

**GUIDE
FOR THE DEVELOPMENT OF
SECURITY TARGETS
CONFORMING TO THE
IEEE STD 2600 SERIES OF
PROTECTION PROFILES**

By the IEEE Hardcopy Device and System Security
Working Group

<http://grouper.ieee.org/groups/2600/>

Version 1.1
January 2011

CONTENTS

1	Introduction.....	- 5 -
1.1	Purpose and Scope.....	- 5 -
1.2	Audience.....	- 5 -
1.3	Organization of the Guide	- 6 -
1.4	Normative References	- 6 -
1.5	Participation	- 7 -
2	PROTECTION PROFILE	- 8 -
2.1	Common Criteria.....	- 8 -
2.2	Protection Profiles	- 8 -
3	IEEE Std 2600™-2008	- 11 -
3.1	Introduction	- 11 -
3.2	IEEE Std 2600 Structure	- 12 -
3.2.1	IEEE Std 2600 Operational Environments	- 12 -
3.2.1.1	Operational Environment A	- 12 -
3.2.1.2	Operational Environment B	- 12 -
3.2.1.3	Operational Environment C	- 13 -
3.2.1.4	Operational Environment D	- 13 -
3.3	Relationship to the IEEE Std 2600 Series of Protection Profiles	- 13 -
4	IEEE STD 2600 SERIES OF PROTECTION PROFILES	- 15 -
4.1	Introduction	- 15 -
4.2	IEEE Std 2600 Series of Protection Profiles Structure and Content	- 15 -
4.2.1	Protection Profile and SFR Packages.....	- 15 -
4.2.1.1	Introduction and Rationale.....	- 15 -
4.2.1.2	Common PP	- 15 -
4.2.1.3	SFR Packages.....	- 16 -
4.2.1.4	Conformance rules	- 16 -
4.2.2	TOE Model	- 17 -
4.2.2.1	Introduction and Rationale.....	- 17 -
4.2.2.2	Users and Subjects	- 17 -
4.2.2.3	Users	- 18 -
4.2.2.4	Assets	- 18 -
4.2.2.4.1	User Data	- 19 -
4.2.2.4.2	TSF Data.....	- 19 -
4.2.2.4.3	Functions.....	- 19 -
4.2.2.5	Operations	- 19 -
4.2.2.6	Channels.....	- 19 -
4.2.3	Threats, Policies, and Assumptions	- 20 -
4.2.3.1	Introduction and Rationale.....	- 20 -
4.2.3.2	Threats.....	- 20 -
4.2.3.3	Organizational Security Policies	- 20 -
4.2.3.4	Assumptions.....	- 20 -
4.2.4	Security Objectives	- 21 -
4.2.4.1	Objectives that Counter Threats	- 21 -
4.2.4.2	Objectives that Enforce OSPs	- 21 -
4.2.4.3	Objectives that Uphold Assumptions.....	- 21 -
4.2.5	Security Functional Requirements.....	- 22 -

4.2.5.1	Extended Components	- 22 -
4.2.5.2	Objectives that May be Fulfilled by the TOE or Its Environment	- 22 -
4.2.5.3	Objectives Fulfilled by PP SFRs and Package SFRs	- 23 -
4.2.6	Dependencies in SFR Packages	- 23 -
5	IEEE STD 2600 SERIES OF PROTECTION PROFILES – VENDOR USAGE GUIDELINES..	- 24 -
5.1	Introduction	- 24 -
5.2	Choosing the Appropriate Operational Environment For Certification.....	- 24 -
5.3	Guidelines for Distinguishing Among the Four IEEE Std 2600 Operational Environments..	- 26 -
5.4	How Vendors Can Fulfill Security Objectives Inside the TOE and Outside the TOE	- 32 -
5.4.1	Storing Audit Data Inside or Outside the TOE	- 32 -
5.4.2	Identification and Authentication Requirements Inside or Outside of the TOE	- 33 -
6	IEEE STD 2600 SERIES OF PROTECTION PROFILES – ST AUTHOR USAGE GUIDELINES ...	- 35 -
6.1	Introduction	- 35 -
6.2	General ST Author Guidance	- 35 -
6.3	Examples of Demonstrating Conformance to the IEEE Std 2600 Series of Protection Profiles ..	- 37 -
6.3.1	General Conformance Demonstration	- 37 -
6.3.1.1	Source of Reliable Time Stamps.....	- 37 -
6.3.1.2	Conformance to the NVS SFR package.....	- 38 -
6.3.1.3	Conformance to the SMI SFR package.....	- 39 -
6.3.1.4	Common Security Requirements Rationale	- 39 -
6.4	Determining TSF Confidential vs. TSF Protected Data	- 40 -
6.5	Threats/Objectives Applicable to Each Operational Environment	- 42 -
6.5.1	O.AUDIT.LOGGED Security Objective	- 42 -
6.6	Specifying Security Functional Requirements in STs	- 43 -
6.6.1	Security Audit Logging (Class FAU)	- 44 -
6.6.1.1	Specification of Audit Log Requirements in the ST	- 46 -
6.6.1.2	FTP_CIP_EXP.1 Audit Data Logging	- 47 -
6.6.2	User Data Protection (Class FDP)	- 47 -
6.6.3	User Identification and Authentication (Class FIA)	- 50 -
6.6.3.1	Documenting Authentication Performed by the HCD in STs	- 50 -
6.6.3.2	Authentication and Re-authentication of Print Jobs on Compliant Printers.....	- 50 -
6.6.4	Documenting Time Stamps for Audit Logs Generated Outside the TOE in STs (FPT_STM).....	- 51 -
6.6.5	Software Verification Self-Test (FPT_TST).....	- 51 -
6.6.6	Confidentiality and Integrity of Stored Data (FTP_CIP_EXP).....	- 51 -
6.6.7	Restricting Forwarding of Data to External Interfaces (FPT_FDI_EXP).....	- 53 -
6.6.8	Protection of User Credentials Leaving/Entering an SMI Interface When Scanning to a Remote Destination on IEEE Stds 2600.1 and 2600.2 Compliant Products	- 53 -
6.6.9	Iterating the FMT_MTD.1 SFR	- 54 -
FMT_MTD.1(b).....	- 54 -	
6.7	Common Access Control SFP	- 54 -
6.7.1	Allowing One User to See or Modify Another User’s Documents.....	- 56 -
6.8	Important Things to Do and To Avoid	- 56 -
6.8.1	General ST Content	- 57 -
6.8.2	ST Introduction – TOE Overview.....	- 57 -
6.8.3	ST Conformance Claims.....	- 57 -
6.8.4	ST Security Problem Definition.....	- 60 -
6.8.5	ST Security Objectives	- 61 -
6.8.6	Extended Components Definitions	- 62 -
6.8.7	TOE summary specification	- 62 -

6.9	Guidance on PP Application Notes	- 63 -
6.9.1	General PP Application Notes	- 64 -
6.9.2	Common SFR PP Application Notes (PP Clause 10)	- 66 -
6.9.3	SFR Package Usage	- 75 -
6.9.4	PRT SFR Package PP Application Notes	- 76 -
6.9.5	SCN SFR Package PP Application Notes	- 77 -
6.9.6	CPY SFR Package PP Application Notes	- 77 -
6.9.7	FAX SFR Package PP Application Notes	- 78 -
6.9.8	DSR SFR Package PP Application Notes	- 80 -
6.9.9	NVS SFR Package PP Application Notes	- 81 -
6.9.10	SMI SFR Package PP Application Notes	- 82 -
6.10	Security Assurance Requirements (SARs) Guidance	- 84 -
6.11	Additional ST Author Guidance	- 85 -
7	IEEE STD 2600 SERIES OF PROTECTION PROFILES – CUSTOMER USAGE GUIDELINES....	- 86 -
7.1	Introduction	- 86 -
7.2	What Common Criteria Certification Means	- 86 -
7.2.1	Common Criteria As It Relates to HCDs	- 86 -
7.3	Identifying the Appropriate Operational Environment	- 87 -
7.4	Configuring the Product	- 88 -
7.5	Understanding Product Compliance	- 88 -
7.5.1	Specifying Certification Level in a Request for Proposal	- 89 -
7.6	Examples	- 89 -
8	IEEE STD 2600 SERIES OF PROTECTION PROFILES FAQs.....	- 90 -
8.1	General Interest Questions	- 90 -
8.2	Questions For ST Authors	- 92 -
8.3	Questions for HCD Vendors	- 93 -
8.4	Questions for Common Criteria Evaluators	- 93 -
9	Glossary (Informative).....	- 94 -
10	Acronyms (Informative)	- 96 -
11	Informative References	- 98 -
12	International Perspectives	- 99 -
13	IEEE 2600 Series of Protection Profiles Errata	- 100 -
13.1	IEEE Std 2600.1 Errata	- 100 -
13.2	IEEE Std 2600.2 Errata	- 103 -
13.3	IEEE Std 2600.3 Errata	- 104 -
13.4	IEEE Std 2600.4 Errata	- 104 -
14	Future Considerations	- 105 -

1 Introduction

1.1 Purpose and Scope

This Guide for Development of Security Targets Conforming to the IEEE Std 2600 Series of Protection Profiles (PPs) provides a basis for developing, evaluating and implementing Security Targets and Protection Profiles written to conform to one of the following four documents¹:

1. IEEE Std 2600.1™-2009 IEEE Standard for a Protection Profile in Operational Environment A
2. IEEE Std 2600.2™-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment B
3. IEEE Std 2600.3™-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment C
4. IEEE Std 2600.4™-2010 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment D

It also provides explanatory information on the format and content of these four PPs in the IEEE 2600 Series of Protection Profiles and explains some of the key decisions made that influenced their format and content.

It also explains how to create a Common Criteria Security Target (ST) that conforms to one of the IEEE Std 2600 Series of Protection Profiles. One important goal of this Guide is to ensure a consistency across all ST documents created from one of the IEEE Std 2600 Series of Protection Profiles.

Note that all four PPs comprising the IEEE Std 2600 Series of Protection Profiles are approved by the IEEE, but that only two of these PPs – IEEE Std 2600.1 [B8] and IEEE Std 2600.2 [B9] – were Common Criteria certified when this document was published.

1.2 Audience

This document serves three primary groups with respect to information technology (IT) product security:

1. ST Authors and Consultants: Individuals or groups responsible for writing Security Targets that conform to one of the IEEE Std 2600 Series of Protection Profiles.
2. Developers and Vendors: Hardcopy product providers, product developers and security analysts, including but not limited to product vendors, integrators, and value added resellers.
3. Consumers: Individuals or groups (e.g., product evaluators, system security officers, system certifiers, and system accreditors) responsible for the Common Criteria assessment of IT product security or for specifying requirements for IT product security (e.g., policy makers and regulatory officials, system architects, integrators, acquisition managers, product purchasers, and end users).

Secondary audiences include technical educators, standards bodies, and the research and development community.

The guidance provided in this document also applies to anyone who wants to write a Protection Profile that conforms to one of the IEEE Std 2600 Series of Protection Profiles.

¹ In the rest of this document these four PPs will be referred to individually, respectively, as “IEEE Std 2600.1”, “IEEE Std 2600.2”, “IEEE Std 2600.3” and “IEEE Std 2600.4” and referred to collectively as the “IEEE Std 2600 Series of Protection Profiles”.

1.3 Organization of the Guide

This remainder of this Guide is organized as follows:

- Clause 2 provides a brief overview of the Common Criteria and Protection Profiles.
- Clause 3 discusses IEEE Std 2600TM-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security and its relationship to the IEEE Std 2600 Series of Protection Profiles that this Guide is designed to support.
- Clause 4 gives a more details on the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles.
- Clauses 5 -7 provide guidance on how to use the four Protection Profiles from three perspectives: that of a hardcopy device² (HCD) vendor (Clause 5), that of an author of a Security Target that is to conform to one of the Protection Profiles (Clause 6) and that of a consumer who will be purchasing an HCD product certified against one of the Protection Profiles (Clause 7).
- Clause 8 provides answers to some Frequently Asked Questions about the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles.
- Clauses 9-12 provide additional supporting information.
- Clause 13 provides a list of errors and corrected text in any of the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles.
- Clause 14 lists issues that may be included in future updates of this PP Guide.

Unless noted otherwise all text, especially in Clauses 5-8, applies to all four Protection Profiles that comprise the IEEE Std 2600 Series of Protection Profiles.

1.4 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.

- [B1] IEEE Std 2600TM-2008, IEEE Standard for Information Technology: Hardcopy System and Device Security
- [B2] Common Criteria for Information Technology Security Evaluation Version 3.1 Release 1 - Part 1: Introduction and general model³, available from:
<http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf>
- [B3] Common Criteria for Information Technology Security Evaluation Version 3.1 Release 2 - Part 2: Security functional requirements³, available from:
<http://www.commoncriteriaportal.org/public/files/CCPART2V3.1R2.pdf>
- [B4] Common Criteria for Information Technology Security Evaluation Version 3.1 Release 2 - Part 3: Security Assurance Requirements³, available from:
<http://www.commoncriteriaportal.org/public/files/CCPART3V3.1R2.pdf>
- [B5] Common Methodology for Information Technology Security Evaluation Version 3.1 Release 2 - Evaluation Methodology, available from:
<http://www.commoncriteriaportal.org/public/files/CEMV3.1R2.pdf>

² See Clause 9 for the definition of Hardcopy Device.

³ Also listed as ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation

- [B6] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, available from:
<http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf>
- [B7] ISO/IEC⁴ TR 15446, Information Technology – Security techniques - Guide for the production of Protection Profiles and Security Targets, First Edition, 2004-07-01, available from:
<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.
- [B8] IEEE 2600.1™-2009 IEEE Standard for a Protection Profile in Operational Environment A
- [B9] IEEE 2600.2™-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment B
- [B10] IEEE 2600.3™-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment C
- [B11] IEEE 2600.4™-2010 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment D

1.5 Participation

At the time this document was prepared, the Hardcopy Device and System Security Working Group had the following membership:

Don Wright, *Chair*
Lee Farrell, *Vice-chair*
Brian Smithson, *Secretary*
Alan Sukert, *Lead Editor*

Carmen Aubry
Shah Bhatti
Nancy Chen
Peter Cybuck
Nick Del Re
Satoshi Fujitani
Tom Haapanen

Akihoko Iwasaki
Harry Lewis
Takanori Masui
Ron Nevo
Yusuke Ohta
Ken Ota
Glen Petrie

Jerry Thrasher
Hiroki Uchiyama
Shigeru Ueda
Brian Volkoff
Bill Wagner
Sameer Yami

⁴ ISO – International Organization for Standardization; IEC – International Electrotechnical Commission

2 PROTECTION PROFILE

As stated in 1.1, the purpose of this document is to provide guidance on how to write Security Targets that comply with the Common Criteria and conform to one of the IEEE 2600 Series of Protection Profiles. To put this guidance in the proper context, this document briefly discusses what the Common Criteria and a Protection Profile are.

2.1 Common Criteria

The Common Criteria (CC) Part 1, Part 2 and Part 3 ([B2]-[B4]), along with its companion Common Methodology for Information Technology (IT) Security Evaluation (CEM) [B5], are the technical basis for an international agreement, known as the Common Criteria Recognition Arrangement (CCRA)⁵ [B6], which ensures that:

1. Products can be evaluated by competent and independent licensed laboratories to determine the fulfillment of particular security properties, to a defined level of assurance.
2. Supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.
3. The certification of the security properties of an evaluated product can be issued by a number of Evaluation Schemes⁶, with this certification being based on the result of their evaluation.
4. These certificates, up to Evaluation Assurance Level (EAL) 4, are recognized by all the signatories of the CCRA.

The contents of each of the four documents that comprise the Common Criteria can be found from the Common Criteria portal at <http://www.commoncriteriaportal.org>.

2.2 Protection Profiles

The CC defines a Protection Profile, like the four Protection Profiles that comprise the IEEE Std 2600 Series of Protection Profiles, as “an implementation-independent statement of security needs for a TOE (Target of Evaluation) type.” A PP is intended to describe a TOE type (in this case HCDs). The same PP may therefore be used as a template for many different STs to be used in different evaluations against the TOE type covered by the PP. A PP describes the general requirements for a TOE type, and is therefore typically written by either:

1. A user community seeking to come to a consensus on the requirements for a given TOE type (which is the case for the PPs covered by this document).
2. A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE.
3. A government or large corporation specifying its requirements as part of its acquisition process.

PPs are written in a way so that they don't mandate a specific solution for meeting the functional and assurance requirements specified in the PPs. For example, in specifying the FIA_UID SFR, IEEE Std 2600.1 [B8] does not mandate how the requirement for user identification is to be satisfied; as a result user

⁵ The Common Criteria Recognition Arrangement (CCRA) provides for mutual acceptance and recognition by all twenty-five countries that are signatories of the agreement of a Common Criteria certification carried out by any one of the countries that are signatories of the agreement.

⁶ An Evaluation Scheme is the administrative and regulatory framework under which the CC is applied by an evaluation authority within one of the countries that are signatories of the CCRA. For example, the National Information Assurance Partnership (NIAP) is the Evaluation Scheme in the United States.

identification can be implemented completely within the TOE or can be implemented by both the TOE and an external IT Product such as a Kerberos server and the TOE could still conform to IEEE Std 2600.1.

Specifics on the intent, format and content of a typical Protection Profile can be found in Chapter 9 of the CEM v3.1R2 [B5] and CC Part 1 v3.1R1 [B2]. Table 1 maps the Protection Profile content to the clauses of each of the PPs that comprise the IEEE Std 2600 Series of Protection Profiles.

