1.

PP APPLICATION NOTE 63. FMT_SMF.1 may perform management functions that are recommended for FIA_UID.1 and FPT_STM.1.

FMT_SMR.1 Security roles

Hierarchical to: **No other components**

Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].

PP APPLICATION NOTE 64. The role "Nobody" cannot be assigned to any user. It is included in FMT_SMR.1.1 only because it has been used as a role in other SFRs.

FMT_SMR.1.2 The TSF shall be able to associate users with roles**, except for the role "Nobody" to which no user shall be associated**.

PP APPLICATION NOTE 65. FMT_SMR.1 is a dependency of FMT_MSA.1, FMT_MSA.3, and FMT_MTD.1.

10.7 Class FPR: Privacy

There are no Class FPR security functional requirements for this Protection Profile.

10.8 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

PP APPLICATION NOTE 66. This Protection Profile interprets FPT_STM.1 to be satisfied if reliable time stamps are generated inside the TOE, outside the TOE, or both.

PP APPLICATION NOTE 67. If reliable time stamps are generated outside of the TOE, the ST Author should consider including additional SFRs to ensure their reliability (e.g., authenticating the source of the time stamps, protecting the integrity of time stamp delivery, or checking the availability of the time stamp service).

PP APPLICATION NOTE 68. If a product can use either internal or external time stamp sources, then the ST Author should express them as distinct modes of operation so that each can be evaluated.

PP APPLICATION NOTE 69. FPT_STM.1 is a dependency of FAU_GEN.1.

FPT_TST.1 TSF testing

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorised user*, *at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF data*].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

PP APPLICATION NOTE 70. FPT_TST.1.3 is intended to verify that the TSF executable code has not been modified by malfunction.

PP APPLICATION NOTE 71. FPT_TST.1 is a principal SFR to fulfill O.SOFTWARE.VERIFIED.

10.9 Class FRU: Resource utilization

There are no Class FRU security functional requirements for this Protection Profile.

10.10 Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

PP APPLICATION NOTE 72. FTA_SSL.3 is a principal SFR to fulfill O.USER.AUTHORIZED and O.INTERFACE.MANAGED.

10.11 Class FTP: Trusted paths/channels

There are no Class FTP security functional requirements for this Protection Profile.

10.12 Common security requirements rationale

Table 19 and Table 20 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 19—Completeness of security requirements

SFRs	Objectives									
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED
FAU_GEN.1										**P**
FAU_GEN.2										**P**
FDP_ACC.1(a)	**P**	**P**	**P**							
FDP_ACC.1(b)							**P**			
FDP_ACF.1(a)	S	S	S							
FDP_ACF.1(b)							S			
FDP_RIP.1	**P**									
FIA_ATD.1							S			
FIA_UAU.1							**P**	**P**		
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S
FIA_USB.1							**P**			
FMT_MSA.1(a)	S	S	S							
FMT_MSA.1(b)							S			
FMT_MSA.3(a)	S	S	S							
FMT_MSA.3(b)							S			
FMT_MTD.1				**P**	**P**	**P**				
FMT_SMF.1	S	S	S	S	S	S				
FMT_SMR.1	S	S	S	S	S	S	S			
FPT_STM.1										S
FPT_TST.1									**P**	
FTA_SSL.3							**P**	**P**		

Table 20—Sufficiency of security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT	Protection of User Data from unauthorized disclosure or alteration	**FDP_ACC.1(a)**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1(a)	Supports access control policy by providing access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MSA.1(a)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(a)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_RIP.1**	**Enforces protection by making residual data unavailable.**
O.CONF.NO_DIS, O.PROT.NO_ALT, O.CONF.NO_ALT	Protection of TSF Data from unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MTD.1	**Enforces protection by restricting access.**
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
O.USER.AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	**FDP_ACC.1(b)**	**Enforces authorization by establishing an access control policy.**
		FDP_ACF.1(b)	Supports access control policy by providing access control function.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_UAU.1	**Enforces authorization by requiring user authentication.**
		FIA_UID.1	**Enforces authorization by requiring user identification.**
		FIA_USB.1	**Enforces authorization by distinguishing subject security attributes associated with user roles.**
		FMT_MSA.1(b)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(b)	Supports access control function by enforcing control of security attribute defaults.

Objectives	Description	SFRs	Purpose
		FMT_SMR 1	Supports authorization by requiring security roles.
		FTA_SSL.3	**Enforces authorization by terminating inactive sessions.**
O.INTERFACE.MANAGED	Management of external interfaces	**FIA_UAU.1**	**Enforces management of external interfaces by requiring user authentication.**
		FIA_UID.1	**Enforces management of external interfaces by requiring user identification.**
		FTA_SSL.3	**Enforces management of external interfaces by terminating inactive sessions.**
O.SOFTWARE.VERIFIED	Verification of software integrity	**FPT_TST.1**	**Enforces verification of software by requiring self-tests.**
O.AUDIT.LOGGED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**
		FIA_UID.1	Supports audit policies by associating user identity with events
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.

11. Security assurance requirements (APE_REQ)

Table 21 lists the security assurance requirements for 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A, and related SFR packages, EAL 3 augmented by ALC_FLR.2.

Table 21—IEEE 2600.1 Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL3)
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing—sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Rationale:

This Protection Profile has been developed for Hardcopy Devices used in restrictive commercial information processing environments that require a relatively high level of document security, operational accountability, and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 3 is appropriate.

EAL 3 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

12. SFR Packages introduction

12.1 SFR Packages usage

The class of Hardcopy Device (HCD) products encompasses a wide variety of functions and configurations, from small non-networked printers to large networked multifunction devices. To accommodate such a wide variety of products, this standard is structured as a common Protection Profile that applies to all HCDs and a set of named Security Functional Requirements (SFR) packages that may apply to some HCD configurations.

To use this standard, authors shall compose a Security Target or Protection Profile which conforms to the Protection Profile identified in 3.2 and its common SFRs and conforms to *any and all* SFR packages identified in 12.2 that apply to functions which are present in their Target of Evaluation. The formal conformance requirements are described in 6.4.

PP APPLICATION NOTE 73. A conforming ST must conform to the access control subjects, objects, security attributes, and rules, which are specified in 10.4 of this standard, and to those which are specified in the access control SFRs of every SFR Package to which the ST claims conformance. The ST Author may define additional subjects, objects, security attributes, or rules that do not contradict those in 10.4 and claimed SFR Packages.

12.2 SFR Packages reference

Title: 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as printers, paper-based fax machines, and MFPs) that perform a printing function in which electronic document input is converted to physical document output.

Title: 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2

Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as scanners, paper-based fax machines, and MFPs) that perform a scanning function in which physical document input is converted to electronic document output.

Title: 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This Protection Profile shall be used for HCD products (such as copiers and MFPs) that perform a copy function in which physical document input is duplicated to physical document output.

Title: 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as fax machines and MFPs) that perform a scanning function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a printing function in which a telephone-based document facsimile (fax) reception is converted to physical document output.

Title: 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products (such as MFPs) that perform a document storage and retrieval feature in which a document is stored during one job and retrieved during one or more subsequent jobs.

Title: 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for products that provide storage of User Data or TSF Data in a nonvolatile storage device (NVS) that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel. This package applies for TOEs that provide the ability to protect data stored on Removable Nonvolatile Storage devices from unauthorized disclosure and modification. If such protection is supplied only by the TOE environment, then this package cannot be claimed.

Title: 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A
Package version: 1.0, dated June 2009
Common Criteria version: Version 3.1 Revision 2
Common Criteria conformance: Part 2 extended and Part 3 conformant
Package conformance: EAL3 augmented by ALC_FLR.2
Usage: This SFR package shall be used for HCD products that transmit or receive User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio frequency wireless media. This package applies for TOEs that provide a trusted channel function allowing for secure and authenticated

communication with other IT systems. If such protection is supplied by only the TOE environment, then this package cannot be claimed.

12.3 SFR Package functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 22.

Table 22—SFR Package functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.NVS	Nonvolatile storage: a function that stores User Data or TSF Data on a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from the TOE by authorized personnel
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

12.4 SFR Package attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that depend on the function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 23.

Table 23—SFR Package attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+NVS	Indicates data that are stored on a nonvolatile storage device.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

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

13.1 PRT SFR Package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.PRT function as defined in 12.3. As a minimum, the package provides access controls for releasing pending hardcopy output to a Hardcopy Output Handler. It may also be used to specify additional rules for previewing or modifying documents before printing.

13.2 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 24 is referenced in the Class FDP SFRs that follow.