Table 1. Typical PP Format and Content

CC Part 1 Chapter	IEEE Std 2600.X Clause	Title	Content
1	4 - 6	PP Introduction (APE_INT)	<ul style="list-style-type: none"> • PP Reference - identifies that particular PP • TOE Overview - briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware / software / firmware available to the TOE
2	7	Conformance Claims (APE_CCL)	<ul style="list-style-type: none"> • Describes how STs and/or other PPs must conform to that PP • Describes how the PP conforms with other PPs and with packages
3	8	Security Problem Definition (APE_SPD)	<p>Defines the security problem that is to be addressed in terms of:</p> <ul style="list-style-type: none"> • Threats – Describes the threats that are to be countered by the TOE, its operational environment, or a combination of the two • OSPs – Describes the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two • Assumptions - Describes the physical, personnel and connectivity assumptions that are made about the operational environment to be able to provide security functionality

CC Part 1 Chapter	IEEE Std 2600.X Clause	Title	Content
4	9	Security Objectives (APE_OBJ)	<p>Provides a concise and abstract statement of the intended solution to the problem as it pertains to the TOE, development environment and operational environment⁷. Includes:</p> <ul style="list-style-type: none"> • A set of short, understandable and clear statements that taken together form a high-level solution to the security problem • A set of statements describing the goals that the operational environment should achieve • A security objectives rationale providing a map showing which security objectives address which threats, OSPs and assumptions along with the associated justification for this mapping
5	10	Extended components definition (APE_ECD)	<p>Description of new components⁸ for the TOE type that are not based on components in either CC Part 2 or CC Part 3.</p>
6	11 – 19	Security Functional Requirements (APE_REQ)	<p>Contains two groups of requirements:</p> <ul style="list-style-type: none"> • The <i>security functional requirements (SFRs)</i> - a translation of the security objectives for the TOE into a standardized language, usually at a more detailed level of abstraction, to provide an exact description of what is to be evaluated • The <i>security assurance requirements (SARs)</i> - a description of how assurance is to be gained that the TOE meets the SFRs in a standardized language to provide an exact description of what is to be evaluated <p>Includes respective mappings of SFRs to security objectives and SARs to security objectives along with the justification for these two sets of mappings.</p>

⁷ Based on the logic that if all security objectives are achieved then the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

⁸ In this context a component is the smallest selectable set of elements on which requirements may be based.

3 IEEE Std 2600™-2008

3.1 Introduction

IEEE Std 2600™-2008, "Standard for Information Technology: Hardcopy System and Device Security" was developed by the Hardcopy Device and System Security Working Group, a standards project sponsored by the IEEE Information Assurance Standards Committee (IASC) of the IEEE Computer Society and was approved in 2008 by the IEEE Standards Association (IEEE-SA). The purpose of this standard is to guide manufacturers or users of hardcopy devices in the secure installation, configuration, or usage of these devices and systems. This reflects the increased awareness by industry and government agencies that networked printers and other hardcopy peripherals (such as copiers and multifunction devices) contain many of the same communications, processing and storage components and are connected to the same local or wide area networks as other components such as network connected workstations, servers and PCs. These networked HCDs are subject to many of the same security problems, threats and vulnerabilities as these other network nodes.

IEEE Std 2600 was also motivated by the enactment of laws and regulations that explicitly or implicitly include information security and privacy requirements. For example, the US has established laws such as the Health Insurance Portability and Accountability Act (HIPAA), which requires healthcare organizations to protect the privacy and security of confidential health information; the Safeguards Rule in the Gramm-Leach-Bliley Act, which calls on financial institutions to have comprehensive security programs that keep customer information secure and confidential; and portions of the Sarbanes-Oxley Act of 2002 that involve establishing and maintaining internal controls over the unauthorized disclosure and accuracy of a company's financial data. Failure to provide adequate hardcopy device and systems security could result in non-compliance with key portions of these laws and lead to severe penalties or legal action against users of hardcopy device and systems.

IEEE Std 2600 was therefore written to meet the two goals of:

1. Providing guidance in the secure architecture, design, and out-of-box configuration of HCDs for manufacturers.
2. Providing guidance in the secure installation, configuration, and use of HCDs for end users and their supporting organizations.

More specifically, the purpose for writing the IEEE Std 2600 was to:

1. Define the requirements for all aspects of security (including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users and IT professionals on the secure selection, installation, configuration and usage of hardcopy devices and systems; including printers, copiers, and multifunction devices.
2. Address issues related to security of hardcopy devices and systems such as authentication, authorization and the privacy of data sent to and from devices and residing on them, as well as such areas as data integrity and device management.
3. Identify security threats against hardcopy devices and systems and instruct manufacturers and software developers on appropriate security capabilities to include in their hardcopy devices and systems, and instruct users on appropriate ways to use these security capabilities.

3.2 IEEE Std 2600 Structure

IEEE Std 2600 is structured as follows:

- Clause 1 provides the scope and purpose of the standard and an overview of the standard's structure.
- Clause 2 provides the definitions, special terms, acronyms, and abbreviations used in the standard.
- Clause 3 describes the typical structure, architecture, and functions of a hardcopy device.
- Clause 4 describes the various security environments of hardcopy devices considered by the standard.
- Clause 5 describes the various assets of a hardcopy device.
- Clause 6 describes the threats against hardcopy devices that are considered by the standard.
- Clause 7 describes some of the mitigation techniques for manufacturers, IT administrators, and users to address each threat described in Clause 6.
- Clause 8 indicates specific security objectives by operational environment that are mandatory for conformance with the standard and provides example mitigation techniques that may be used to accomplish these objectives.
- Annex A describes the best practices for manufacturers, IT administrators, and users of hardcopy devices for various general security measures for hardcopy devices.
- Annex B provides additional references, which may add to the understanding of other parts of the standard.

3.2.1 IEEE Std 2600 Operational Environments

The assets, threats, mitigation techniques and security objectives described in the IEEE Std 2600 are centered on four general classes of operational environments that represent the types of operational environments that organizations and users would typically either implement or access. These four operational environment classes are described in the following clauses.

3.2.1.1 Operational Environment A

Operational Environment A is the “high accountability” Operational Environment. This operational environment covers information processing environments where (1) regulatory requirements such as HIPAA, (2) industry requirements such as the Payment Card Industry Data Security Standard (PCI DSS) or (3) the sensitive nature of the assets and information that needs to be protected necessitates what would be considered qualitatively as a “high” level of security.

Operational Environment A can also describe what could be termed “islands” (i.e., a portion of the equipment) located within another operational environment. A typical corporate enterprise environment, for example, would be classified as Operational Environment B. Within a corporate enterprise, for example, three desktops that hold confidential employee data and one printer that outputs that data could be thought of collectively as an Operational Environment A island within Operational Environment B.

Operational Environment A is described more fully in IEEE Std 2600 [B1], Clause 4.2.

3.2.1.2 Operational Environment B

Operational Environment B is the “Enterprise” Operational Environment. Operational Environment B covers the type of information processing environment one would typically find in a medium-to-large company or in governmental offices where security is important but not to the level that would be required

in Operational Environment A. In most respects, however, Operational Environment B is similar to Operational Environment A.

Operational Environment B is described more fully in IEEE Std 2600 [B1], Clause 4.3.

3.2.1.3 Operational Environment C

Operational Environment C is the “Public” Operational Environment. Operational Environment C addresses the type of information processing environment one would typically find in a public library or similar type of operation whose main role is to serve the public at large. Operational Environment C also covers businesses like retail print or copy shops or an internet café that services the public on a “for a fee” basis.

Operational Environment C is described more fully in IEEE Std 2600 [B1], Clause 4.4.

3.2.1.4 Operational Environment D

Operational Environment D is the “SOHO” (i.e., Small Office – Home Office) Operational Environment. Operational Environment D documents the type of information processing environment one would find in a home-run business, telecommuters who work from home or out of their car (such as service technicians) or small-to-medium businesses (typically with fewer than 50 employees).

Operational Environment D is described more fully in IEEE Std 2600 [B1], Clause 4.5.

3.3 Relationship to the IEEE Std 2600 Series of Protection Profiles

As described in 3.1, the scope of IEEE Std 2600 was to:

- Define security requirements for manufacturers, users, and others on the selection, installation, configuration and usage of hardcopy devices (HCDs)
- Provide a standard that identifies security exposures for these HCDs and systems
- Instruct manufacturers and software developers on appropriate security capabilities to include in their devices and systems
- Instruct users on appropriate ways to use these security capabilities

Correspondingly, the scope of the four Protection Profiles that comprise the IEEE Std 2600 Series of Protection Profiles is to document a standard for a Common Criteria Protection Profile for Hardcopy Devices to be used by manufacturers of hardcopy devices to:

- Write conformant Security Target documents for Common Criteria certification of their hardcopy device products
- Write conformant Protection Profiles for hardcopy devices

The IEEE Std 2600 Series of Protection Profiles are closely related to IEEE Std 2600. IEEE Std 2600 is a general standard for hardcopy device security containing a large amount of content that is beyond the scope of or otherwise inappropriate for a Common Criteria Protection Profile. However, the major security objectives of IEEE Std 2600 are codified as the four Protection Profiles that comprise the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]) so that hardcopy device vendors can develop conforming products and have them Common Criteria certified as such.

In particular, the mandatory⁹ security objectives in IEEE Std 2600 [B1] Clause 8.1.1 are represented in the Security Objectives (APE_OBJ) clause of IEEE Std 2600.1 [B8]. Similarly, the security objectives in IEEE

⁹Mandatory security objectives in IEEE Std. 2600 are distinguished by use of the word “shall”. Non-mandatory objectives use the word “should”.

Std 2600 [B1] Clause 8.1.2 are represented in the Security Objectives (APE_OBJ) clause of IEEE Std 2600.2 [B9], the security objectives in IEEE Std 2600 Clause 8.1.3 are represented in the Security Objectives (APE_OBJ) clause of IEEE Std 2600.3 [B10] and the security objectives in IEEE Std 2600 Clause 8.1.4 are represented in the Security Objectives (APE_OBJ) clause of IEEE Std 2600.4 [B11].

4 IEEE STD 2600 SERIES OF PROTECTION PROFILES

4.1 Introduction

This clause provides information about the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]) that were created to accompany IEEE Std 2600 [B1], and which this document is intended to support. Included in this clause are discussions as to why these four Protection Profiles were created, a discussion of the underlying model that the Protection Profiles are based on and a detailed discussion of the contents of the four Protection Profiles.

4.2 IEEE Std 2600 Series of Protection Profiles Structure and Content

4.2.1 Protection Profile and SFR Packages

4.2.1.1 Introduction and Rationale

Unlike most Protection Profiles, each Protection Profile within the IEEE Std 2600 Series of Protection Profiles is composed of a common PP section and one or more packages of Security Functional Requirements (SFRs). The purpose of this structure is to permit vendors to create conforming Security Targets (STs) for a variety of HCD configurations, ranging from a single-function device like a printer or copier to a complex multifunction device with options like nonvolatile storage or network interfaces.

This structure is necessary because the Common Criteria does not allow elements such as threats, policies, assumptions, or objectives to be applied only under certain conditions such as the presence of a fax function or network interface in a conforming product. In addition, some national CC Schemes regard any mention of functionality in a PP as an implicit requirement that conforming products provide that function. This is a general issue with the CC, not one that is particular to HCDs, and may be addressed in future versions of the CC.

The use of SFR packages was chosen after several alternatives had been explored. The concept of packages is described in Chapter 8 of the CC Part 1, Introduction and General Model [B2]. A package is a named set of security requirements, and may be either a functional package containing SFRs or an assurance package containing Security Assurance Requirements (SARs). Assurance packages are widely used to describe evaluation assurance levels.

The way this structure is used is that the common PP contains all of the necessary elements of a standard PP including all SFRs that are common to any supported HCD configuration. The SFR packages provide additional SFRs to support the additional functions that may be present in a particular supported HCD configuration. The common PP section is a complete PP, but in practice, it will usually be combined with at least one SFR package because few supported HCD configurations requiring certification are fully represented by only the common PP.

4.2.1.2 Common PP

The common PP applies to any supported HCD configuration and contains all of the necessary elements of a PP. These elements are:

- An introduction and overview of the TOE
- Conformance claims and conformance rules
- A security problem definition, including all threats, organizational security policies, and assumptions
- All security objectives for the TOE and its environment

- Extended component definitions that may be used either in the Common PP or in one or more of the SFR packages
- SFRs and SARs that apply to all supported HCD configurations

4.2.1.3 SFR Packages

SFR packages contain only those SFRs that apply to specific HCD functions. There are several packages available, and they can be combined to represent a wide variety of typical HCD configurations. These SFR packages are:

PRT – SFR Package for Hardcopy Device Print Functions

SCN – SFR Package for Hardcopy Device Scan Functions

CPY – SFR Package for Hardcopy Device Copy Functions

FAX – SFR Package for Hardcopy Device Fax Functions

DSR – SFR Package for Hardcopy Device Document Storage and Retrieval Functions

NVS – SFR Package for Hardcopy Device Nonvolatile Storage Functions

SMI – SFR Package for Hardcopy Device Shared-medium Interface Functions

For example:

1. If the TOE of a conforming ST is a printer, then that ST would conform to the PRT SFR package.
2. If the TOE is a fax machine that can also make local copies, then its ST would conform to the FAX and CPY SFR packages.
3. If the TOE is a multifunction printer/scanner/copier with a network interface, then its ST would conform to the PRT, SCN, CPY, and SMI SFR packages.

The requirements specified by each SFR package are additive. Applied to the previous set of examples:

1. An ST that conforms to the PRT package would need to satisfy the common PP requirements *and* the PRT requirements.
2. An ST that conforms to the FAX and CPY packages would need to satisfy the common PP requirements *and* the FAX requirements *and* the CPY requirements.
3. An ST that conforms to the PRT, SCN, CPY, and SMI packages would need to satisfy the common PP requirements *and* the PRT, SCN, CPY, *and* SMI requirements.

4.2.1.4 Conformance rules

There are three conformance rules in the PP for all conforming STs:

1. The ST must claim demonstrable conformance to the PP. This is a normal conformance rule for Protection Profiles. Demonstrable conformance is defined in Annex D of the CC Part 1, Introduction and General Model [B2].
2. If a TOE performs a function that is specified for one of the SFR packages, then its ST must also claim demonstrable conformance to that SFR package. This rule ensures that all conforming products satisfy all applicable security functional requirements that apply to the configuration of the TOE. The functions are defined in the SFR Packages Introduction clause of the standard.
3. A TOE must perform at least one of the following functions: printing, scanning, copying, and faxing. This rule ensures that the PP is applied to a hardcopy device and not some other kind of device.

4.2.2 TOE Model

4.2.2.1 Introduction and Rationale

In addition to supporting many different HCD configurations, the IEEE Std 2600 Series of Protection Profiles are designed to support a wide variety of implementations, independent of particular vendors, architectures, and nomenclatures. Therefore, an abstract, implementation-neutral TOE model has been used. The model is intended only to address those elements that are needed to describe the security problems and solutions of HCDs: users, assets, operations, and channels.

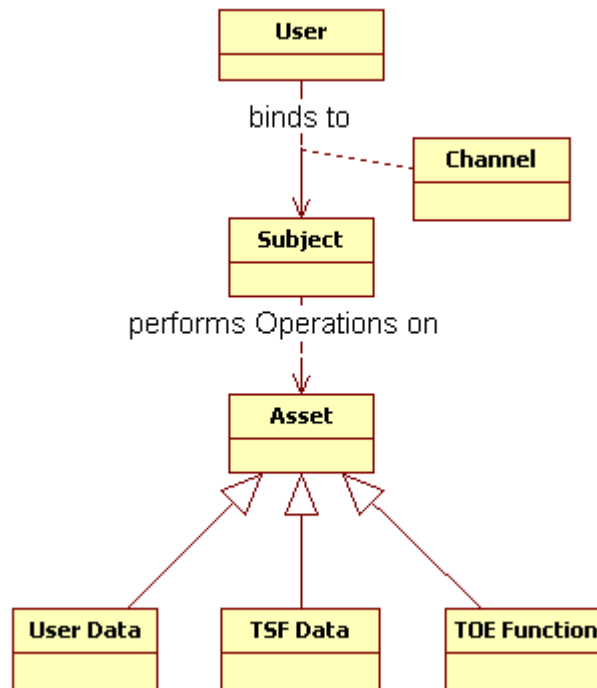


Figure 1 TOE Model

Items in Figure 1 are further discussed in the following subclauses.

4.2.2.2 Users and Subjects

Figure 1 indicates that Users bind to Subjects. This concept of binding is an important concept in the underlying model the Common Criteria uses to define the various Security Functional Requirements in Common Criteria Part 2 [B3]. What “binding” means in this context is that for a User to make use of the TOE Security Functions implemented in the TOE, one or more Subjects will have to be activated. In activating Subjects, some or all of the User’s security attributes become associated with the Subjects when they are activated. Putting this concept in different words, once it is activated a Subject acts on behalf of the User that activated it to perform some task associated with one or more TOE security functions.

The action of a User associating all or part of that User’s security attributes with an activated Subject that then acts on behalf of the user to perform some Operation is denoted by the Common Criteria as “binding”. The rules governing how a User binds with a Subject for a given TOE (i.e., how the User’s security attributes become initially associated with a Subject or are changed) are defined in the FIA_USB (User-subject binding) SFR (see Common Criteria Part 2 [B3] for a more detailed description of the FIA_USB SFR).

As indicated in Clause 5.2 in any PP from the IEEE Std 2600 Series of Protection Profiles [B8]-[B11], Users are not distinguished from Subjects. This is because in the case of most HCDs the two entities are treated as the same with the same security attributes. As an example, if a user sends network credentials to an external server to be authenticated, the actual user enters in the credentials (like username and password) to the HCD which are then passed on to the Third Party server that does the actual authentication. From an HCD perspective the operation is to pass through the credentials to the network interface; the Subject that performs the operation can be thought of as the user, so for all practical purposes the User and the Subject are the same entity in this case. A secondary reason for equating Users and Subjects for the four PPs is that the Common Criteria doesn't handle the distinction between Users and Subjects in a clean way in some SFRs.

However, an ST Author is always allowed in an ST to distinguish between Users and Subjects if that makes sense for the TOE in question. If that is desired, the ST Author should make sure that in the FIA_USB.1 SFR this distinction is made very clear, that the rules for associating User and Subject security attributes are clearly defined in the FIA_USB.1 SFR, and that some type of Application Note is provided that indicates why Users and Subjects are being distinguished from each other for this TOE.

4.2.2.3 Users

Only two kinds of users are defined: Normal and Administrator. A Normal user (U.NORMAL) is one who is authorized to perform hardcopy operations. An Administrator (U.ADMINISTRATOR) is one who is authorized to manage some or all of the TOE in ways that affect TOE security. In situations where any authorized user is concerned, the designation U.USER is employed.

There may be other kinds of users, such as those who are authorized to manage parts of the TOE that do not affect security. Those users do not need to be considered in the PP or in a conforming ST.