Table 24—PRT Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+PRT	Read	U.NORMAL	Denied, except for his/her own documents

PP APPLICATION NOTE 74. In these cases, "Read" refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

PP APPLICATION NOTE 75. A User will need to authenticate using the Operator Panel on the TOE to perform "Read" operations. If the User has authenticated using Operator Panel when submitting a print job, and that session is still active, then reauthentication is not necessary. However, if that session is no longer active or the User authenticated and submitted the print job over a different Interface, then the User will need to authenticate using Operator Panel in order to establish a new session before being permitted to perform the "Read" operation.

PP APPLICATION NOTE 76. If a conforming TOE provides a feature for modifying a submitted document before printing, then the ST Author should add additional rules for D.DOC (+PRT) using the Modify operation.

FDP_ACC.1 Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1 The TSF shall enforce the **PRT Access Control SFP in Table 24 on the list of subjects, objects, and operations among subjects and objects covered by the PRT Access Control SFP in Table 24.**

PP APPLICATION NOTE 77. FDP_ACC.1 is a principal SFR to fulfill O.DOC.NO_DIS and is a dependency of FDP_ACF.1.

FDP_ACF.1 Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **PRT Access Control SFP in Table 24** to objects based on the following: **the list of subjects and objects controlled under the PRT Access Control SFP in Table 24, and for each, the indicated security attributes in Table 24**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the PRT Access Control SFP in Table 24 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 78. FMT_MSA.3 is a dependency of FDP_ACF.1. That dependency is resolved by 10.6 for the Common Access Control SFP, but it does not specify the PRT Access Control SFP. Therefore, the ST Author should add the PRT Access Control SFP to FMT_MSA.3 in a conforming Security Target, and should consider the management of attributes and roles that are needed to support the PRT Access Control SFP.

PP APPLICATION NOTE 79. FDP_ACF.1 is a dependency of FDP_ACC.1.

13.3 PRT security requirements rationale

Table 25 and Table 26 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 25—Completeness of PRT security requirements

	Objectives
SFRs	O.DOC.NO_DIS
FDP_ACC.1	**P**
FDP_ACF.1	S

Table 26—Sufficiency of PRT security requirements

Objectives	**Description**	**SFRs**	**Purpose**
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_ACC.1**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1	Supports access control policy by providing access control function.

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

14.1 SCN SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.SCN function as defined in 12.3. As a minimum, the package provides access controls for transmitting scanned documents to another IT device. It may also be used to specify additional rules for previewing or modifying scanned documents before transmitting them to another IT device.

14.2 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 27 is referenced in the Class FDP SFRs that follow.

Table 27—SCN Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+SCN	Read	U.NORMAL	Denied, except for his/her own documents

PP APPLICATION NOTE 80. In these cases, "Read" refers (as a minimum) to the transmission of User Document Data through an Interface to a destination of the user's choice. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

PP APPLICATION NOTE 81. If a conforming TOE provides a feature for modifying a scanned document before transmission, then the ST Author should add additional rules for D.DOC (+SCN) using the Modify operation.

FDP_ACC.1 Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1 The TSF shall enforce the **SCN Access Control SFP in Table 27 on the list of subjects, objects, and operations among subjects and objects covered by the SCN Access Control SFP in Table 27.**

PP APPLICATION NOTE 82. FDP_ACC.1 is a principal SFR to fulfill O.DOC.NO_DIS and is a dependency of FDP_ACF.1.

FDP_ACF.1 Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **SCN Access Control SFP in Table 27** to objects based on the following: **the list of subjects and objects controlled under the SCN Access Control SFP in Table 27, and for each, the indicated security attributes in Table 27**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the SCN Access Control SFP in Table 27 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 83. FMT_MSA.3 is a dependency of FDP_ACF.1. That dependency is resolved by 10.6 of IEEE Std 2600.1 for the Common Access Control SFP, but it does not specify the SCN Access Control SFP. Therefore, the ST Author should add the SCN Access Control SFP to FMT_MSA.3 in a conforming Security Target, and should consider the management of attributes and roles that are needed to support the SCN Access Control SFP.

PP APPLICATION NOTE 84. FDP_ACF.1 is a dependency of FDP_ACC.1.

14.3 SCN security requirements rationale

Table 28 and Table 29 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 28—Completeness of SCN security requirements

SFRs	Objectives
	O.DOC.NO_DIS
FDP_ACC.1	**P**
FDP_ACF.1	S

Table 29—Sufficiency of SCN security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_ACC.1**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1	Supports access control policy by providing access control function.