There also may be specializations of users, such as Normal users who are allowed or denied printing in color, or Administrators who can modify user accounts but cannot modify the TOE's networking parameters. Those specializations may need to be considered in a conforming ST, and it is the responsibility of the ST Author to define their roles and permissions accordingly. If specialized roles are defined in an ST, they should be defined as specializations of one of the different kinds of users (i.e., of U.NORMAL and U.ADMINISTRATOR).

4.2.2.4 Assets

Generally speaking, an asset is something that its owner considers to be valuable. That value may be tangible or intangible, and in many cases, the value only becomes apparent in the absence of the asset. HCD assets can be broadly categorized as:

1. Documents that are being processed or stored by the TOE. Documents are typically valued in terms of some cost associated with unauthorized access, such as disclosure, modification, or in some cases, possession or use.
2. Information about document processing that is pending or occurring. Information about document processing is typically valued in terms of how it might be misused to alter an active processing job.
3. Information that is relevant to the security of the TOE, its IT environment, or its records of usage. Security-relevant information is typically valued in terms of how the information can be misused by unauthorized persons for such purposes as to defeat the security policies of the TOE, to attack other related information systems, to learn from the descriptive names of documents or to analyze traffic for usage. In some cases, unauthorized disclosure and modification pose a security risk, but in other cases disclosure is benign (and perhaps operationally necessary) but unauthorized modification poses a security risk.

4. The use of the TOE itself. Use is typically valued in terms of some cost associated with unauthorized use. Depending on the customer's environment, it may be lost revenue, misallocation of budgets, or deprivation of authorized use.

For CC purposes assets need to be categorized somewhat differently than HCD assets are typically categorized because the CC distinguishes between data that is (a) created by and for users, which does not affect the operation of the TSF, and (b) created by and for the TOE, which might affect the operation of the TSF.

4.2.2.4.1 User Data

User Data is categorized as either User Document Data (D.DOC), representing documents that are being processed or stored by the TOE, and User Function Data (D.FUNC), representing information about document processing that is pending or occurring.

4.2.2.4.2 TSF Data

TSF Data is categorized as either TSF Protected Data (D.PROT), representing security-relevant information for which disclosure is acceptable but unauthorized alteration would have an adverse effect on security, and TSF Confidential Data (D.CONF), representing security-relevant information for which either unauthorized disclosure or alteration would have an adverse effect on security.

The choice of categorizing specific data objects as either Protected or Confidential is one of the key responsibilities of the ST Author. Some examples are given in the PP, but the ST Author is required to identify and categorize TSF Data because such choices depend on the particular architecture and implementation of a conforming product.

4.2.2.4.3 Functions

Functions refer to the ability to perform document processing operations such as printing, scanning, copying, faxing, and storage/retrieval. Authorization to perform such operations is controlled by access controls. The PP does not consider options within those functions, such as the option to print in color, because that kind of option is related to cost control and not security control.

4.2.2.5 Operations

Access controls are specified in terms of five operations that can be performed by a subject on an object: 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).

4.2.2.6 Channels

The IEEE Std 2600 Series of Protection Profiles introduces a new term, "channels", to describe all of the mechanisms through which data can be transferred into and out of the TOE. Two of the channels are for hardcopy handlers (input and output), and the other two channels are for electronic and operator interfaces (private-medium and shared-medium).

The distinction between private-medium and shared-medium interfaces is that the communications medium used by a shared-medium interface can be simultaneously accessed by multiple users and therefore requires additional security measures to mitigate the threat of intercepted communications.

Examples of shared-medium interfaces are Ethernet, Wi-Fi¹⁰, and Bluetooth¹¹. Although Bluetooth is

¹⁰ The Wi-Fi® trademark is owned by the Wi-Fi Alliance [C5]

¹¹ The Bluetooth® trademark is owned by the Bluetooth Special Interest Group (SIG) [C6]

considered a “personal area network” with limited physical range, it is nonetheless subject to intercepted communications in much the same way as a Wi-Fi® connection.

Examples of private-medium interfaces are IEEE 1284 “parallel port”, USB (but not wireless USB), IrDA®¹², and an HCD’s operator panel. Although IrDA® is a wireless interface, it makes a line-of-sight connection and its communications are not likely to be intercepted.

4.2.3 Threats, Policies, and Assumptions

4.2.3.1 Introduction and Rationale

Conventional threat definitions include a threat agent, an asset, and an adverse result of some action of the threat agent against the asset. In most but not all cases in this PP, it was possible to define threats using those components. However, some cases were not as straightforward and required the use of Organizational Security Policies (OSPs).

4.2.3.2 Threats

Threats are described in very general terms: there are threats of unauthorized disclosure or alteration of User Document Data and TSF Confidential Data, and threats of unauthorized alteration of User Function Data and TSF Protected Data.

This is different from how threats are described in IEEE Std 2600 [B1]. For example, for threats of unauthorized access, IEEE Std 2600 distinguishes between data at rest and data in transit. The PP cannot make such a distinction and also maintain independence from requiring network functionality that is implied by “data in transit”. Instead, the PP identifies general threats of unauthorized access, counters them with general objectives to protect against unauthorized access, and fulfills the objectives with access control requirements. If networking functionality is present, then the SFR package for shared-medium interfaces places additional requirements for use of trusted channels of communication that further fulfill the general objective.

4.2.3.3 Organizational Security Policies

Due to the general applicability of the PPs to a variety of customer environments, some security risks could not be described in terms of clearly identified threats against assets by threat agents. In such cases, the PPs use Organizational Security Policies (OSPs) as the basis for objectives and functional requirements.

For example, it is generally understood that user authorization is needed for security, but the reason it is needed depends on factors that are known only by individual customers. Customers might want to prevent unauthorized access to document data, ensure auditability of access to document data, ensure accountability of HCD usage, or some combination of these or other purposes. Instead of presuming the customer’s purpose for requiring user authorization, an OSP is used to require authorization based on unstated policies of the TOE’s owner.

Similarly, OSPs are used to require audit logging (in some environments), software self-test, and protection of external interfaces from misuse.

4.2.3.4 Assumptions

Not all security risks can be countered solely by IT mechanisms, and some assumptions about the TOE environment and personnel are needed to help ensure the success of those IT mechanisms that are employed. In these PPs, there are two categories of assumptions:

¹² The IrDA® trademark is owned by the Infrared Data Association.

1. Physical and logical protection of the TOE.
2. Training and trust of personnel.

Physical protection is assumed, because otherwise, the TOE could be subjected to physical, electrical, or software alteration that is beyond the scope of a PP at or below Evaluation Assurance Level 3.

Logical protection of the TOE is assumed, because unrestricted public access to interfaces would subject the TOE to threats that are beyond the scope of a PP at or below Evaluation Assurance Level 3.

Training of normal users, and training and trust of personnel is assumed, because without such assumptions, there is little assurance that IT-based security mechanisms will be faithfully configured and used.

4.2.4 Security Objectives

4.2.4.1 Objectives that Counter Threats

Each threat has a companion access control objective for the TOE. For example, the threat that document data is disclosed (T.DOC.DIS) to unauthorized persons has a companion TOE objective O.DOC.NO_DIS.

To support those objectives, there is a TOE objective that users are identified, authenticated, and authorized (O.USER.AUTHORIZED) and a non-IT environment objective that the TOE Owner authorizes users according to security policies (OE.USER.AUTHORIZED).

4.2.4.2 Objectives that Enforce OSPs

The OSP that users must be authorized is enforced by a TOE objective that users are identified, authenticated, and authorized (O.USER.AUTHORIZED) and a non-IT environment objective that the TOE Owner authorizes users according to security policies (OE.USER.AUTHORIZED).

The OSP that software is self-verified (P.SOFTWARE.VERIFICATION) is enforced by a TOE objective to self-verify its software (O.SOFTWARE.VERIFIED).

The OSP that security-relevant events are maintained in a protected log which is reviewed by authorized personnel (P.AUDIT.LOGGING) is enforced by a TOE objective to record such events (O.AUDIT.LOGGED) IT environmental objectives to provide protected storage and authorized access to such logs (OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED), and a non-IT environment objective that such logs are reviewed (OE.AUDIT.REVIEWED). The default case is that the storage of and access to audit logs is performed outside of the TOE. If one or both can be performed inside the TOE, then the ST Author would need to create TOE objectives that parallel the IT environmental objectives (see 4.2.5.1 for details).

The OSP that external interfaces are protected (P.INTERFACE.MANAGEMENT) is enforced by a TOE objective to manage the use of interfaces (O.INTERFACE.MANAGED) and an IT environmental objective that the interfaces are protected from unmanaged access (OE.INTERFACE.MANAGED).

4.2.4.3 Objectives that Uphold Assumptions

The assumption that physical access to the TOE is protected (A.ACCESS.MANAGED) is upheld by a non-IT environmental objective to restrict or monitor access to the TOE (OE.PHYSICAL.MANAGED).

The assumptions that users are trained or trusted (A.USER.TRAINING, A.ADMIN.TRAINING, and A.ADMIN.TRUST) are upheld by companion non-IT environmental objectives (OE.USER.TRAINED, OE.ADMIN.TRAINED, and OE.ADMIN.TRUSTED, respectively).

4.2.5 Security Functional Requirements

4.2.5.1 Extended Components

Common Criteria Part 1 [B2] mandates that all of the security components¹³ for a TOE (in the case of a Security Target) or for a class of TOEs (in the case of a Protection Profile) should be based on either Common Criteria Part 2 [B3] (for Security Functional Requirements) or Common Criteria Part 3 [B4] (for Security Assurance Requirements). However, Common Criteria Part 2 [B2] also recognizes that there are two cases where that might not be possible:

- The security objectives for the TOE (or class of TOEs) cannot be translated to one of the SFRs in Common Criteria Part 2 [B3].
- A security objective for the TOE (or class of TOEs) can be translated to one of the SFRs in Common Criteria Part 2 [B3], but only with great difficulty and/or complexity.

In these two situations, the ST or PP is allowed to define a unique component just for that ST or PP called an ‘Extended Component’. The rules that apply to the labeling, format, level of detail, etc., for the components defined in Common Criteria Part 2 or 3 ([B3] or [B4]) must apply to the ‘Extended Component’.

In the case of the IEEE Std 2600 Series of Protection Profiles it was found that Extended Components were needed in two instances:

1. There is no existing SFR in Common Criteria Part 2 [B3] that adequately defines the requirements for protecting the confidentiality and integrity of removable nonvolatile storage (see 9 for the definition of this term) when that storage is removed from the TOE. Existing SFRs in the FDP Class for User data protection and in the FPT class for Protection of the TSF do address protection of the confidentiality and integrity of User Data and TSF Data, respectively, but not in a consistent way.

Since both User Data and TSF Data can be stored in removable nonvolatile storage, what is needed is an SFR that consistently deals with the requirements for protection of the confidentiality and integrity of both types of data in a consistent way. Hence the FPT_CIP_EXP.1 (Confidentiality and Integrity of Stored Data) extended component was created for the IEEE Std 2600 Series of Protection Profiles.

2. There is no existing SFR in Common Criteria Part 2 [B3] that addresses protection of both User Data and TSF Data as that data are directly forwarded from one external interface to another external interface. As was the case for FPT_CIP_EXP.1, the FDP Class and FPT Class both have SFRs that address protection of User Data and TSF Data, respectively, as that data is either exported from the TOE via an external interface to another trusted IT product or imported from another trusted IT product outside of the TOE into the TOE via an external interface.

However, neither class had an SFR that addressed both User Data and TSF Data in a consistent manner, and just as importantly, addressed the ability to prohibit the direct forwarding of both types of data from one external interface to another when such a prohibition was needed. As a result, for the IEEE Std 2600 Series of Protection Profiles the FPT_FDI_EXP.1 (Restricted forwarding of data to external interfaces) extended component was created.

More guidance on both of these extended components can be found in 6.9.9 Items a) and b), respectively.

4.2.5.2 Objectives that May be Fulfilled by the TOE or Its Environment

Depending on the architecture and implementation of a particular conforming TOE, some functions could be performed using resources in the TOE’s IT environment, or performed internally within the TOE, or performed either or both ways at the option of the TOE administrator. To allow for these variations, the default requirement is that such functions are performed using resources in the environment.

¹³ A component is defined in [B2] as the “smallest selectable set of elements on which requirements may be based”.

This default was chosen because from the TOE's point of view, that is the least restrictive approach and it allows the ST Author to opt for the more restrictive approach of performing those functions internally within the TOE. By choosing the least restrictive approach as the default requirement, the ST Author can maintain demonstrable conformance to the PP if he/she opts for a more restrictive approach.

If a conforming ST allows a function to be performed internally or externally, at the option of the administrator, then both situations should be expressed in the ST as distinct modes of operation so that they can be evaluated separately.

The two cases in which this situation occurs in the PPs are:

1. User identification and authentication
2. Audit log storage protection and access restriction

4.2.5.3 Objectives Fulfilled by PP SFRs and Package SFRs

All security objectives are fulfilled by SFRs in the common PP section, but some additional requirements are needed to completely fulfill those objective in the presence of optional functions represented by SFR packages. The Shared-medium Interface package provides several good examples of this:

1. In the common PP, data protection objectives are fulfilled by requiring access controls. However, by introducing data in transit over a shared-medium interface, those access controls no longer provide complete protection. Additional protection is provided by a new requirement to use trusted channels for communications through that interface.
2. In the common PP, interface management objectives are fulfilled by requiring user identification and authentication and by terminating inactive sessions. However, by introducing interfaces to a shared-medium, additional measures are needed to protect against misuse of those interfaces. That protection is provided by a new requirement to ensure that data transmitted to those interfaces is under TSF control.
3. As a side-effect of requiring the use of trusted channels, some additional security-relevant events must be logged. This results in an additional audit generation requirement in this package.

Additional requirements appear in each of the SFR packages that are specified in the PP for each operational environment. If an SFR package is not included in a particular operational environment, this means that no additional requirements were created by the presence of a function. For example, the SFR package for a printing function (PRT) appears in the PPs for operational environments A and B, but not C or D, because the objective to protect document data from unauthorized disclosure is present in environments A and B but is not present in environments C or D. However, for operational environments C and D security objectives for printers are adequately covered by the SFRs in the common PP section.

4.2.6 Dependencies in SFR Packages

All SFR dependencies are resolved in the common PP. However, some SFR dependencies in the SFR packages are not resolved within the same package but instead rely on the presence of the dependent SFRs in the common PP.

For example, the dependency of FAU_GEN.1 on FPT_STM.1 is not resolved in the Shared-medium Interface package (SMI), but instead relies on the presence of FPT_STM.1 in the common PP.

A more interesting example is in the PRT, SCN, CPY, FAX, and DSR packages. In those packages, there are access control security function policies (SFPs) that include FDP_ACF.1. FDP_ACF.1 has a dependency on FMT_MSA.3, which is present in the common PP. The packages can resolve the dependency on FMT_MSA.3 by relying on its presence in the common PP, but only if the ST Author adds the SFP from the package to the list of SFPs that are specified in FMT_MSA.3.

5 IEEE STD 2600 SERIES OF PROTECTION PROFILES – VENDOR USAGE GUIDELINES

5.1 Introduction

This clause provides some detailed guidance on how to use the IEEE 2600 Series of Protection Profiles, from the perspective of a vendor that wants to certify a product that conforms to a PP selected from the IEEE Std 2600 Series of Protection Profiles.

For this guidance some general conventions will be used as follows:

1. Any threats, assumptions and security objectives mentioned in this document are defined and described in detail in the PPs that comprise the IEEE Std 2600 Series of Protection Profiles ([B8] - [B11]).
2. The four PPs that comprise the IEEE Std 2600 Series of Protection Profiles ([B8] - [B11]) together define seven Security Functional Requirement (SFR) packages that will be denoted in this clause as follows:
 - PRT (Print) -- 2600.x-PRT SFR Package for Hardcopy Device Print Functions¹⁴
 - SCN (Scan) -- 2600.x-SCN SFR Package for Hardcopy Device Scan Functions¹⁵
 - CPY (Copy) -- 2600.x-CPY SFR Package for Hardcopy Device Copy Functions¹⁵
 - FAX (Facsimile) -- 2600.x-FAX SFR Package for Hardcopy Device Fax Functions¹⁵
 - DSR (Document Storage and Retrieval) -- 2600.x-DSR SFR Package for Hardcopy Device Document Storage and Retrieval Functions¹⁵
 - NVS (Nonvolatile Storage) -- 2600.x-NVS SFR Package for Hardcopy Device Nonvolatile Storage Functions¹⁵
 - SMI (Shared-medium Interface) -- 2600.x-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions¹⁵

5.2 Choosing the Appropriate Operational Environment For Certification

In selecting an operational environment for product certification, two key criteria should be considered:

1. Functional criteria: the product has operational functions or features supporting the usage scenarios for users in the particular operational environment.

Selecting which Operational Environment an HCD product should be certified against could be looked at several ways. One of these ways is to look at the major features – like printing, copying, scanning, faxing - and potential usage scenarios for that product irrespective of what security features might be included in the machine.

As an example, consider a small 15 pages per minute (ppm) stand-alone personal printer in a doctor's office¹⁵. The fact that this printer is in a doctor's office in and of itself does not necessarily mean that this device should be considered part of Operational Environment A where regulatory compliance issues (HIPAA in this case) necessitate a certain degree of information security to protect patient records and patient confidentiality. If the printer is only being used to print blank information forms for completion by the patient HIPAA would probably not apply so Operational Environment A would not be the appropriate environment for certifying this printer. More likely Operational Environment D

¹⁴ Where x=1 for Operational Environment A; x=2 for Operational Environment B; x=3 for Operational Environment C and x=4 for Operational Environment D.

¹⁵ The reader is reminded that the intended use of an HCD determines the appropriate operational environment, and therefore the security features that are required to support that appropriate operational environment, and not the size, speed or complexity of the HCD.

would be the appropriate environment for certifying this printer because the TOE does not need to protect document data; it only needs to be secured against network-based attacks that could be used to compromise other systems in the doctor's office.

On the other hand, if you take this same 15 ppm stand-alone personal printer in a doctor's office, but now the doctor uses this printer to print patient bills or patient medical information (e.g., test results) now you have a different scenario. HIPAA likely does now apply to this use of the printer, so Operational Environment A might very well be the applicable environment because now the confidentiality of patient information comes into play.

Let's take another example, in this case a 30 ppm HCD that does print-copy-scan-fax. The fact that we have an HCD doesn't imply any specific operational environment until we look at how this HCD is used. If the HCD were not network connected and in a public library where it was only used by library patrons to make copies of pages or print articles, then Operational Environment C would almost certainly apply because of the public-facing nature of the device. If this same HCD was network connected in a 10-person architect's office where it is used to print/copy/fax blueprints, building plans, etc. then Operational Environment D would be the appropriate choice because, as indicated in 3.2.1.4, we have here a small, private information processing environment where most of the security is provided by office members keeping track of visitors and their access to the device.

Take this same network connected device and put it in a 100-person engineering office for a defense contractor and then either Operational Environments A or B would apply. Which of these two Operational Environments applies depends mainly on whether the device handles day-to-day information (both proprietary and non-proprietary) needed to operate the business as described in 3.2.1.2 (in that case Operational Environment B would apply) or handles cost and confidential information governed by government regulations as described in 3.2.1.1 (in that case Operational Environment A would apply).

Functional criteria are used for determining what products belong in which operational environment by the non-security related functions or features they must have for the environment. The criteria that is used for determining what HCDs belong in a specific Operational Environment is based on both security and non-security related functions or features; however, an ST, by definition, must describe only the security-related functions or features of the targeted HCD.

2. Security criteria: the product has security functions or features suitable for solving the security problems in the particular operational environment specified in IEEE Std 2600.

Some of the general types of security features that an HCD can provide are:

- Identification, authentication and authorization of users/System Administrators before being able to access the appropriate functions of the HCD.
- Protection against disclosure of residual User Document Data that may reside on the HCD after processing of a user document is completed.
- Protection of HCD configuration parameters, settings, logs, and other security information from unauthorized disclosure or alteration.
- Protection of internal HCD software, firmware or other digital resources like downloadable fonts from unauthorized alteration while residing on the HCD.
- Recording and analysis of logs of security-related events or HCD functions that occur within the HCD.
- Protection of User Data and TSF Data that is sent between the HCD and another trusted IT product over a network interface from unauthorized disclosure or alteration.

5.3 Guidelines for Distinguishing Among the Four IEEE Std 2600 Operational Environments

This subclause provides guidelines on some elements a product vendor should consider in determining whether the HCD to be certified provides suitable solutions for the security problems identified in the four IEEE Std 2600 Operational Environments.

1. **The assets the product must protect.**

Table 2 compares the assets that must be protected and what kinds of protections are required at a minimum among the four Operational Environments.

Table 2. Assets Protected Per Operational Environment¹⁶

Asset	Operational Environment			
	A	B	C	D
User Document Data	UD, UA	UD ¹⁷ , UA ¹⁹	UD ¹⁸	
User Function Data	UA	UA ¹⁹		
TSF Protected Data	UA	UA	UA	UA
TSF Confidential Data	UA, UD	UA, UD	UA, UD	UA, UD
External Interfaces	UU	UU	UU	UU
Executable Code	UM	UM	UM	UM
Audit Logs	UA, UD	UA, UD	UA, UD	

Key: UD – Protected from Unauthorized Disclosure
 UA – Protected from Unauthorized Alteration
 UU – Protected from Unauthorized Usage
 UM – Protected from Unintentional Malfunction

ST must provide the complete list of user data and TSF Data to be protected by the TOE (here the TOE is the product being described by the ST). The asset list must cover the assets listed in the above table for a particular environment.

2. **The security assumptions made in the environment.**

Table 3 compares the assumptions for the four different Operational Environments.

Table 3. Security Assumptions Per Operational Environment¹⁹

Assumption	Operational Environment			
	A	B	C	D
A.ACCESS.MANAGED	√	√	√	√
A.USER.TRAINING	√	√		
A.ADMIN.TRAINING	√	√	√	√
A.ADMIN.TRUST	√	√	√	√

The ST must not make more assumptions than those assumptions specified in the PP from the IEEE Std 2600 Series of Protection Profiles associated with each Operational Environment. If an assumption is removed, either of the two conditions must be true:

¹⁶ The definition of each asset can be found in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

¹⁷ At rest (stored) only

¹⁸ Deleted data only

¹⁹ The definition of each assumption can be found in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

- The product must provide sufficient security features or functions so that by the enforcement of these security features or functions the removed assumption will always be evaluated to true.
- The organization in the environment will enforce additional organizational security policies (OSPs) so that by enforcing these OSPs the removed assumption will always be evaluated to true.

As an example, if an HCD is placed in a company with a large number of employees there is always the concern that in tough economic times large involuntary employee layoffs could occur. In such an environment there is a strong likelihood of insider threats by employees due to reasons such as retaliation for layoffs or firings or due to industrial espionage. Senior management would want to make sure that access to HCDs is properly managed so laid off employees can't somehow copy or destroy files after they have been laid off. In addition, they would want to make sure that employees and administrators are properly trained in the company's policies and practices governing improper access to HCDs and that the administrators are trusted to follow the applicable corporate policies. In this type of environment all four assumptions would apply, so a vendor should treat this environment as either Operational Environment A or B for security purposes. Determining which one of the environments would depend on some of the other factors discussed in this clause, showing that these factors cannot be considered in isolation of each other.

Contrast this with a hotel business center. You would want any administrators to be properly trained and trusted in this case because HCD resources tend to be very valuable and you would also want access to the HCDs properly managed so that the HCDs do not just disappear one night. However, user training is not critical because HCDs in hotel business centers typically provide only basic functions like printing, faxing and Internet access that most users know how to use already or can learn very quickly on their own. In that type of environment, from Table 3 it would be clear that the Hotel providing this Business Center should treat this environment as either Operational Environment C or D (in this case taking other factors into consideration it would likely be Operational Environment C).

3. **Security objectives of the TOE and Operational Environments.**

Table 4 compares the security objectives for the TOE in each of the four Operational Environments.

Table 4. Security Objectives of the TOE and Operational Environment²⁰

Security Objective	Operational Environment			
	A	B	C	D
O.DOC.NO_DIS	√			
O.DOC_REST_NO_DIS		√		
O.DOC_DELETED.NO_DIS			√	
O.DOC.NO_ALT	√			
O.DOC_REST_NO_ALT		√		
O.FUNC.NO_ALT	√			
O.FUNC_REST.NO_ALT		√		
O.PROT.NO_ALT	√	√	√	√
O.CONF.NO_DIS	√	√	√	√
O.CONF.NO_ALT	√	√	√	√
O.USER.AUTHORIZED	√	√		
O.ADMIN.AUTHORIZED ²¹			√	√
O.INTERFACE.MANAGED	√	√	√	√
O.SOFTWARE.VERIFIED	√	√	√	√

²⁰ The definition of each OSP can be found in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

²¹ In Operational Environments A and B, identification, authentication and authorization of administrators to perform administrative functions is implicitly included as part of the O.USER.AUTHORIZED security objective.

Security Objective	Operational Environment			
	A	B	C	D
O.AUDIT.LOGGED	√	√	√	
OE.AUDIT_STORAGE.PROTECTED	√	√	√	
OE.AUDIT_ACCESS.AUTHORIZED	√	√	√	
OE.INTERFACE.MANAGED	√	√	√	√
OE.PHYSICAL.MANAGED	√	√	√	√
OE.USER.AUTHORIZED	√	√		
OE.ADMIN.AUTHORIZED ²²			√	√
OE.USER.TRAINED	√	√		
OE.ADMIN.TRAINED	√	√	√	√
OE.ADMIN.TRUSTED	√	√	√	√
OE.AUDIT.REVIEWED	√	√	√	

The product described by the ST must have functions or features covering all security objectives listed in Table 4 for the product’s intended Operational Environment.

The product may have more security features or functions covering security objectives other than those listed in the above table. If so, these security features or functions must not violate the assumptions made in the environment or any security objectives listed in the above table for a particular environment. However, a TOE can always be more restrictive in terms of any assumptions made in the environment or any security objectives included in the ST. For example, the OE.AUDIT.REVIEWED security objective in IEEE Std 2600.1, IEEE Std 2600.2 and IEEE Std 2600.3 states that the TOE owner will make sure that audit logs are reviewed at appropriate intervals. As these three PPs are written this objective can be met by the TOE’s non-IT environment; there is nothing that prohibits an HCD vendor in a device designed for an Operational Environment A customer to implement the function of reviewing audit logs in the TOE itself. In that case the ST would indicate that the assumption is a “Security Objective of the TOE” and not a “Security Objective for the non-IT environment”, but the ST would still conform to IEEE Std 2600.1 for this case.

The reverse is not true. An HCD vendor cannot design an HCD so that one of the assumptions or security objectives required by the TOE to perform is moved to the IT or non-IT environment. For example, suppose an HCD vendor wanted to develop an HCD that would conform with IEEE Std 2600.1. The O.AUDIT.LOGGED security objective requires that the TOE create and maintain an audit log; if the HCD in this instance didn’t create and maintain an audit but assumed that this would be done in the non-IT environment, this HCD could not claim conformance to IEEE Std 2600.1 because the TOE didn’t meet its required security objectives.

It is noted here that conformance to IEEE Std 2600.1 can be claimed if the HCD creates and maintains the required auditable event log entries and then downloads these log entries to an audit log stored externally to the HCD in some trusted IT product. This is because once the audit log entries are downloaded from the HCD the HCD is no longer responsible for storage and maintenance of the audit log entries; that is being done by the IT environment.

With this in mind, let’s look at a some examples of the applicable Security Objectives can influence the choice of Operational Environment. Consider first the large company used in the example applied to Table 3. Large companies tend to be subject to many different types of regulations depending on the nature of the business and have serious concerns for both internal and external threats to access confidential company data for profit motives. In such companies senior management has to make sure that company protected data²³ is not disclosed to unauthorized persons while company confidential data is not disclosed to or modified by unauthorized persons, especially when that data is being stored

²² In Operational Environments A and B, permission by the TOE Owner for administrators to perform administrative functions is implicitly included as part of the OE.USER.AUTHORIZED security objective.

²³ See 6.4 for a further discussion of TSF Protected Data vs. TSF Confidential Data.

on the HCD device. Thus the ‘NO_DIS’ and ‘NO_ALT’ security objectives in Table 4 would apply to these types of companies. To counter the insider threats management would want to make sure that users are properly authorized to access HCDs when they attempt to do so, thus making the O.USER.AUTHORIZED security objective valid here also.

You could run through the similar arguments for all the other security objectives listed (for example, large companies usually have a need to manage physical access to critical or sensitive corporate accesses thus making the OE.PHYSICAL.MANAGED security objective important) and show that because of the security objectives required large companies should normally be considered as Operational Environment A or B. Note that from a security objective perspective the main difference between Operational Environments A and B is that in Operational Environment B User Document Data and User Function Data only has to be protected from unauthorized disclosure or alteration, as applicable, when that data is at rest (i.e., is being stored in the device), whereas in Operational Environment A User Document Data and User Function Data has to be protected from unauthorized disclosure or alteration in all cases – both at rest and in transit to/from the HCD. The large company in this example would have to assess the security risk to its data when it is in transit as well as when it is being stored in the HCD to decide whether Operational Environment A or B applied.

If we take the hotel business center that we used in discussing Table 3, the security objectives dealing with protected and confidential data would be valid here because there would have to be provisions made for customers to process data that to the customer is considered either protected or confidential data. The hotel business center would probably not need to worry much about logging and analyzing audit events on its HCDs but you would still want to make sure the HCDs were properly administered and physically monitored so that unauthorized persons are prevented from misusing the HCD. In addition, by the nature of a hotel business center being registered at the hotel is usually sufficient to obtain the “user authorization” credentials needed to use the center (so no special user authorization security objective is warranted) and the same rationale discussed for Table 3 applies here also for not needed a security objective around user training. If you go through a similar analysis on all the security objectives in Table 4 one could conclude that a hotel business center would fall under the security objectives consistent with Operational Environment C.

4. **The organizational security policies (OSPs) in the environment.**

Table 5 compares the organizational security policies that must be enforced in the four Operational Environments.

Table 5. OSPs Per Operational Environment²⁴

OSP	Operational Environment			
	A	B	C	D
P.USER.AUTHORIZATION	√	√		
P.ADMIN.AUTHORIZATION ²⁵			√	√
P.SOFTWARE.VERIFICATION	√	√	√	√
P.AUDIT.LOGGING	√	√	√	
P.INTERFACE.MANAGEMENT	√	√	√	√

In determining the applicable Operational Environment based on review of relevant OSPs, the HCD vendor should keep in mind that a product can add more OSPs than the ones listed in the above table for the desired Operational Environment and still claim conformance with the applicable PP from the IEEE Std 2600 Series of Protection Profiles, as long as the added OSPs do not make the security

²⁴ The definition of each OSP can be found in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

²⁵ In Operational Environments A and B, the organizational policy that governs authorization of administrators to manage the TOE is implicitly included as part of the P.USER.AUTHORIZATION OSP.

objectives for the product less strict than the required OSPs for the desired Operational Environment²⁶. A possible exception might be in the case that one of the assumptions listed in Table 5 is removed in favor of a corresponding OSP, but that is generally not a recommended approach.

Looking at Table 5, we see that the key differences between Operational Environment OSP requirements are whether the P.USER.AUTHORIZATION, P.ADMIN.AUTHORIZATION and P.AUDIT.LOGGING OSPs are included. Taking our hotel business center again, based on the discussion in 3.2.1 this type of business would fit into Operational Environment C. Looking at this type of business from a policy perspective, the HCDs in a hotel business center would be relatively easy and straightforward to use so there would be no real need for formal user policy. On the other hand, there might be a need for an audit logging capability to make sure that only authorized hotel guests or persons who pay to access the Business Center are utilizing the HCDs or that only authorized persons are making configuration changes. It makes sense, then, that for this kind of use the P.USER.AUTHORIZATION OSP would not be needed, which is consistent with the OSPs in Operational Environment C.

Now consider Operational Environment B in a large company (see 3.2.1.2). Here the MFDs are definitely networked for access from offices and would typically be a mix of stand-alone printers and medium to high ppm MFDs because of the large volume and size of documents that typically need to be processed. In that type of environment you want to make sure persons using these HCDs are properly authorized to do so and can access only those services they are authorized to access (for example, only certain employees may be allowed to make color copies); thus the need for a User Authorization policy that is understood and followed by all users. Similarly, in a large office environment where insider threats are always a large concern strong policies about not installing any unauthorized software and making sure all security events (like attempted unauthorized logins) are recorded are also necessary. Finally, because system administrators (SAs) can't be sure who will attempt to connect to the HCDs or what they will attempt to intercept via the network a strong policy governing protection of data sent to or from HCDs is necessary. Thus, the policies that are needed are consistent with Operational Environment B.

5. **The security functions or features meeting the SFRs.**

Table 6 compares the differences of SFRs for the four operational environments.

²⁶ The vendor should ensure that the SFRs for the desired Operational Environment cover (see Table 6) and don't conflict with any new OSPs added.

Table 6. Security Requirements Per Operational Environment^{27,28}

SFR	Operational Environment			
	A	B	C	D
Common SFRs				
FAU_GEN.1	√	√	√	
FAU_GEN.2	√	√	√	
FDP_ACC.1(a)	√	√		
FDP_ACC.1(b)	√	√		
FDP_ACF.1(a)	√	√		
FDP_ACF.1(b)	√	√		
FDP_RIP.1	√	√	√	
FIA_ATD.1	√	√	√	√
FIA_UAU.1	√	√	√	√
FIA_UID.1	√	√	√	√
FIA_USB.1	√	√	√	√
FMT_MSA.1(a)	√	√		
FMT_MSA.1(b)	√	√		
FMT_MSA.3(a)	√	√		
FMT_MSA.3(b)	√	√		
FMT_MTD.1	√	√	√	√
FMT_SMF.1	√	√	√	√
FMT_SMR.1	√	√	√	√
FPT_STM.1	√	√	√	
FPT_TST.1	√	√	√	√
FTA_SSL.3	√	√	√	√
PRT SFR Package				
FDP_ACC.1	√	√		
FDP_ACF.1	√	√		
SCN SFR Package				
FDP_ACC.1	√	√		
FDP_ACF.1	√	√		
CPY SFR Package				
FDP_ACC.1	√	√		
FDP_ACF.1	√	√		
FAX SFR Package				
FDP_ACC.1	√	√		
FDP_ACF.1	√	√		
DSR SFR Package				
FDP_ACC.1	√	√		
FDP_ACF.1	√	√		
NVS SFR Package				
FPT_CIP_EXP.1	√	√		
SMI SFR Package				
FAU_GEN.1	√	√	√	
FPT_FDI_EXP.1	√	√	√	√
FPT_ITC.1	√	√	√	√

²⁷ The definition of each SFR can be found in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

²⁸ For the FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 SFRs, the '(a)' iterations are for data access control and the '(b)' iterations are for function access control.

In the case of SFRs it's a little more difficult to show how particular SFRs apply to a particular Operational Environment. Instead, let's look at a couple of the SFRs to show how they would or would not apply to two different businesses.

Consider the difference between the front office of an auto repair shop versus the hotel business center used above. For the auto repair shop the principle security guideline is likely the PCI DSS because the shop accepts credit cards. The PCI DSS explicitly and implicitly requires that the HCDs used in this shop meet a minimum set of security requirements that, if not followed, can lead to serious fines for the repair shop. Among them are maintenance and support for audit logging of events so it can be indicated who (and when) processed customer personal identifiable information or credit card information (hence the need for the two FAU_GEN SFRs). Access control is also critical to make sure that unauthorized persons do not have the ability to view or modify customer information (hence, the need for the FDP_ACC and FDP_ACF Access Control SFRs and the FIA_UAU and FIA_UID Identification and Authentication SFRs). Since customer information subject to PCI DSS can be printed, scanned, copied and faxed as well as stored in the HCD the Access Control SFRs must also apply to the PRT, SCN, CPY, FAX and DSR SFR Packages in this case.

Contrast this with the hotel business center. User identification and authentication is not required in this case because the hotel really does not care who uses the HCD in the hotel business center. That is why in a hotel business center user identification and authentication is accomplished by use of a common "guest" account that is provided at hotel registration; there is no need for the strict access control requirements needed by the auto shop to comply with PCI DSS. Minimal audit logging is still needed in the case of the hotel business center for purposes of logging security violations associated with unauthorized logins. However, the audit logging requirements for the hotel business center can be less stringent because there is no need to provide individual accountability. Thus in the case of the hotel business center there can be the need for the FIA_UAU and FIA_UID Identification and Authentication SFRs but not for the FDP_ACC and FDP_ACF Access Control SFRs.