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

15.1 CPY SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.CPY function as defined in 12.3. As a minimum, the package provides access controls for releasing pending copies of documents to a Hardcopy Output Handler. It may also be used to specify additional rules for previewing or modifying documents before producing hardcopy output.

15.2 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 30 is referenced in the Class FDP SFRs that follow.

Table 30—CPY Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+CPY	Read	This package does not specify any access control restriction.	

PP APPLICATION NOTE 85. In this case, “Read” refers to the release of pending hardcopy output to a Hardcopy Output Handler. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

PP APPLICATION NOTE 86. For F.CPY, there are no access control requirements for release of User Document Data to the Hardcopy Output Handler because the Normal User who submitted the job is physically present when User Document Data are supplied to the Original Document Handler. The ST Author may create more restrictive access control rules.

PP APPLICATION NOTE 87. If a conforming TOE provides a feature for modifying a scanned document before producing hardcopy output, then the ST Author should add additional rules for D.DOC (+CPY) using the Modify operation.

FDP_ACC.1 Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1 The TSF shall enforce the **CPY Access Control SFP in Table 30** on **the list of subjects, objects, and operations among subjects and objects covered by the CPY Access Control SFP in Table 30**.

PP APPLICATION NOTE 88. FDP_ACC.1 is a principal SFR to fulfill O.DOC.NO_DIS and is a dependency of FDP_ACF.1.

FDP_ACF.1 Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **CPY Access Control SFP in Table 30** to objects based on the following: **the list of subjects and objects controlled under the CPY Access Control SFP in Table 30, and for each, the indicated security attributes in Table 30**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the CPY Access Control SFP in Table 30 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 89. FMT_MSA.3 is a dependency of FDP_ACF.1. That dependency is resolved by 10.6 of IEEE Std 2600.1 for the Common Access Control SFP, but it does not specify the CPY Access Control SFP. Therefore, the ST Author should add the CPY Access Control SFP to FMT_MSA.3 in a conforming Security Target and should consider the management of attributes and roles that are needed to support the CPY Access Control SFP.

PP APPLICATION NOTE 90. FDP_ACF.1 is a dependency of FDP_ACC.1.

15.3 CPY security requirements rationale

Table 31 and Table 32 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 31—Completeness of CPY security requirements

SFRs	Objectives
	O.DOC.NO_DIS
FDP_ACC.1	**P**
FDP_ACF.1	S

Table 32—Sufficiency of CPY security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_ACC.1**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1	Supports access control policy by providing access control function.

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

16.1 FAX SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.FAX function as defined in 12.3. As a minimum, the package provides access controls for retrieving received documents, for transmitting received documents to another IT device, and for transmitting sent documents to another fax device. It may also be used to specify additional rules, roles, or mechanisms to transfer ownership of a received document to one or more intended recipients.

16.2 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 33 is referenced in the Class FDP SFRs that follow.

Table 33—FAX Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+FAXIN	Read	U.NORMAL	Denied, except for his/her own documents
	+FAXOUT	Read	U.NORMAL	Denied, except for his/her own documents

PP APPLICATION NOTE 91. In these cases, “Read” refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler for receiving faxes (+FAXIN) and to the transmission of User Document Data through an Interface for sending or receiving faxes (+FAXOUT or +FAXIN). It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

PP APPLICATION NOTE 92. For receiving fax documents (+FAXIN), the “owner” of a received fax job is considered to be U.ADMINISTRATOR. The ST Author may refine this role if a conforming TOE provides a specific role for fax administration.

PP APPLICATION NOTE 93. If a conforming TOE provides a feature that allows an administrator to manage ownership of a received fax job—typically, to transfer ownership to one or more intended recipients of a fax document—then the ST Author should consider adding a rule to the FAX Access Control SFP such as “D.DOC +FAXIN Read U.NORMAL ‘Allowed if this User is authorized by U.ADMINISTRATOR’”.

Alternatively, the ST Author may define and use attributes for this purpose in the FAX Access Control SFP, provided that the initialization and management of such attributes are specified in such as in FMT_MSA.1 and FMT_MSA.3. In either case, the ST Author should precisely define the ownership rules for both User Documents and User Function Data associated with such documents.