5.4 How Vendors Can Fulfill Security Objectives Inside the TOE and Outside the TOE

A TOE can fulfill the security objectives for the desired Operational Environment in multiple ways and still claim conformance to the applicable PP from the IEEE Std 2600 Series of Protection Profiles. The following subclauses provide some examples of how this can be done within the framework of the Common Criteria and the IEEE Std 2600 Series of Protection Profiles.

5.4.1 Storing Audit Data Inside or Outside the TOE

If the TOE representing an HCD does not provide an internal capability to store and provide access to audit records, then by the security objectives for the IT environment OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED any storage and access to audit records is being done by the IT environment. Any implementation would not have to meet or exceed these two security objectives, but the TOE could not claim the additional audit-related SFRs such as FAU_STG.1, FAU_STG.4, FAU_SAR.1 or FAU_SAR either.

If the HCD does provide an internal capability to store and provide access to audit records, security objectives OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED would need to be replaced in the ST by corresponding security objectives for the TOE. As an example, security objectives O.AUDIT_STORAGE.PROTECTED and O.AUDIT_ACCESS.AUTHORIZED could be defined as:

Objective	Definition
O.AUDIT_STORAGE.PROTECTED	The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.

In addition to including these additional security objectives, the HCD would also have to provide the capability to ensure that:

- Stored audit records are protected from unauthorized access, deletion and modification (e.g., FAU_STG.1 and FAU_STG.4)
- Those audit records can be analyzed in order to detect potential security violations, and only by authorized persons (e.g., FAU_SAR.1 and FAU_SAR.2)

In the case where the HCD and its IT environment together perform the functions of audit record storage and access, then separate security objectives and SFRs that apply to the audit record storage and access functions performed by the TOE and by the IT environment, respectively, as discussed in general terms in 6.6 and 6.8.5, would have to be included in the ST. For example, suppose that the HCD provides access to the audit records but the records are actually stored in an external server that is part of the IT environment. In that case:

- Separate security objectives and SFRs would have to be included in the ST for the HCD's role in providing access to the audit log (e.g., FIA_UID.1) and in ensuring that stored audit records are protected by the IT environment from unauthorized access, deletion and modification (e.g., FAU_STG.1 and FAU_STG.4) and
- Separate security objectives (and probably additional assumptions) would have to be included in the ST covering the IT environment's role in protecting audit records from unauthorized access, deletion and modification. These IT environment security objectives would also need to be traced, as applicable, in the ST to the SFRs the TOE must conform to.

Note that in evaluating a TOE in the case where the HCD and its IT environment together perform the functions of audit record storage and access, these two modes of operation would have to be evaluated separately since either approach could be used.

5.4.2 Identification and Authentication Requirements Inside or Outside of the TOE

It is a common scenario for a HCD print function in enterprise environments to have the following configuration:

- Direct print connections (human users submitting print jobs to a HCD print function)
- Connections to one or several print servers (human users submitting print jobs to a print server, then the print server submits the print jobs to HCD print function)

IEEE Std 2600.1 and IEEE Std 2600.2 compliant TOEs require user authentication before print job submission. The CC defines a "user" as a synonym for "external entity", which is then defined as "any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE". With this definition, each of the print servers in this scenario might be considered a "user" for which the TOE must require identification and authentication, the method used for authentication can be different for different kind of "users". The vendor might choose to propose multiple authentication mechanisms for different users as long as all users are required to properly authenticate themselves to the HCD. A compliant product might even offer print server connections to the TOE using different authentication methods: an Internet Protocol Security (IPSec) protected connection, another one using a Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protected connection with client authentication, and a third one using yet another authentication method (e.g. a one-time password).

A topic to be considered by vendors addressing identification and authentication (I&A) concerns in an enterprise environment is where the I&A will be performed:

- External to the TOE by a trusted product in the IT environment (e.g., the HCD forwards the request to a trusted external third party (like Lightweight Directory Access Protocol (LDAP))). Note that this is typically the default case
- Internally by the TOE
- Both internally by the TOE and externally by a trusted IT product in the TOE's IT environment

Similar to the discussion in 5.4.1, if user I&A is being performed outside of the TOE then the ST would have to include the necessary security objectives and SFRs (e.g., FIA_UAU.1 and FIA_UID.1) to ensure that:

- Users are being properly identified and authenticated before being allowed to perform the security functions documented in the ST
- Associated TSF data like user names and passwords are protected from unauthorized disclosure or modification while being transmitted over the network from the TOE to the trusted IT product (see 6.6.8 for additional discussion on this topic)

If user I&A is performed internally by the TOE, then the appropriate security objectives and SFRs for performing the I&A function (e.g., FIA_AFL.1 and FIA_UAU.7) need to be added to the ST.

If user I&A can be performed both internally by the TOE or externally by a trusted product in the IT environment, then separate security objectives have to be included for:

- The TOE's role in performing the actual I&A functions and/or in ensuring the external trusted IT product properly performs the I&A functions
- The TOE's role in protecting the confidentiality and integrity of any TSF data transmitted from the TOE to the trusted IT product
- The trusted IT product's role in performing the I&A function

As in the case for audit data storage, the two modes of performing the I&A function would have to be evaluated separately since either approach could be used.

The author of an ST that specifies a print server as an (IT) user that submits jobs to the TOE on behalf of other (human) users needs to define the method used to authenticate the print server "user". In addition, the ST needs to define the assumptions made about the print server (basically: a "remote trusted IT product" that preserves the integrity and confidentiality of all the user and TSF data (like a PIN code) related to the job). Adding such an assumption does not break the compliance to the PP as long as the assumption is completely related to a function that is additional to the ones mentioned in the PP (which is the case for an assumption that only relates to the print server). IEEE Std 2600.1 and IEEE Std 2600.2 compliant TOEs also require that the user proves job ownership on the Operator Panel of the TOE before he retrieves the hardcopy output. A possible way to achieve this is via a pin code selected by the end-user before sending the job to the print server.

See 6.6.3 and 6.9.2 for more details on how the ST should address the I&A function in these three cases.

6 IEEE STD 2600 SERIES OF PROTECTION PROFILES – ST AUTHOR USAGE GUIDELINES

6.1 Introduction

This clause provides some detailed guidance from the perspective of an ST Author who wants to create an ST for a specific product that conforms to one of the IEEE Std 2600 Series of Protection Profiles that best represents the security requirements and intended Operational Environment for the product to be certified.

The general conventions that applied to Clause 5 apply to this clause also.

6.2 General ST Author Guidance

In general a PP describes the general security requirements for a class of TOEs (in this case, HCDs), whereas an ST describes security requirements for a specific TOE (in this case, a specific HCD product). A PP may therefore be used as a template for many different STs to be used in different HCD evaluations.

An ST compliant to one of the IEEE Std 2600 Series of Protection Profiles is expected to be conformant to Common Criteria Parts 1, 2 and 3 ([B2], [B3] and [B4]), in general.

In Common Criteria Part 1 [B2] the CC requires that an ST provides the following mandatory structured content:

1. ST Introduction that describes the HCD to be evaluated (the TOE) in a narrative way on four levels of abstraction:
 - The ST reference which provides identification material for the ST
 - The TOE reference which provides identification material for the TOE that is referenced by the ST.
 - The TOE overview that briefly describes the TOE including:
 - a). Usage and major security features of the TOE

It is important to note that in the IEEE Std 2600 Series of Protection Profiles it is assumed that the TOE security functionality (TSF) is equivalent to the TOE. The ST author may make a distinction between the TSF and the TOE functions if desired to do so.
 - b). TOE Type
 - c). Required non-TOE hardware/software/firmware
 - The TOE description that describes the TOE in more detail.

A critical part of the TOE description is the TOE boundary. It was the intent of the authors of the IEEE Std 2600 Series of Protection Profiles that the TOE in all cases would be the entire HCD. Whether or not the TOE boundary includes the entire HCD, the ST Author must include within the TOE boundary all the software or hardware components that are required to implement the security-relevant functions and meet the SFRs included in the ST. The TOE boundary should also include the software or hardware to implement all of the applicable features – Print, Copy, Scan and Fax, Document Storage & Retrieval, Removable Nonvolatile Storage and Shared-medium interfaces – that are included in the HCD.

2. Conformance claims that describe how the ST conforms with:

- The Common Criteria itself
- Common Protection Profiles and one or more of the SFR Packages
- Conformance Rationale

To conform to IEEE Std 2600 [B1], an ST must prove demonstrable conformance to the Common Protection Profiles and one or more of the SFR Packages mandated by the PP selected. That is, any TOE that conforms to the Common Protection Profiles and one or more of the SFR Packages mandated by that PP also complies with the applicable ST, and all operational environments that comply with an ST also conform to one of the PP and the packages mandated by that PP. In other words, the ST has the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

3. Security problem definition that includes:

- Threats against the assets in the operational environment of the TOE
- Organizational security policies (OSPs) that are to be enforced by the TOE, its operational environments, or a combination of the two.
- Assumptions on the operational environment that are not to be evaluated.

Note that for TOEs in Operational Environment D that are to conform to IEEE Std 2600.4, the security problem definition is not required in the ST, because IEEE Std 2600.4 conforms to EAL 1 that does not require a security problem definition. The ST Author can include a security problem definition in an ST conforming to IEEE Std 2600.4 if desired.

4. Security objectives that clearly and concisely state the solution to the security problems:

- Security objectives for the TOE
- Security objectives for the operational environment
- Relation between security objectives and the security problem definition that shows:
 - a. Mapping between security objectives and the security problem definition
 - b. Justification for the mapping
 - c. Rationale on how threats are countered

Note that for TOEs in Operational Environment D that are to conform to IEEE Std 2600.4, the following items are not required but can be included at the ST Author's discretion: the security objectives for the TOE and the relation between the security objectives and the security problem definition.

5. Extended Components Definitions that are not based on components in either Common Criteria Part 2 [B3] or Common Criteria Part 3 [B4].

6. Security Requirement

- Security functional requirements (SFRs) that translate security objectives for the TOE into CC SFRs provided in Common Criteria Part 2 [B3]. SFRs must completely address the security objectives. There is no need to translate security objectives for the operational environment, because the operational environment is not evaluated.
- Security assurance requirements (SARs) that describe how the TOE is to be evaluated, including the security requirement rationale for the SARs.
- Security requirements rationale

Note that for TOEs in Operational Environment D that are to conform to IEEE Std 2600.4, as was the case for the security problem definition, the security requirements rationale is not required in the ST

because IEEE Std 2600.4 conforms to EAL 1 that does not require a security requirements rationale. The ST Author can include a security requirements rationale in an ST conforming to IEEE Std 2600.4 if desired, but only when the security problem definition is also included in the ST.

7. TOE summary specification

1. Provide the general technical mechanism that the TOE uses for meeting security objectives, at the level of detail so that potential customers can understand the general form and implementation of the TOE.

6.3 Examples of Demonstrating Conformance to the IEEE Std 2600 Series of Protection Profiles

6.3.1 General Conformance Demonstration

Given the requirement for an ST to show “demonstrable conformance” to one or more of the PPs from the IEEE Std 2600 Series of Protection Profiles, the ST Author has some latitude in defining the security objectives, SFRs and SARs in the ST to meet the security problem defined in the applicable PP. An important caveat, though, is that the ST Author must provide adequate rationale in the ST to demonstrate that the ST is “equivalent to or more restrictive than” the PP from the IEEE Std 2600 Series of Protection Profiles the ST is claiming conformance to. Part of this rationale must involve the ST Author ensuring that the TOE fulfills all of the TOE security objectives documented in the ST and that the TOE always performs the necessary functions to meet the SFRs documented in the ST.

For demonstrable conformance to one of the IEEE Std 2600 Series of Protection Profiles, an ST must demonstrate that it conforms to all of the Common SFRs that are included in Clause 10 of the applicable Protection Profile to which conformance is being claimed. The ST Author should note that, depending on what security functions the TOE itself performs, it may be necessary in the ST to specify a more restrictive SFR or set of SFRs from the corresponding common SFR(s) in the applicable Protection Profile.

Demonstrable conformance in this context also encompasses whether it is necessary to conform to one or more of the SFR Packages in the applicable PP from the IEEE Std 2600 Series of Protection Profiles. The basic rule is that if the TOE performs the function stated in an SFR Package, the ST must demonstrate that it conforms to all the SFRs defined in that applicable SFR package. Another aspect of “demonstrable conformance” is that the ST Author has the option of combining within a single clause the common SFRs with all of the SFRs in the SFR Packages the TOE must conform to as long as the traceability between SFR Package SFRs and security objectives is maintained.

The ST Author should look at CC Part 1 [B2], Annex D, Page 83 for a more thorough explanation of what “demonstrable conformance” means.

Examples to better understand how “demonstrable conformance” can be applied to the case of conformance to one of the PPs from the IEEE Std 2600 Series of Protection Profiles are provided in the following subclauses.

6.3.1.1 Source of Reliable Time Stamps

The TOE security functionality provides reliable time stamps for use in the audit logs and other security functions where it is important to know when the events in question occurred. As stated in the PP Application Notes associated with the FPT_STM.1 SFR (see IEEE Std 2600.1 [B8], Clause 10.8) the TOE could generate these time stamps using the TOE’s internal system clock or the TOE could get time from an external time server using Network Time Protocol (NTP) or some other time protocol. In the first case the ST Author would claim the FPT_STM.1 SFR as part of the TOE Summary Specification in the ST. In the second case the ST Author would have to include in the ST any assumptions and/or security objectives for the IT environment related to generating reliable time stamps by the IT environment and, as the PP Application Notes for the FPT_STM.1 SFR suggest may have to provide one or more additional SFRs for ensuring that the time stamps obtained from the IT environment are properly authenticated and protected

from alteration so that they are reliable. Further discussion of such an added SFR is included in the Additional Guidance for PP APPLICATION NOTES 66 – 68 in 6.9.2, Item 5.a.

6.3.1.2 Conformance to the NVS SFR package

The NVS package covers the threat that removing a nonvolatile storage device designed to be removed by authorized personnel (for instance, a system administrator on a customer's site) would potentially allow an attacker to acquire the device and analyze its content off-line. There are several possible implementation methods for addressing conformance with the NVS SFR package.

The first step is for the ST Author to determine whether an ST can claim conformance to the NVS SFR package:

1. If the product doesn't support this feature (e.g., the product does not have a nonvolatile storage device designed to be removed by authorized personnel) then this package is not required to be included in the HCD evaluation. However, if the product has a nonvolatile storage that is not designed to be removed by authorized personnel the ST Author can still claim conformance to the NVS SFR package if desired.
2. If the product offers this feature (i.e., the product does have a nonvolatile storage device designed to be removed by authorized personnel) but the protection in integrity and confidentiality is supplied by a third party product (like a Full Disk Encryption hard disk) which is not intended to be part of CC certification (e.g., because the HCD vendor can not provide the artifacts required in order to demonstrate conformance to the NVS package) then conformance to the NVS SFR package can not be claimed.

The next step is for the ST Author to determine how conformance with the NVS SFR package can be claimed:

3. If the product offers this feature and the protection in integrity and confidentiality is supplied by the HCD vendor, then conformance to this package can be claimed. The vendor has several ways to fulfill the security requirements mandated by this package:
 - use of an encrypted file system
 - use of hardware solutions to encrypt the nonvolatile storage media
 - use of nonvolatile storage media encryption software
4. If the product offers this feature and the protection in integrity and confidentiality is supplied by a third party product intended to be part of CC certification (e.g., the HCD vendor has an agreement with the third party in order to provide the evidence required for Common Criteria certification) then conformance to this package can be claimed.
5. If the product offers this feature and the integrity and confidentiality protection is supplied by a third party product that has itself already been CC certified, then this package may be claimed by a TOE composed of the vendor's HCD and the certified third party product. It is beyond the scope of this document to describe the requirements and process for TOE composition.
6. If the product offers this feature and the integrity and confidentiality protection is supplied by a third party product that has not been CC certified and if the documents and artifacts required for the CC certification of the TOE with the NVS product cannot be provided by the third party, the conformance to the NVS SFR Package cannot be claimed by any combination of the vendor's HCD and the third party product.

6.3.1.3 Conformance to the SMI SFR package

The trusted path requirements in the SMI SFR package cover the threat of an attacker accessing or modifying sensitive information as it is being transmitted over shared-medium interfaces²⁹ by capturing the data as they are in transit. Depending on HCD implementation, the shared interface can be different: e.g., Ethernet card, Wi-Fi® cards. In order to allow flexibility, these profiles allow vendors to decide, depending on their implementation, what kind of security sensitive management data needs to be protected only in integrity and what information needs both integrity and confidentiality protection.

Beside the freedom to decide on security sensitive management data classification, the vendor can also choose the technique employed in order to provide confidentiality and integrity protection (for instance, the use of TLS or IPSec).

The ST Author should consider the following in determining whether to claim conformance to the SMI SFR Package:

1. If the TOE has a shared-medium interface (i.e., the connection between the TOE and the other trusted IT product is via a shared-medium interface) then the ST must claim conformance to the SMI SFR Package.
2. If the TOE implements as part of the TOE security functionality both a trusted path and the ability to restrict data forwarding, then the ST Author can claim conformance to the SMI SFR package.
3. If the required trusted path is provided by an external trusted IT product (e.g., a third party Network Interface Card (NIC) or some other third party component that internally implements IPSec) instead of the TOE, then the “trusted path” that would provide the full protection of any transmitted data is not being provided fully by the TSF within the TOE.

In this case the ST Author has two choices to claim conformance with the SMI SFR package in the ST:

- a). Include the third party NIC or component as part of the TOE that is being evaluated or
- b). Use a the third party component providing the trusted path that itself has already been Common Criteria certified and then use the new CC Version 3.1 composition assurance packages to claim conformance to the SMI SFR Package³⁰.

Take, for example, the case where the TOE is a printer in a public library (so IEEE Std 2600.3 for Operational Environment C would apply) and a NIC is used to provide a wireless connection from the printer to user laptops. The NIC may provide the basic security functions needed to ensure a trusted path using secure broadband between the user laptops and the printer instead of the printer itself. If this printer is to conform to IEEE Std 2600.3 then the TOE either has to be expanded to include this NIC or the NIC itself has to be a Common Criteria certified product; otherwise conformance to IEEE Std 2600.3 can't be claimed.

6.3.1.4 Common Security Requirements Rationale

Common Criteria Part 3 [B4], Section 11.4, pages 70-71 provides the high-level requirements for what is to be discussed as part of the security requirements rationale. The intent of the security requirements rationale is to demonstrate that the SFRs selected adequately counter the threats stated earlier in the ST as well as enforce all OSPs and uphold all assumptions stated in the ST. In addition, the CEM [B5], Section 10.8.2 provides further guidance on how evaluators will be reviewing the security requirements rationale to make sure it meets the corresponding Common Criteria Part 3 requirements.

²⁹ See Annex A in any of the IEEE Std 2600 Series of Protection Profiles ([B8] – [B11]) for a definition of this term.

³⁰ Note that the same type of argument would apply to the NVM SFR Package discussed in 6.3.1.2 if protection of the confidentiality and integrity of stored data is accomplished partially by the TOE and partially by the IT Environment.

In demonstrating “demonstrable conformance” of the ST to one or more PPs from the IEEE Std 2600 Series of Protection Profiles, the approach the ST Author can use for documenting the security requirements rationale, especially in the case where only Part 2 Conformance and Part 3 Conformance are being claimed, is to include the security requirements rationale verbatim from Clause 10.12 of the PP from the IEEE Std 2600 Series of Protection Profile. However, before doing this the ST Author should first check with the Evaluation Lab performing the certification to make sure that this approach is acceptable to the country Scheme in which the certification is being done; if this approach is not accepted by the applicable country Scheme the ST Author should negotiate an acceptable approach with the country Scheme via the Evaluation Lab and then use the negotiated approach.

6.4 Determining TSF Confidential vs. TSF Protected Data

The IEEE Std 2600 Series of Protection Profiles require that an ST must provide the list of TSF Confidential Data and TSF Protected Data³¹ for SFRs that protect TSF Data³¹ of a specific TOE. TSF Confidential Data and TSF Protected Data are the two types of critical data used by the security functions of the TOE to enforce the security of the TOE correctly and effectively.

The choice of what constitutes TSF Data for a given TOE varies with the TOE so there are no definitive rules as to what the list of TSF Data should be. Some categories of data that the ST Author should consider as TSF Data are:

- User and administrator identification data like usernames
- User, administrator, protocol (e.g., SNMP) and external server authentication data like passwords
- External server authentication settings
- Network configuration settings
- Device security configuration settings such as IP addresses or ports to be opened/closed/blocked
- Device security status information such as the enablement status of security features (such as secure protocols, disk overwriting or disk encryption) or security protocols
- Device security attributes such as power on/power off status or device time settings
- User security attributes such as user access permissions
- Cryptographic key information and key generation algorithms
- Access Control Lists
- Job-related authentication data (e.g., secure print passwords)
- Audit Logs
- Job destination or address lists such as Fax destination phone numbers
- Mailbox information for stored jobs
- Authentication failure data such as successful/unsuccessful login attempts
- Job logs
- User and administrator session information
- Job accounting data (i.e., data on how many pages have been copied, printed, scanned, etc.)
- Device fault status data
- TOE Software (should be treated as TSF protected data)

The data that have to be treated as protected or confidential varies with each TOE, as well as the TOE’s environment. For example, a user’s password clearly has to be treated as protected information so that it cannot be modified by anyone other than the user or an administrator, because the user in question wouldn’t then be able to authenticate himself or herself to access his or her files. However, a user’s password must also be treated as confidential information so that it is not disclosed to anyone, because disclosure would make it possible for potential attackers could authenticate themselves as the user should they know the user’s username and then would have complete access to the user’s files and stored information.

³¹ See IEEE 2600.1 [B8], Annex A Glossary for definitions of these terms.

However, a user's username is different. Clearly, a user wouldn't prefer that someone else knows the user's username because that could give a potential attacker information that might provide insight into guessing the user's password. However, there are situations in which usernames are necessarily public information, such as to identify the owner of a print job or to grant shared access to a stored document. Assuming that some type of two-factor authentication is in place, disclosure of a user's username in and of itself isn't damaging as it is useless for authentication purposes without the user's password. What might be a problem is if there was some way to change a user's username; then the user would not be able to authenticate himself or herself to access his or her files just as was the case for the user's password. From a security perspective, then, a user's username would be considered protected information that could be disclosed but not altered without causing irreparable harm.

The above example is designed to show on a practical level the difference between confidential and protected data. For each TOE the ST author has to determine what the appropriate protected data is, what the appropriate confidential data is, and then which of the data in each of the two categories are to be explicitly specified in the ST.

For ST purposes the ST Author only has to be concerned with TSF Data in general; TSF Confidential and TSF Protected Data in particular. There is no simple formula for doing this, but here is a process to do this task that should be of help:

1. First, determine what your TSF Data assets are. Write down all the different types of TSF Data and information that could be processed by the TOE in its intended operational environment.

This will clearly be different for each environment – if the TOE is designated for a hospital, the types of data mentioned above become applicable; for a merchant the type of data that the Payment Card Industry Data Security Standard (PCI DSS) discusses and references (e.g., credit card account numbers) becomes important. The ST Author should work with persons who know the TOE and its intended use in coming up with this list of TSF Data assets.

2. After you've defined your list of assets you need to ask the following two questions for each TSF Data asset:
 - If this TSF Data asset was disclosed to someone not authorized to view it would that cause any harm?
 - If this TSF Data asset was altered by someone not authorized to view or alter it would that cause any harm?

If the answer to only the first question is "yes" then the TSF Data asset should be treated as TSF Protected Data; if the answer to both questions are yes then the TSF Data should be treated as TSF Confidential Data. If the answer to neither question is "yes" then you should reexamine the asset and determine if the asset really should be considered as TSF Data.

In this context you have to consider "harm" in the broadest sense of a negative impact of some kind to individuals within the company or the company itself. One way to look at it is the "newspaper" test – if news that this asset was disclosed to or altered by an unauthorized person made the newspaper, would that be treated as bad news? If the answer is "yes" then the asset has to be considered protected or confidential data as applicable.

3. Once you've narrowed down your TSF Data assets to those that should be treated as protected and confidential data, then you should look at the specific protected and confidential data and ask this third question:
 - If I didn't explicitly protect this data from unauthorized disclosure or alteration would that be perceived as negatively impacting the security of the TOE?

If the answer is 'Yes' then you should include that data explicitly in the ST. Note that the question is posed in terms of perception because from a practical standpoint that should be how security is viewed – in the "eyes of the beholder" as the phrase goes. You should base what data you explicitly protect on what data are perceived as being critical to the individuals or businesses involved.

4. Finally, note that in the list of potential assets above for the ‘TOE software’ entry it is indicated that the ST Author should consider ‘TOE software’ as being TSF protected data. TOE software must be considered as TSF Data because TOE software clearly meets the definition for TSF Data in Clause 9 of this document - “Data created by and for the TOE that might affect the operation of the TOE”. The rationale for treating the TOE software as TSF protected data rather than as TSF confidential data is that disclosure of TOE software to someone who is neither the Administrator or the owner of the TOE software is often not only allowable, but often is necessary. Otherwise, a service technician or software developer who is authorized to change the TOE software to fix software problems found in the field would not be able to do so. On the other hand, clearly you do not want anyone who isn’t authorized to change the TOE software, such as a potential attacker, making any unauthorized alterations (think viruses and worms, for example) in the TOE software.

6.5 Threats/Objectives Applicable to Each Operational Environment

This clause includes additional explanation of selected SFRs, threats and security objectives.

The threats, security objectives, and SFRs that apply to a TOE in each operational environment depend on the following factors:

1. The type of environment in which the TOE is operating, and hence the assumptions of the operational environment that must be made.
2. The assets of the owner processed by the TOE, the functions and configurations of the TOE that allow the owner’s assets to be processed in the operational environment, and hence the threats to the TOE in the operational environment. The common basic threats are unauthorized disclosure, modification, and denial of service.
3. The security objectives of the TOE, and hence the SFRs that translate the objectives into CC SFRs. Common security objectives are protection for confidentiality, integrity, and availability.
4. The security objectives to be enforced by the operational environment of the TOE, by organizational security policies, or a combination of the two.

Clauses 4.2.3 - 4.2.5 summarize the threats for assets, security objectives, OSPs, assumptions, and SFRs that apply to each environment for the HCD TOE type. For an ST written for a specific TOE, only those threats/assets, security objectives, OSPs, assumptions in the PP for each environment relevant to the functions the specific TOE has or is configured with should apply to the ST.

The ST Author should also be cognizant that when a security objective such as O.CONF.NO_DIS indicates that TSF or User Data is to be protected from unauthorized disclosure or alteration this protection must apply to all data of that type produced by the TOE in performing its functions. This protection cannot be selectively applied to a type of data in one case but not in another.

6.5.1 O.AUDIT.LOGGED Security Objective

The O.AUDIT.LOGGED security objective states that “*The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration*”³². One problem with this security objective is that the PPs do not include any assumptions in Clause 7.4 of each PP about the TOE maintaining or protecting the audit records stored in the audit log. The only related discussion is in PP APPLICATION NOTE 5 (see 6.9.1, Item 5.a) which suggests that the ST Author 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 in the case the TOE provides an internal capability to provide access to audit records; note that only access to audit records is mentioned here and not the case where the TOE provides for the maintenance and protection of the audit records.

³² IEEE 2600.1 [B8], Clause 8.1, page 14.

It should be noted here that the O.AUDIT.LOGGED security objective could be interpreted as requiring that the TOE maintain the audit log and not allow a trusted IT product that is part of the TOE IT environment (e.g., an external log server or a System Administrator's PC) to maintain the audit log. It was the intent of the P2600 Working Group that created the IEEE Std 2600 Series of Protection Profiles that an external log server or other trusted IT product that is part of the TOE IT environment can be used to maintain the audit log. If that is the case, then the Common SFRs defined in Clause 10.1 in each applicable Protection Profile are adequate to meet this security objective and the ST Author does not have to include any additional SFRs from the FAU class. However, if the TOE does maintain the audit log then, just as was suggested in the paragraph above, the ST Author should add any additional security objectives and SFRs from the FAU class necessary to meet the O.AUDIT.LOGGED security objective and to ensure that the TOE maintains the audit log in a way that prevents the unauthorized disclosure and alteration of audit log entries.

If the TOE does provide for the maintenance and protection of audit records, the ST Author should add in the ST to the Security objectives rationale table³³ that the P.AUDIT.LOGGING OSP³⁴ is additionally enforced by the O.USER.AUTHORIZED or O.ADMIN.AUTHORIZED security objectives³⁵ and the OE.USER.AUTHORIZED or OE.ADMIN.AUTHORIZED security objectives.

Finally, the O.AUDIT.LOGGED security objective does require that the audit log document "TOE use". The intent of the authors of the IEEE Std 2600 Series of Protection Profiles is that "TOE use" in the context of this security objective meant, as a minimum, the inclusion of the security-related auditable events as documented in the Audit data requirements table in the applicable PP chosen from the IEEE Std 2600 Series of Protection Profiles; thus inclusion in the ST of the Audit data requirements table from the applicable PP chosen from the IEEE Std 2600 Series of Protection Profiles would suffice to meet the O.AUDIT.LOGGED security objective. For example, job completion is only included as a required auditable event in IEEE Std 2600.1[B8]; for the other three PPs from the IEEE Std 2600 Series of Protection Profiles (IEEE Std 2600.2 [B9], IEEE Std 2600.3 [B10] and IEEE Std 2600.4 [B11]) the ST Author can choose not to collect job completion or even job initiation events, and still meet the O.AUDIT.LOGGED security objective as long as the auditable events listed in the Audit data requirements table for the PP chosen are being collected.

IEEE Std 2600.3 [B10] includes audit logging requirements and the associated O.AUDIT LOGGED security objective. The ST Author should keep in mind that it was the intent of the authors of IEEE Std 2600.3 that the audit logging in IEEE Std 2600.3 should be only for the purposes of logging security violations and not for assigning individual accountability to any actions taken.

6.6 Specifying Security Functional Requirements in STs

The IEEE 2600 Series of Protection Profiles have defined the following sets of SFRs a conforming HCD must meet:

- A set of common SFRs for which all HCDs must implement sufficient security functions to meet the requirements. This set of common SFRs are defined in IEEE Std 2600.1 for Operational Environment A, IEEE Std 2600.2 for Operational Environment B, IEEE Std 2600.3 for Operational Environment C, and IEEE Std 2600.4 for Operational Environment D.

³³ IEEE 2600.1 [B8], Clause 8.4, page 14

³⁴ Applies to IEEE 2600.1 [B8], IEEE 2600.2 [B9] and IEEE 2600.3 [B10] only. See IEEE 2600.1 [B8], Clause 7.3, page 13 for a definition of the P.AUDIT.LOGGING OSP.

³⁵ O.USER.AUTHORIZED and OE.USER.AUTHORIZED apply to IEEE 2600.1 [B8] and IEEE 2600.2 [B9] only; O.ADMIN.AUTHORIZED and OE.ADMIN.AUTHORIZED apply to IEEE 2600.3 [B10] only. See IEEE 2600.1 [B8], Clauses 8.1 & 8.3, pages 14-15 and IEEE 2600.3 [B10], Clauses 8.1 & 8.3, pages 13-14.

- Several sets of SFRs called SFR packages that a HCD must meet for one or more of the following functions it implements or supports: print, scan, copy, fax, data storage and retrieval, nonvolatile storage, shared medium interfaces. The corresponding SFRs for the packages are defined in the named SFR Packages in the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]).

The guidance in ISO/IEC³⁶ TR 15446 Section 6 [B7] provides a good step-by-step approach towards determining the principal and supporting SFRs that should be included in an ST. The following subsections provide additional guidance on specific SFRs that are included in either the set of common SFRs or the SFRs contained in the SFR packages.

In the subclauses that follow the notational conventions specified in IEEE Std 2600.1 [B8], Clause 1.4, Page 2 for documenting SFRs will be used. Specifically:

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.

6.6.1 Security Audit Logging (Class FAU)

The IEEE Std 2600 Series of Protection Profiles specify that all organizations using the TOE must implement the security audit logging policy for which, at a minimum:

- The TOE must meet the security objective O.AUDIT.LOGGED which requires the TOE to have audit functions specified in Common Criteria language as FAU_GEN.1.1 and FAU_GEN.1.2 that requires the TOE to generate audit logs at a choice of level of detail for a specific set of security related events.
- If the audit records are exported from the TOE to another trusted IT product, the TOE environment must meet OE.AUDIT_STORAGE.PROTECTED that protects the stored audit data from unauthorized disclosure, deletion and alteration and OE.AUDIT_ACCESS.AUTHORIZED to ensure that those records can be analyzed in order to detect potential security violations, and only by authorized persons.

For the first bullet above the ST needs to choose one of four possible audit levels of detail (minimum, basic, detailed or not specified)³⁷ in the select statement of FAU_GEN.1.1 and the additional security related events (this can be “none” if there aren’t any) in the assignment statements in the FAU_GEN.1.1 for which the TOE must generate audit data besides those specified in the “Audit Data Requirement” table of IEEE 2600.x³⁸ to be claimed for conformance. The table specifies the minimum set of events for which audit data are required to be generated at the specified level of detail, if the “minimum” level of audit data generation is selected by the ST.

To better understand the Security Audit Logging requirements in the context of the audit levels, let’s look at Table 15 and Table 16 from IEEE Std 2600.1 [B8] in some detail.

³⁶ ISO – International Organization for Standardization; IEC – International Electrotechnical Commission

³⁷ For more details on the definition of the audit levels see the discussion in CC Part 2 [B3], Annex C.3, Page 189.

³⁸Where x=1 for Operational Environment A; x=2 for Operational Environment B; x=3 for Operational Environment C and x=4 for Operational Environment D.

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

“Table 16 —Audit data recommendations”

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

If the ST Author chooses the “not specified” audit level, which is typically what is chosen, that means the ST Author needs to indicate in the ST specification of the FAU_GEN.1 SFR the information included in Tables 15 and 16 for the required and recommended auditable events associated with the TOE. Each required and recommended auditable event is associated with an SFR that is specified in the ST. Each SFR documented in CC Part 2 [B3] includes as part of its requirements any auditable events that must be collected based on the audit level chosen by the ST Author. For example, if you look at the specification of the FDP_ACF.1 SFR in CC Part 2, it includes the following as part of its specification:

<p>Audit: FDP_ACF.1</p> <p>The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:</p> <ul style="list-style-type: none"> a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.

This means that if the Minimal audit level is selected by the ST Author, then the “Successful requests to perform an operation on an object covered by the SFP” must be included in the FAU_GEN.1 SFR description in the ST as a required auditable event. Similarly, if the Basic audit level is selected by the ST Author, then all requests to perform an operation on an object covered by the SFP” must be included in the FAU_GEN.1 SFR description in the ST as a required auditable event and if the Detailed audit level is selected by the ST Author, then “The specific security attributes used in making an access check” must be included in the FAU_GEN.1 SFR description in the ST as a required auditable event.

If “Not Specified” level is chosen by the ST Author, the ST Author is free to specify a relevant and applicable auditable event that will be included in the FAU_GEN.1 SFR specification. In the case of Tables 15 and 16 in IEEE Std 2600.1, since “not specified” was chosen for the audit level associated with the FDP_ACF.1 SFR, the PP Author was free to select an appropriate auditable event to be associated with this SFR; in the case of IEEE Std 2600.1 it was “Job completion” as a required auditable event and “Job initiation” as a recommended auditable event.

The IEEE Std 2600.1 authors chose the indicated audit level for the remaining SFRs listed in Tables 15 and 16; if you examined the relevant clause in CC Part 2 for the FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1, and FPT_STM.1 SFRs the ST Author will see that in each case the auditable event specified in CC Part 2 for the relevant SFR and defined audit level is the auditable event listed in Table 15. In the case of FTA_SSL.3 the ST Author should note that the auditable event listed in Table 15 is not the auditable event defined in CC Part 2 for the FTA_SSL.3 SFR and “Minimum” audit level (as indicated in the Errata statement #1 in Clause 13).