PP APPLICATION NOTE 94. If a conforming TOE provides a feature that allows an administrator to manage the transmission of outgoing fax documents, then the ST Author should consider adding an additional rule to the FAX Access Control SFP for D.DOC(+FAXOUT) that permits the administrator to Read, and an additional rule for D.FUNC that permits the administrator to Modify.

PP APPLICATION NOTE 95. If a conforming TOE provides a feature that allows an administrator to delete outgoing fax documents, then the ST Author should consider adding additional rules to the FAX Access Control SFP for D.DOC(+FAXOUT) and D.FUNC that permit the administrator to Delete.

PP APPLICATION NOTE 96. If a conforming TOE provides a feature for modifying a document before creating hardcopy output or transmitting outgoing fax documents, then the ST Author should add additional rules for D.DOC(+FAXIN) or D.DOC(+FAXOUT), respectively, using the Modify operation.

FDP_ACC.1 Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1 The TSF shall enforce the **FAX Access Control SFP in Table 33 on the list of subjects, objects, and operations among subjects and objects covered by the FAX Access Control SFP in Table 33.**

PP APPLICATION NOTE 97. FDP_ACC.1 is a principal SFR to fulfill O.DOC.NO_DIS and is a dependency of FDP_ACF.1.

FDP_ACF.1 Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **FAX Access Control SFP in Table 33** to objects based on the following: **the list of subjects and objects controlled under the FAX Access Control SFP in Table 33, and for each, the indicated security attributes in Table 33**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the FAX Access Control SFP in Table 33 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 98. FMT_MSA.3 is a dependency of FDP_ACF.1. That dependency is resolved by 10.6 of IEEE Std 2600.1 for the Common Access Control SFP, but it does not specify the FAX Access Control SFP. Therefore, the ST Author should add the FAX Access Control SFP to FMT_MSA.3 in a

conforming Security Target and should consider the management of attributes and roles that are needed to support the FAX Access Control SFP.

PP APPLICATION NOTE 99. FDP_ACF.1 is a dependency of FDP_ACC.1.

16.3 FAX security requirements rationale

Table 34 and Table 35 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 34—Completeness of FAX security requirements

SFRs	Objectives
	O.DOC.NO_DIS
FDP_ACC.1	**P**
FDP_ACF.1	S

Table 35—Sufficiency of FAX security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	**FDP_ACC.1**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1	Supports access control policy by providing access control function.

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

17.1 DSR SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.DSR function as defined in 12.3. As a minimum, the package provides access controls for storing and retrieving documents. It may also be used to specify additional rules for modifying stored documents, and roles, mechanisms, or rules for authorizing a user or users to access documents that have been stored by a different user.

17.2 Class FDP: User data protection

The Security Function Policy (SFP) described in Table 36 is referenced in the Class FDP SFRs that follow.

Table 36—DSR Access Control SFP

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+DSR	Read	U.NORMAL	Denied, except (1) for his/her own documents or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE

PP APPLICATION NOTE 100. In these cases, "Read" refers (as a minimum) to the transmission of User Document Data through an Interface to a destination of the user's choice. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

PP APPLICATION NOTE 101. If a conforming TOE provides a feature for modifying a document that has been stored in the TOE, then the ST Author should add additional rules for D.DOC (+DSR) using the Modify operation.

PP APPLICATION NOTE 102. An access control rule for creating documents is not specified, because it is assumed that all users who are allowed to use the DSR function are automatically allowed to create documents. The ST Author may introduce more restrictive rules for document creation if the conforming TOE enforces such rules.

PP APPLICATION NOTE 103. The ST Author should specify appropriate roles or mechanisms for authorizing users to read or modify another user's documents, if such functions are provided by a conforming TOE.

FDP_ACC.1 Subset access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.1.1 The TSF shall enforce the **DSR Access Control SFP in Table 36 on the list of subjects, objects, and operations among subjects and objects covered by the DSR Access Control SFP in Table 36**.

PP APPLICATION NOTE 104. FDP_ACC.1 is a principal SFR to fulfill O.DOC.NO_DIS and is a dependency of FDP_ACF.1.

FDP_ACF.1 Security attribute based access control

Hierarchical to: **No other components**

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **DSR Access Control SFP in Table 36** to objects based on the following: **the list of subjects and objects controlled under the DSR Access Control SFP in Table 36, and for each, the indicated security attributes in Table 36**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the DSR Access Control SFP in Table 36 governing access among Users and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

PP APPLICATION NOTE 105. FMT_MSA.3 is a dependency of FDP_ACF.1. That dependency is resolved by 10.6 of IEEE Std 2600.1 for the Common Access Control SFP, but it does not specify the DSR Access Control SFP. Therefore, the ST Author should add the DSR Access Control SFP to FMT_MSA.3 in a conforming Security Target, and should consider the management of attributes and roles that are needed to support the DSR Access Control SFP.

PP APPLICATION NOTE 106. FDP_ACF.1 is a dependency of FDP_ACC.1.

17.3 DSR security requirements rationale

Table 37 and Table 38 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 37—Completeness of DSR security requirements

SFRs	Objectives
	O.DOC.NO_DIS
FDP_ACC.1	**P**
FDP_ACF.1	S

Table 38—Sufficiency of DSR security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure or alteration	**FDP_ACC.1**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1	Supports access control policy by providing access control function.

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

18.1 NVS SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.NVS function as defined in 12.3. As a minimum, the package provides protection for User Data and TSF Data that are stored on Removable Nonvolatile Storage devices when such devices are removed from the protection of the environment of the TOE.

A Removable Nonvolatile Storage device is a nonvolatile storage device that is part of the evaluated TOE but is designed to be removed from and reinserted into the TOE by authorized personnel. If any nonvolatile storage devices are present in a conforming TOE, the ST Author should identify which are or are not designed to be removable.

Removing and transporting such a device outside the protection of the environment of the TOE would potentially allow an attacker to analyze its content off-line. Re-inserting the device from outside of the protection of the environment of the TOE would potentially allow an attacker to introduce malicious content into the TOE.

If the TOE has the capability to store User Data or TSF Data on such a device, the security objective of protecting this data can only be achieved when the confidentiality and integrity of the data are preserved

even in the case of an attacker that analyzes the content of the Removable Nonvolatile Storage device using a system capable of reading the content of the device.

18.2 Class FPT: Protection of the TSF

FPT_CIP_EXP.1 Confidentiality and integrity of stored data

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FPT_CIP_EXP.1.1 The TSF shall provide a function that ensures the confidentiality and integrity of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

PP APPLICATION NOTE 107. The ST Author should define the methods used to protect the confidentiality and integrity of the data in the ST. In the case cryptographic methods are used, the ST Author should include the appropriate SFRs from the FCS class and check for guidance on the use of cryptographic functions specific to the scheme in which the TOE is being certified.

FPT_CIP_EXP.1.2 The TSF shall provide a function that detects and performs [assignment: *list of actions*] when it detects alteration of user and TSF data when either is written to [assignment: ***a Removable Nonvolatile Storage device***].

PP APPLICATION NOTE 108. The ST Author should to define the actions to be taken in case the TOE detects an integrity error when reading data that have been previously stored with confidentiality and integrity protection.

PP APPLICATION NOTE 109. FPT_CIP_EXP.1 is a principal SFR to fulfill O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT.

18.3 NVS security requirements rationale

Table 39 and Table 40 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 39—Completeness of NVS security requirements

SFRs	Objectives					
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT
FPT_CIP_EXP.1	**P**	**P**	**P**	**P**	**P**	**P**

Table 40—Sufficiency of NVS security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, O.CONF.NO_ALT	Protection of User and TSF Data from unauthorized disclosure or alteration	**FPT_CIP_EXP.1**	**Enforces protection by requiring protected storage methods.**

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

19.1 SMI SFR package introduction

This SFR package must be applied to a conforming Security Target or Protection Profile if its Target of Evaluation performs an F.SMI function as defined in 12.3. As a minimum, the package provides protection for User Data or TSF Data that are transmitted or received over shared-medium interfaces and, if needed, management control of data transmission involving shared-medium interfaces.

19.2 Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: **No other components**

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions; and
- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 41;** [assignment: *other specifically defined auditable events*].

PP APPLICATION NOTE 110. If the ST Author specifies one of the Common Criteria defined audit levels (minimum, basic, or detailed), there may be some conflict among the requirements of that audit level and the requirements listed in Table 41. The ST shall specify the greater of those requirements.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 41: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*]

Table 41—SMI Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required

PP APPLICATION NOTE 111. FPT_STM.1 is a dependency of FAU_GEN.1, but that dependency is resolved by 10.8 of IEEE Std 2600.1.