6.6.1.1 Specification of Audit Log Requirements in the ST

To specify the minimum audit generation requirements necessary in the ST, the ST Author should be concerned with the union of (1) the list of any auditable events the ST author specifies in the FAU_GEN.1.1 SFR in the ST and (2) the list of auditable events that are listed in the appropriate “Audit data requirements” table in a PP from the IEEE Std 2600 Series of Protection Profiles that the ST is to conform to. The ST Author has the option to add to the list of auditable events specified in the ST any or all of the “recommended” auditable events listed in the appropriate “Audit data recommendations” table in a PP from the IEEE Std 2600 Series of Protection Profiles that the ST is to conform to. Note, however, that any differences between the auditable events listed in FAU_GEN.1.1 and the list of auditable events in the applicable “Audit data recommendations” table will have to be reconciled by the ST Author in the ST; otherwise the ST might not be found to conform to the applicable PP.

If the ST Author does not choose to list any auditable items in FAU_GEN.1.1 that are specific for the TOE in question (by choosing the “not specified” level of audit option), then the auditable events the TOE will be required to generate and record will only be the list of auditable events that are listed in the appropriate “Audit data requirements” table in the PP from the IEEE Std 2600 Series of Protection Profiles that the ST is to conform to.

In most cases the ST author should use the “not specified” option for the audit event level of audit in FAU_GEN.1.1 because the list of auditable events in the appropriate “Audit data recommendations” table forms the required minimum set of auditable events that must be generated and recorded to conform with the relevant PP, and in most HCDs audit event generation will likely not go beyond this minimum set.

If the TOE is generating and recording audit events that are outside of the list of auditable events specified in the relevant PP’s “Audit data requirements” table these additional auditable events should be listed in FAU_GEN.1.1. The ST Author is cautioned, however, that if any of the other three levels of audit (minimum, basic or detailed) are specified in FAU_GEN.1.1 that means that any relevant audit requirements in CC Part 2 for the specified level of audit in any of the other Security Audit (FAU) family SFRs specified in the ST must be met for the ST to conform to the PP. For example, if the “basic” level of audit is specified in FAU_GEN.1.1, that would mean that if the ST included the FAU_SAR.1 (Audit Review) SFR the TOE would not only have to record the set of auditable events listed in FAU_SAR.1.1 it would also have to generate and record an auditable event corresponding to each time any information is read from the audit record (see Common Criteria Part 2 [B3], page 37).

Another important caution here is that if the ST Author specified a level of audit other than “not specified” in FAU_GEN.1.1 then there could be a conflict between the level of audit specified in FAU_GEN.1.1 and the level of audit associated with one or more of the auditable events listed in the applicable “Audit data requirements” table. In that case the level of audit specified in the “Audit data requirements” table would take precedence over the level of audit specified in FAU_GEN.1.1. For example, assume an ST is written to conform to IEEE Std 2600.1; if in an ST FAU_GEN.1.1 specifies a “minimum” level of audit that would conflict with the “basic” level of audit specified for the successful/unsuccessful use of authentication mechanisms in the “Audit data requirements” table for IEEE Std 2600.1. To be conformant to IEEE Std 2600.1, any “basic” level of audit requirements in FAU SFRs specified in the ST would have to be met for the successful/unsuccessful use of authentication mechanisms auditable event.

Depending on the audit level selected by the ST Author for the SFRs included in the ST’s Security Requirements, there may be conflicts between the auditable events required for these SFRs by the audit level selected and the auditable events required for the same SFRs by the “Audit Data Requirement” table in the applicable IEEE Std 2600.x³⁹ PP. In case of such conflicts the ST Author should specify in the “Audit Data Requirement” table in the ST the auditable events required by the higher audit level⁴⁰.

³⁹ Where x=1 for Operational Environment A; x=2 for Operational Environment B; x=3 for Operational Environment C and x=4 for Operational Environment D.

⁴⁰ For example, a ‘Basic’ audit level is a higher audit level than a ‘Minimum’ audit level. See [B3], Section 7.12.5 for definitions of the various audit levels that can be specified for an SFR.

The ST Author should keep in mind that as a minimum the auditable events specified in the Audit data requirements table from the PP selected from the IEEE Std 2600 Series of Protection Profiles must always be collected. If the ST Author wants to add any additional auditable events beyond the minimums set required, the ST Author should be aware that Common Criteria Part 3 [B4] mandates specific auditable events that must be collected based on the audit level specified in the ST Audit data requirements table. Further, these mandated auditable events supersede anything specified in the ST Audit data requirements table. For example, if the ST Author selects the “Minimum” audit level for any additional auditable event then the TOE must generate whatever is required by Common Criteria Part 3 for the “Minimum” level in all the SFRs included in the ST in addition to the auditable elements required by the PP selected from the IEEE Std 2600 Series of Protection Profile.

If the ST Author does not want to supply any of auditable events mandated by audit the level chosen for any, the ST Author should specify in the FAU_GEN.1 SFR’s Audit data requirements table the “Not Specified” audit level for any additional auditable events listed in the ST.

For the second bullet if the TOE provides an internal capability to store and access audit records, then the ST Author should add appropriate objectives (e.g., O.AUDIT_STORAGE.PROTECTED that requires SFRs (e.g. FAU_STG.1, and FAU_STG.4) to protect audit records stored internally) and (e.g. O.AUDIT_ACCESS.AUTHORIZED that requires SFRs (e.g., FAU_SAR.1, FAU_SAR.2) to ensure the internally stored audit records can be analyzed in order to detect potential security violations, and only by authorized persons.

The ST author should document that any internal TOE capability for storing and providing access to audit records performs an equivalent or more restrictive solution to that which is required by OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACCESS.AUTHORIZED.

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.

The ST should not select the “minimum” level of audit data generation, and list fewer audit events than those specified in the Audit Data Requirement table in the applicable PP from the IEEE Std 2600 Series of Protection Profiles, and still claim conformance to that PP.

6.6.1.2 FTP_CIP_EXP.1 Audit Data Logging

The extended component FPT_CIP_EXP.1 SFR in Clause 9 of any of the IEEE Std 2600 Series of Protection Profiles suggests recording the event “failure condition that prohibits the function to work properly, detected attempts to bypass this functionality” for a Basic level of audit detail, and as such does not recommend any required management functions. In the NVS SFR Package, the PPs didn’t extend any audit requirement to the instantiation of the FPT_CIP_EXP.1.

If the ST Author wants to add any audit log requirements for the NVS SFR Package or if “Basic” is specified in the common SFR section of the ST, the associated auditable event must be specified somewhere in the ST. The ST Author has the option of either (1) including the desired auditable event in the FAU_GEN.1 SFR specification in the Common PP portion of the ST or (2) adding the FAU_GEN.1 SFR with the appropriate “Audit data requirements” or “Audit data requirements” table in the NVS SFR Package in exactly the same way IEEE Std 2600.1 does for the auditable event associated with the SMI SFR Package (see IEEE Std 2600.1 [B8], Clause 19.2).

Note that the recommendation in the PPs is that the “Failure condition” audit event be a recommended not a required auditable event. In the case that the TOE does collect such “failure condition” auditable events the ST Author can make this auditable event required rather than recommended.

6.6.2 User Data Protection (Class FDP)

The IEEE Std 2600 Series of Protection Profiles specify the minimum user data protection objectives for the TOE: O.DOC.NO_DIS, O.DOC.NO_ALT, and O.FUNC.NO_ALT that require the TOE to provide access control functions to the functions or services provided by the TOE, and restrict the access to user

documents and function data enabled by the access to the TOE functions or services. These TOE requirements are specified in Common Criteria language as the following:

- FDP_ACC.1(a) : For common access control rules for accessing user document data and user function data. The IEEE Std 2600 Series of Protection Profiles defines the minimum of these rules in the Common Access Control SFP table that requires that a Normal User is only allowed to “delete” his/her own user document data, and “modify and delete” his/her own function data.
- FDP_ACC.1(b): For common access control rules for TOE functions. There is no minimum defined by the IEEE Std 2600 Series of Protection Profiles. The ST should specify one for the TOE.
- FDP_ACC.1 or FPT_CIP_EXP.1 specified in individual SFR packages for controlling access to user document and function data.

The User Data access control SFP for a conforming Security Target is composed of rules defined in the Common Access Control SFP and all SFPs that have been included by conformance with SFR packages. For example, suppose an ST is being written for a digital copier that only performs copy and fax functions. In that case the ST would have to include as the User Data access control SFP the access control requirements FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attribute based access control) SFRs from the Common Security functional requirements, the FDP_ACC.1 and FDP_ACF.1 SFRs from the IEEE 2600.x-COPY SFR Package and the FDP_ACC.1 and FDP_ACF.1 SFRs from the IEEE 2600.x-FAX SFR Package⁴¹.

However, for the case of an ST is being written for a HCD device that copies, prints, has nonvolatile memory which is not removable as defined in the IEEE Std 2600 Series of Protection Profiles, doesn't have Fax, stores and retrieves documents on the HCD and is not connected to the network then User Data access control SFP would consist of:

1. The access control requirements FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attribute based access control) SFRs from the Common Security functional requirements,
2. The FDP_ACC.1 and FDP_ACF.1 SFRs from the IEEE 2600.x-PRT SFR Package,
3. The FDP_ACC.1 and FDP_ACF.1 SFRs from the IEEE 2600.x-PRT SCN SFR Package and
4. The FDP_ACC.1 and FDP_ACF.1 SFRs from the IEEE 2600.x-DSR SFR Package⁴³.

The ST author may refine the access control rules to further restrict user access to HCD functions or to user data. But such refinements should not violate the access control policy composed of rules defined in the Common Access Control table and all SFPs that have been included by conformance with SFR packages, or the three user data protection objectives for the TOE: O.DOC.NO_DIS, O.DOC.NO_ALT, and O.FUNC.NO_ALT.

The PRT, SCN, CPY, FAX and DSR SFR Packages⁴² add additional access control rules specific to the function discussed in each SFR package. Just as the Common Access Control rule defines the minimum access control requirements for accessing user and TSF Data on any HCD, these function-specific access control rules define the minimum access control requirements for accessing user or TSF Data that is specific for the function in question. In Common Criteria terminology, the specific access control rules are:

1. Print (PRT) -- Requires that access to “read” a user’s document data (where “read” in this context means to release the user document data to a Hardcopy Output Handler for later pickup) is denied to everyone except for a Normal User, and only for his/her own documents. Note that once the printed document is actually output to the Hardcopy Output Handler it is no longer considered as being processed by the TOE but rather is considered as part of the TOE environment; any security objectives, threats, and requirements of the TOE environment would apply to the printed document at this point.

⁴¹ Where x=1 for Operational Environment A and x=2 for Operational Environment B.

⁴² Applies to IEEE 2600.1 [B8] and IEEE 2600.2 [B9] only

2. Scan (SCN) -- Requires that access to “read” his/her own user document data (where “read” in this context means to transmit the user document data through some interface to a destination (assumed to be a trusted IT product⁴³) of the user’s choice) is denied to everyone except for a Normal User, and only for his/her own documents. Note that once the scanned document reaches its final destination it is no longer considered as being processed by the TOE; the security objectives, threats, and requirements of the TOE environment outside the TOE would not apply to the scanned document at this point.
3. Copy (CPY) -- This SFR package does not specify any minimum “read” access control requirements that are unique to a copy job (where “read” has the same contextual meaning here as is the case for the PRT SFR Package). This is because, from a practical perspective, there is the unstated but practical assumption that the user will be present to perform his/her own copy function and thus will either place their own document in the Hardcopy Output Handler or will just pick up the copy output and take it back to their workspace.
4. Fax (FAX) -- Here access control rules have to deal with two different scenarios – sending a Fax to another destination or receiving a Fax from another source location. The rule for an incoming Fax is similar to the access control rule for a print job -- requires that access to “read” incoming Fax documents (where “read” in this context means to release the hardcopy output from the incoming Fax to a Hardcopy Output Handler for later pickup as well as the transmission of the incoming Fax through an interface from the source to the TOE) is denied to everyone except for a Normal User, and only for his/her own incoming Fax documents. For access control purposes it is assumed that the Administrator is the owner of an incoming Fax because no user of the TOE actually initiates an incoming Fax – it is initiated from outside the TOE. Since every job should have an owner it made sense to let the Administrator own any job that doesn’t have a clear TOE user as an owner, which is certainly the case this time.

The rule for outgoing (“send”) Faxes is similar to the access control rule for a scan job -- requires that access to “read” an outgoing Fax documents (where “read” in this context means to transmit the outgoing Fax through some interface to a destination of the user’s choice) is denied to everyone except for a Normal User, and only for his/her own outgoing Fax documents.

Note that just as was the case for a printed document once a received Fax document reaches its final destination it is no longer considered as being processed by the TOE; it is considered to be outside of both the TOE and the TOE environment so that the security objectives, threats, and requirements of the TOE and the TOE environment would not apply to the Fax document at this point. Similarly, an outgoing Fax is like a Scan job in that once it reaches its final destination (another trusted IT product that receives the outgoing Fax) the security objectives, threats, and requirements of this trusted IT product that receives the outgoing Fax would apply once the outgoing Fax was received.

5. Document Storage and Retrieval (DSR) – In this case the access control rules are slightly more complicated. The basic rule is similar to the Scan case, in that access to “read” user document data (where “read” means to transmit the user document data through some interface to a destination (assumed to be a trusted IT product⁴⁴) of the user’s choice just as it did in the Scan case) is denied to everyone except for a Normal User, and only for his/her own documents.

However, since we are talking about documents that are stored and retrieved in some type of memory in the TOE, the access control rule has to be relaxed a little to allow the owner of a document to be able to grant permission to other users to be able to read that owner’s document, while still retaining ownership of that document. To handle this situation the access control rule for DSR also requires that access to “read” a stored document is denied to anyone except another user (where “user” here can be another application; not necessarily just a person) if that user is authorized to do so by the TOE.

The ST Author is always free to define more stringent access control requirements if needed for any of the SFR packages just as is the case for the common access control requirements. See 6.9 and its subclauses for additional guidance on these access control rules.

⁴³ “IT Product” here is either a client or server where the submitted scan is finally stored.

⁴⁴ “IT Product” here is either a client or server where the submitted User Document Data is finally stored.

6.6.3 User Identification and Authentication (Class FIA)

The TOE Operational Model defined in Clause 5.4 of each Protection Profile in the IEEE Std 2600 Series of Protection Profiles describes the essential input, output, storage, and processing elements required to perform one or more of the following document processing operations on User Document Data, as well as summarizing the major security features of the TOE.

In summarizing the major security features of the TOE, the first security feature defined is that “All Users are identified and authenticated, and are authorized before being granted permission to perform TOE functions”. The ST Author should be aware that for some TOEs there might be situations where identification and authentication of a TOE user may not be possible. In these cases, the ST Author should document in the ST the specific authorization(s) required to perform the necessary TSFs.

A good example of this is a received Fax document. Typically, in this situation the actual User who is sending the received Fax cannot be identified or authenticated by the TOE (usually all that is identified is the telephone number from which the received fax document was sent). The TOE must still be able to process that received fax document, but it must do so without performing authorization based on the identification and authentication of the sender of the received Fax document. In this case, the ST Author should define in the ST an exception to the O.USER.AUTHORIZED⁴⁵ security objective in the TOE Function Access Control SFP that permits the TOE to process a received fax document without requiring identification and authentication of the sender.

As an example of how this might be done is to modify SFR FDP_ACF.1.3(b) to read something like:

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 , [<i>the user receives a fax document</i>].
-----------------------	---

6.6.3.1 Documenting Authentication Performed by the HCD in STs

If the validity of user credentials is verified directly by the HCD, then that functionality can be included within the TOE description. This type of verification is typically performed by a local authentication agent that stores credentials within the HCD.

If the credentials are sent to an authentication server outside of the HCD and that server tells the HCD whether they are correct, then no part of the HCD directly verifies the credentials. The authentication in this case is performed externally. That is, it is performed by an entity outside of the TOE.

It is the intent of the IEEE Std 2600 Series of Protection Profiles authors that both internal and external authentication is allowed by the IEEE Std 2600 Series of Protection Profiles. If the HCD allows both modes of operation, then the ST Author should either express both as distinct modes of operation (so both can be evaluated) or specify which is to be used in the evaluated configuration.

If internal authentication functionality is included in the TOE description, then appropriate SFRs should be added for authentication handling. Since we can't rely on an external entity to record or act on failed log-in attempts, for example, some functionality to hinder credential-guessing attempts should be implemented in the TOE.

6.6.3.2 Authentication and Re-authentication of Print Jobs on Compliant Printers

Users will need to authenticate using the Operator Panel in the TOE before the release of pending hardcopy output to a Hardcopy Output Handler. If the User authenticated using the Operator Panel when submitting a print job, and that session is still active, then re-authentication is not necessary. However, if that session is

⁴⁵ Applies to IEEE 2600.1 [B8] and IEEE 2600.2 [B9] only

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 release of pending hardcopy output to a Hardcopy Output Handler operation.

6.6.4 Documenting Time Stamps for Audit Logs Generated Outside the TOE in STs (FPT_STM)

The IEEE Std 2600 Series of Protection Profiles allow the TOE to rely on an internal source, external source, or both for reliable time stamps. An ST Author must document the source of the time stamps in the Security Target. If the source of the time stamps is external to the TOE, the ST Author should consider adding additional SFRs that ensure the reliability of the external source. Things to take into consideration when adding additional SFRs are authentication of the source of the time stamps, protection of the integrity of the time stamp delivery, and the availability of the external source providing the time stamps.

6.6.5 Software Verification Self-Test (FPT_TST)

The main purpose of including the TSF self test (FPT_TST) SFR in the IEEE Std 2600 Series of Protection Profiles is to require that an HCD provide some type of power-on integrity self-tests of the operating software included in an HCD. The types of self-tests that must be provided by an HCD to comply with the requirements of the FPT_TST SFR is:

1. Simple Test for Integrity: Check the signature or hash of some or all parts of executable code.

Other types of self-tests that could be provided by an HCD to comply with the requirements of the FPT_TST SFR are:

2. Test for Subset Residue Removal: Checking whether a randomly created file that has been deleted is not available after deletion on the HCD.
3. Test for Reliable Timestamp: Checking whether time information can be obtained reliably from a local time source.
4. Test of Encryption / Decryption: In case Cryptographic mechanisms are used then checking of encryption / decryption functions.
5. Watchdog Mechanism: Check all the system components to verify that they are running as per requirement.
6. Test for Configuration Integrity: Check the hash or signature of configuration settings.

Clarification of "authorized user":

FPT_TST.1.2 and FPT_TST.1.3 specify that the TSF provides capabilities to an "authorized user". Annex A defines "authorized user" as a user who has been authenticated. However, FPT_TST.1.1 permits TSF testing during initial start-up, at which time it might not be possible for a user to have been authenticated.