PP APPLICATION NOTE 112. FAU_GEN.1 is a principal SFR to fulfill O.AUDIT.LOGGED, and is a dependency of FAU_GEN.2.

PP APPLICATION NOTE 113. FAU_GEN.1 performs audit functions that are recommended for FTP_ITC.1 and FPT_STM.1.

19.3 Class FPT: Protection of the TSF

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: **No other components**

Dependencies: **FMT_SMF.1 Specification of Management Functions**
FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface**.

PP APPLICATION NOTE 114. The ST Author can use this SFR to define the roles that are permitted to allow unmediated transmission between Interfaces. If unmediated transmission is never allowed, "Nobody" should be instantiated as the "authorized identified roles."

PP APPLICATION NOTE 115. FMT_SMF.1 is a dependency of FPT_FDI_EXP.1, but that dependency is resolved by 10.6 of IEEE Std 2600.1.

PP APPLICATION NOTE 116. FMT_SMR.1 is a dependency of FPT_FDI_EXP.1, but that dependency is resolved by 10.6 of IEEE Std 2600.1.

PP APPLICATION NOTE 117. FPT_FDI_EXP.1 is a principal SFR to fulfill O.INTERFACE.MANAGED.

19.4 Class FTP: Trusted paths/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: **No other components**

Dependencies: **No dependencies**

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

PP APPLICATION NOTE 118. FTP_ITC.1 is a principal SFR to fulfill O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, and O.CONF.NO_ALT.

19.5 SMI security requirements rationale

Table 42 and Table 43 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 42—Completeness of SMI security requirements

SFRs	Objectives							
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.INTERFACE.MANAGED	O.AUDIT.LOGGED
FAU_GEN.1								**P**
FPT_FDI_EXP.1							**P**	
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**		

Table 43—Sufficiency of SMI security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT, O.PROT.NO_ALT, O.CONF.NO_DIS, O.CONF.NO_ALT	Protection of User and TSF Data from unauthorized disclosure or alteration	**FTP_ITC.1**	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**
O.INTERFACE.MANAGED	Management of external interfaces	**FPT_FDI_EXP.1**	**Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces.**
O.AUDIT.LOGGED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**

Annex A

(normative)

Glossary

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B3] should be referenced for terms not defined in this annex.

Access: Interaction between an entity and an object that results in the flow or modification of data.

Access Control: Security service that controls the use of hardware and software resources and the disclosure and modification of stored or communicated data.

Accountability: Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator: A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Asset: An entity upon which the TOE Owner, User, or manager of the TOE places value.

Authentication: Security measure that verifies a claimed identity.

Authentication data: Information used to verify a claimed identity.

Authorization: Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized User: An authenticated User who may, in accordance with the TSP, perform an operation. This includes Users who are permitted to perform some operations but may be able to attempt or perform operations that are beyond those permissions.

Availability: (A) A condition in which Authorized Users have access to information, functionality, and associated assets when requested. (B) Timely (according to a defined metric), reliable access to IT resources.

Channel: Mechanisms through which data can be transferred into and out of the TOE.

Confidentiality: (A) A condition in which information is accessible only to those authorized to have access. (B) A security policy pertaining to disclosure of data.

Enterprise: An operational context typically consisting of centrally managed networks of IT products protected from direct Internet access by firewalls. Enterprise environments generally include medium-to-large businesses, certain governmental agencies, and organizations requiring managed telecommuting systems and remote offices.

Evaluation Assurance Level: An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Interface: A non-hardcopy interface where either the input is being received from outside the TOE or the output is delivered to a destination outside the TOE.

Function: An entity in the TOE that performs processing, storage, or transmission of data that may be present in the TOE.

Hardcopy Device (HCD): A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones,” and other similar products. *See*: **Multifunction Device**.

Hardcopy Output Handler: Mechanisms for transferring User Document Data in hardcopy form out of the HCD.

Identity: A representation (e.g., a string) uniquely identifying an Authorized User, which can either be the full or abbreviated name of that User or a pseudonym.

Information assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology (IT): The hardware, firmware, and software used as part of a system to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Integrity: (A) A condition in which data have not been changed or destroyed in an unauthorized way. (B) A security policy pertaining to the corruption of data and security function mechanisms.

Job: A document processing task submitted to the hardcopy device. A single processing task may process one or more documents.

Multifunction Device (MFD) and **Multifunction Product (MFP)**: A hardcopy device that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

Nobody: A pseudo-role that cannot be assigned to any User.

Nonvolatile storage: Computer storage that is not cleared when the power is turned off.

Normal User: A User who is authorized to perform User Document Data processing functions of the TOE.

Object: A passive entity in the TOE, that contains or receives information and upon which subjects perform operations.

Operation: A specific type of action performed by a subject on an object.

Operational Environment: The total environment in which a TOE operates, including the consideration of the value of assets and controls for operational accountability, physical security, and personnel.

Operator Panel: A local human interface used to operate the HCD. It typically consists of a keypad, keyboard, or other controls, and a display device.

Organizational Security Policy (OSP): A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Original Document Handler: Mechanisms for transferring User Document Data in hardcopy form into the HCD.

Own or **Ownership**: May refer to a User Document or to User Function Data associated with processing a User Document. Depending upon the implementation of conforming TOE applications, the Owner of a User Function Data associated with a User Document may be different or may have different access control rules. These should be specified in a conforming Security Target.

Private-medium Interface: Mechanism for exchanging data that (1) use wired or wireless electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous users; or, (2) use Operator Panel and displays that are part of the TOE.

Protected: A condition in which data have not been changed or destroyed in an unauthorized way.

Removable nonvolatile storage: Nonvolatile storage that is part of an evaluated TOE but is designed to be removed from the TOE by authorized personnel. *See*: Nonvolatile storage.

Security attribute: A property of subjects, users (including external IT products), objects, information, sessions, and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP): A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Functional Requirement (SFR): A functional requirement which is taken from Part 2 of the Common Criteria and provides the mechanisms to enforce the security policy.

Security Target (ST): An implementation-dependent statement of security needs for a specific identified TOE.

SFR Package: A named set of security functional requirements.

Shared-medium Interface: Mechanism for transmitting or receiving data that uses wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users.

ST Author: The author of a Security Target that conforms to this Protection Profile and related SFR Packages. For simplicity, ST Author also refers to the author of a different Protection Profile that conforms to this Protection Profile and related SFR packages.

Subject: An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Telephone line: An electrical interface used to connect the TOE to the public switch telephone network for transmitting and receiving facsimiles.

Threat: Capabilities, intentions, and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

TSF Data: Data created by and for the TOE, that might affect the operation of the TOE.

TSF Confidential Data: Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.

TSF Protected Data: Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.

TOE Owner: A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

TOE security functionality (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

User: An entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data: Data created by and for the User, that do not affect the operation of the TOE security functionality.

User Document Data: The asset that consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.

User Function Data: The asset that consists of the information about a user's document or job to be processed by the HCD.

Annex B

(normative)

Acronyms

Table B.1—Acronyms

Acronym	Definition
A.	assumption (when used in hierarchical naming)
ADMIN.	administrator (when used in hierarchical naming)
ALT	alteration
CC	Common Criteria
C/IA	IEEE Computer Society Information Assurance
CONF.	confidential (when used in hierarchical naming)
CPY	copy
D.	data (when used in hierarchical naming)
DIS	disclosure
DOC.	document (when used in hierarchical naming)
DSR	document storage and retrieval
EAL	Evaluation Assurance Level
F.	Function (when used in hierarchical naming)
FAX	facsimile
FUNC.	function (when used in hierarchical naming)
HCD	Hardcopy Device
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
MFD	Multifunctional Device
MFP	Multifunctional Product / peripheral / printer
NVS	nonvolatile storage
O.	Security Objective (of the TOE) (when used in hierarchical naming)
OE.	Security Objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PP	Protection Profile
PROT.	protected (when used in hierarchical naming)
PRT	print
SCN	scan
SFP	Security Function Policy
SFR	Security Functional Requirement
SMI	Shared-medium Interface
ST	Security target
Std	standard
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE security policy
U.	user (when used in hierarchical naming)

Annex C

(informative)

Bibliography

[B1] Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 1—Part 1: Introduction and General Model, 2006.[5]

[B2] Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2—Evaluation Methodology, 2007.[6]

[B3] IEEE 100™, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition. New York, Institute of Electrical and Electronic Engineers, Inc.[7,8]

[5] Available from http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf.
[6] Available from http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf.
[7] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org).
[8] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.