The intention of FPT_TST.1.2 and FPT_TST.1.3 is that an "authorized user" may or may not be authenticated, depending on whether the tests are performed during operation or during initial start-up. If tests are performed during initial start-up, the "authorized user" does not need to be authenticated.

This is consistent with the Common Criteria definition of "authorized user" (Part 1, clause 4), in which authentication is not a prerequisite to authorization. Authorization to initiate start-up of the TOE is implicitly controlled by A.ACCESS.MANAGED and its related objective OE.PHYSICAL.MANAGED.

6.6.6 Confidentiality and Integrity of Stored Data (FTP_CIP_EXP)

Some guidelines that the ST Author should consider when instantiating the FTP_CIP_EXP.1 SFR (Confidentiality and Integrity of Stored Data) extended components are as follows:

1. Today many manufacturers are looking at hardware solutions such as fully encrypting disks to meet disk encryption requirements. Some of these drives will not allow data to be written to the drive unless the correct credentials (either the key itself or credentials required to unlock the key stored in a secure area of the drive) are presented. Assuming that this functionality can not be bypassed, detection of modifications is not a useful function within the TOE and therefore it should be possible to instantiate "no action" in the assignment for the "list of actions" in FPT_CIP_EXP.1.2, arguing that unauthorized modification is prevented by the design of the system. This needs to be discussed with the applicable Scheme. In cases where the modification of the encrypted data on the disk is not prevented by the disk itself, to achieve compliance with FTP_CIP_EXP.1 it is necessary for the TOE to ensure that it does not operate with arbitrary data read from the disk. Since the disk is encrypted, simple checksums created by the TOE when it stores data on those disks and verified when the data is read back are sufficient to prohibit that an attacker that does not know the encryption key can alter data in a way that the TOE can not detect.

To summarize: Self-encrypting drives may be used to satisfy FPT_CIP_EXP.1 if the TOE ensures that only such drives are used. If the drive does not provide a function for the prevention of unauthorized modifications or the detection of such modifications, the TOE needs to implement mechanisms that detect unauthorized modifications. Before using self-encrypting drives one should consult the scheme one wants to use for the evaluation to discuss the suggested design.

2. If the ST Author does add this SFR, the ST Author should also add appropriate Application Notes describing how the FPT_STM.1 dependency is resolved in the common SFR section in the ST, that FAU_GEN.1 fulfills O.AUDIT.LOGGED and is a dependency of FAU_GEN.2, and that FAU_GEN.1 performs the audit functions that are recommended (or required if the audit event requirement is put in Table 7) for the FPT_CIP_EXP.1 SFR. See the SMI SFR Package in the IEEE Std 2600 Series of Protection Profiles for examples of what these Application Notes can look like. Finally, the ST Author should make sure the SFR/objective relationships table for the NVS SFR Package is updated to reflect the FAU_GEN.1 SFR added.
3. The instantiation of the FPT_CIP_EXP.1 SFR in the NVS SFR Package, as stated in that SFR package, applies to "User Data and TSF Data that is stored on Removable Nonvolatile Storage devices when such devices are removed from the protection of the environment of the TOE." The ST Author may wonder about what constitutes removal from the "environment of the TOE", especially since Clause 12 in any of the IEEE Std 2600 Series of Protection Profiles states that the NVS SFR package is defined as "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."

The ST Author should keep in mind that the "environment of the TOE" in this context is not the Operational Environment as defined in IEEE Std 2600 [B1] that the PP from the IEEE Std 2600 Series of Protection Profiles the ST will conform to describes. Rather, what this is referring to is the actual physical TOE plus any assumptions about the TOE (e.g., the TOE is being monitored). In that context, the NVS SFR Package only applies to the case where (1) User Data and TSF Data is stored in nonvolatile storage that is designed to be removable from the TOE by an authorized person such as a service technician or an administrator and, most importantly, (2) when that removable nonvolatile storage is actually outside the physical TOE so that it can no longer be protected by the TOE itself and by the assumptions that must be upheld for the PP. In this context the definition of the NVS SFR Package in Clause 12 in any of the IEEE Std 2600 Series of Protection Profiles and the description in the NVS SFR Package itself are not in conflict.

4. The FPT_CIP_EXP.1 SFR in the NVS SFR Package is defined to apply to "a **Removable Nonvolatile Storage device**." That does not preclude this SFR from applying to more than one such "Removable Nonvolatile Storage device". If that is the case, the ST Author should revise the instantiation of the FPT_CIP_EXP.1 SFR in the NVS SFR Package to something like:

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: <i>list of Removable Nonvolatile Storage devices</i>].
------------------------	---

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: *list of Removable Nonvolatile Storage devices*].

6.6.7 Restricting Forwarding of Data to External Interfaces (FPT_FDI_EXP)

The FPT_FDI_EXP.1 SFR (Restricted forwarding of data to external interfaces) as defined in Clause 9 in any of the IEEE Std 2600 Series of Protection Profiles states:

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

One question that is raised in the definition of the FPT_FDI_EXP.1 SFR is how to interpret the phrase “without further processing by the TSF”. The intention of the requirement here is to ensure that the restriction on the data being forwarded between the respective listed external interfaces is (1) a normal function of the TOE (and not a function performed by the TOE IT environment, for example) and (2) does not violate any of the OSPs and SFPs listed for the TOE in the ST. The ST Author should make sure in specifying this SFR in the ST that both conditions are true; otherwise the ST Author will not be able to claim conformance with this SFR.

NOTE: The restriction mentioned in the SFR can be performed as an optional or settable feature of the TOE. However, this restriction of data being forwarded can also be claimed if the restriction is performed based on how the TOE is architected (and not an actual feature of the TOE). In the latter case the ST Author has to include in the ST the appropriate rationale as to how the TOE architecturally conforms to this SFR.

6.6.8 Protection of User Credentials Leaving/Entering an SMI Interface When Scanning to a Remote Destination on IEEE Stds 2600.1 and 2600.2 Compliant Products

IEEE Std 2600.1 [B8] and IEEE Std 2600.2 [B9] require a trusted channel for communication of TSF Data over a Shared-medium Interface. The key requirements that must be met are that the end points of the channel are identified and that the integrity and confidentiality of TSF Data are protected. User credentials for accessing external devices are considered to be TSF Data (see 6.4), so a trusted path is required when transferring user credentials over a Shared-medium interface.

This “trusted path” requirement can be implemented in a variety of mechanisms, not just the more popular use of SSL/TLS or IPsec. For example, signed and encrypted e-mail sent over a network can count as a “trusted channel” since it ensures the endpoints are identified and protects the confidentiality and integrity of the data transmitted. Even a simple protocol that adds checksums to the data and then encrypts both the data and the checksums using a symmetric encryption algorithm could be considered a “trusted channel” in this context as long as each of the TOE’s different communications partners uses a different encryption key. The TOE would have to, in this case, implement some mechanism (which could even be a manual method) for secretly sharing the encryption key with each communication partner.

Kerberos establishes trusted end points and trusted path for any data as long as the data that require confidentiality and integrity protection are properly protected. Therefore, Kerberos can be an option if a trusted channel is required for communication of authentication data. For example, the HCD may offer a Kerberized print service, for which the user has to obtain a Kerberos service ticket before submitting a print job. In the case of a scan to remote destination, the HCD shall obtain a Kerberos service ticket in order to access a Kerberized remote destination.

If the ST Author plans to use Kerberos, there is a dependency on the Kerberos infrastructure that in principle is no different than the dependency on the Public Key Infrastructure when SSL/TLS with client authentication is used. The ST Author would have to state in the ST the appropriate assumptions covering how the IT environment sets up the channel to the Kerberos authentication server.

6.6.9 Iterating the FMT_MTD.1 SFR

In the Errata discussion for the FMT_MTD.1 SFR in 13.1, it was suggested that if the ST Author desired the FMT_MTD.1 SFR could be iterated instead of the current iteration of the FMT_MTD.1.1 component, since the former format is the more correct form per the CC Part 2 [B3].

If the ST Author does want to iterate the FMT_MTD.1 SFR, the iteration would look something like the following:

FMT_MTD.1(a)	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1(a)	The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i>] the [assignment: <i>list of TSF data</i>] to [selection, choose one of: <i>Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]</i>]].
FMT_MTD.1(b)	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1(b)	The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear, [assignment: other operations]</i>] the [assignment: <i>list of TSF data associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL</i>] to [selection, choose one of: <i>Nobody, [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF data is associated]</i>]].

6.7 Common Access Control SFP

The Common Access Control SFP as defined in Clause 10.4 in any of the IEEE Std 2600 Series of Protection Profiles restricts operations on D.DOC and D.FUNC from being performed by anyone except the owner of that data. However, later in Clause 10 in any of the IEEE Std 2600 Series of Protection Profiles the FMT_MSA.3(a) SFR (Static attribute initialisation) is defined as follows:

FMT_MSA.3.1(a)	The TSF shall enforce the Common Access Control SFP in Table 7 , [assignment: <i>access control SFP, information flow control SFP</i>] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i>] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2(a)	The TSF shall allow the [assignment: <i>the authorized identified roles</i>] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.2(a) allows an authorized role to alter the default attribute values when an object or information is created. Typically, either U.ADMINISTRATOR or Nobody will be allowed to alter default attribute values. It is possible in some implementations that a U.NORMAL will be allowed to alter default attribute values associated with some of their own data, and such allowance should be specified carefully so that access control is not compromised.

It is allowable to add additional rules related to access control in the access control SFRs such as FDP_ACF.1.3(a) and FDP_ACF.1.3(b). For example, the ST Author could define a rule that allows the owner to delegate the authority he has on his own objects to another user. PP APPLICATION NOTE 30 implies that this can be done without explicitly stating that the ST author should define additional rules in these SFRs. The Common Access Control SFP in Table 17 (or its equivalent) in the IEEE Std 2600 Series of Protection Profiles just defines the set of "default rules", but does allow the statement of well-defined additional rules as long as these additional rules do not contradict the security objectives. This allows for an additional rule where a user could explicitly authorize another user to delete one or all of the user's documents, but not for a rule where a normal user is allowed to delete a document belonging to another user without being explicitly authorized to do so by either the document's owner or an authorized administrator.

An operation (like the "Delete" operation for objects of type D.DOC) that is subject to the access control policy is considered a "controlled operation". The ST Author is allowed in the ST to define other operations on D.DOC objects where access control rules like the one from the example in the paragraph above would apply. The ST Author would have to define the necessary instances of the FDP_ACF.1.*. SFRs in the ST to cover these other operations. However, any new access control rules governing these other operations included in the ST would have to conform to the security objectives stated in the applicable PP from the IEEE Std 2600 Series of Protection Profiles.

Below are some examples of how some additional access control rules can be specified in an ST:

1. If an HCD has a document storage/retrieval feature that allows a user to modify a document that they have previously stored in the TOE, then the ST Author could add the following rule to the DSR Access Control SFP in Table 36:

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
D.DOC	+DSR	Modify	U.NORMAL	Denied, except for his/her own documents.

2. If an HCD has a document storage/retrieval feature that allows a user to grant Read access to D.DOC for some users, the ST Author would need to define a new security attribute, and could do so as follows:

Designation	Parameters	Definition
+READ	Subject(s)	Indicates that the owner of an Object with this attribute has granted permission to Subject(s) to perform Read operations on that Object.

Then, the ST Author could choose to use that attribute to add an additional rule. That rule could be explicitly stated in FDP_ACF.1.3 as part of the DSR SFR package:

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: A Subject can perform the Read operation on D.DOC, provided that D.DOC has the attribute +READ (Subject) for that Subject.
--------------------	---

3. If an HCD has a document storage/retrieval feature that allows a user to grant more complex access to D.DOC for some users, the ST Author would need to define security attributes, and could do so as follows:

Designation	Parameters	Definition
+GRANTED	Subject(s), Operation(s)	Indicates that the owner of an Object with this attribute has granted permission to Subject(s) to perform Operation(s) on that Object.

Then, the ST Author could choose to use that attribute to add an additional rule. That rule could be explicitly stated in FDP_ACF.1.3 as part of the DSR SFR package:

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: A Subject can perform an Operation on D.DOC, provided that D.DOC has the attribute +GRANTED (Subject, Operation) for that Subject and Operation.
--------------------	---

The ST Author would also need to consider defining rules for how any new attributes are managed, using FMT_MSA.1 for changing attribute values and FMT_MSA.3 for changing the initial attribute values. Here are some examples, based on the DSR example above:

To allow a user to grant Read access to some users, the ST Author could use

FMT_MSA.1.1:	
FMT_MSA.1.1	The TSF shall enforce the DSR Access Control SFP in Table 36 to restrict the ability to modify the security attributes +READ associated with a D.DOC to the owner of that D.DOC.

To allow a user to grant Read access to some users by default for all of that user’s documents, the ST Author could refine FMT_MSA.3.2:

FMT_MSA.3.2	The TSF shall allow the owner of a D.DOC to specify alternative initial values to override the default values for the +READ attribute when an object or information is created.
--------------------	---

6.7.1 Allowing One User to See or Modify Another User’s Documents

As long as it is a *controlled operation* to give a user a read/modify capability, then it is acceptable. By default, the Common Access Control SFP in both IEEE Std 2600.1 [B8] and IEEE Std 2600.2 [B9]⁴⁶ mentions that user access to documents is denied, except for his/her own documents. ST authors can add rules concerning special users as long these rules are not conflicting with the objectives stated in these PPs (for instance, it is not allowed to say that any authenticated user is allowed to read/modify another user’s documents).

If a vendor builds a product for which it is desired that special users (for instance Administrators) be able to read/modify others’ documents, then that should be stated in the ST and is acceptable.

6.8 Important Things to Do and To Avoid

This clause provides detailed guidance for ST authors about some important “Things To Do” and “Things to Avoid” for each section of ST. Most importantly, special attention should be paid to the sections and

⁴⁶ See, for example, IEEE 2600.1 [B8], Clause 10.4, page 24.

each subsection of Conformance Claims, Security Problems, Security objectives, Extended Component Definitions (if any), and each SFR in the security requirements.

To conform to one of the IEEE Std 2600 Series of Protection Profiles, an ST must show demonstrable conformance to one of the IEEE Std 2600 Series of Protection Profiles and those packages mandated by the PP chosen. In other words, a TOE that conforms with a PP from the IEEE Std 2600 Series of Protection Profiles and the packages mandated by the PP chosen also meets the ST for that TOE, and the operational environment that meets the ST for a TOE also meets the applicable PP from the IEEE Std 2600 Series of Protection Profiles and packages mandated by the PP chosen. In other words, the ST has the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

The discussion that follows will be based on the required content of an ST as indicated in Common Criteria Part 3 [B4], Chapter 11. It is not intended to duplicate ST format and content information that a user can find in the normative references in Common Criteria Parts 1, 2 and 3 and the CEM ([B2] – [B5]) and ISO/IEC TR 15446 [B7]; rather the intent is to supplement the information found in those documents. The ST author is free to format the ST as deemed fit or as advised by any consultants being used to help in ST preparation; if the ST author is not sure of what format to use for the ST the best approach is to follow the ST format that is implied by the Class ASE: ST evaluation requirements in Common Criteria Part 3 [B4].

6.8.1 General ST Content

In general, an ST should not be:

1. A detailed specification: An ST is designed to be a security specification on a relatively high level of abstraction. An ST should, in general, not contain detailed protocol specifications, detailed descriptions of algorithms and/or mechanisms, long description of detailed operations etc.
2. A complete specification: An ST is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size and weight, required voltage etc. should not be part of an ST. This means that in general an ST may be a part of a complete specification, but is not a complete specification in itself.

6.8.2 ST Introduction – TOE Overview

The ST should provide a narrative, top-level description of all modules and TOE architecture, functions performed by the modules in providing services to the end users, and handling TOE assets and associated security functions that protect the TOE assets.

The ST author should identify the TOE logical and physical boundary and non-TOE hardware, software and firmware required by the TOE.

6.8.3 ST Conformance Claims

1. CC Conformance:

The ST should state (1) that it is Common Criteria version 3.1 Release 1 Part 1 and Part 3 conformant, and Part 2 conformant if the ST does not claim conformance to either the NVS SFR Package (for IEEE 2600.1 and IEEE Std 2600.2 only) or the SMI SFR Package (for any of the IEEE Std 2600 Series of Protection Profiles) or (2) that it is Common Criteria version 3.1 Release 1 Part 1 and Part 3 conformant, and Part 2 extended if the ST claims conformance to either the NVS SFR Package or the SMI SFR package.

2. SAR Packages and EAL Conformance:

The ST should state that as a minimum conformance requirement it conforms to Common Criteria Evaluation Assurance Level (EAL) required by the PP selected from the IEEE Std 2600 Series of Protection Profiles for the particular Operational Environment claimed by the ST as shown in the following table:

Table 7. EAL Conformance

Operational Environment	EAL Conformance
A	EAL 3 augmented by ALC_FLR.2
B	EAL 2 augmented by ALC_FLR.2
C	EAL 2 augmented by ALC_FLR.1
D	EAL 1

3. PP Conformance:

The ST should state that it conforms to the Common PP for the particular Operational Environment (i.e., IEEE Std 2600.1 for Operational Environment A, IEEE Std 2600.2 for Operational Environment B, IEEE Std 2600.3 for Operational Environment C, or IEEE Std 2600.4 for Operational Environment D) and all the SFR packages applicable to the functions implemented by the TOE as shown in the following tables:

Table 8. Operational Environment A SFR Package Conformance

Functions Implemented by the TOE	SFR Conformance Package
PRT (printing)	IEEE Std 2600.1-PRT: SFR Package for Hardcopy Device Print Functions, Operational Environment A
SCN (scanning)	IEEE Std 2600.1-SCN: SFR Package for Hardcopy Device Scan Functions, Operational Environment A
CPY (copying)	IEEE Std 2600.1-CPY: SFR Package for Hardcopy Device Copy Functions, Operational Environment A
FAX (faxing)	IEEE Std 2600.1-FAX: SFR Package for Hardcopy Device Fax Functions, Operational Environment A
DSR (document storage and retrieval)	IEEE Std 2600.1-DSR: SFR Package for Hardcopy Device Data Store and Retrieval Functions, Operational Environment A
NVS (removable nonvolatile storage)	IEEE Std 2600.1-NVS : SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A
SMI (shared-medium interface)	IEEE Std 2600.1-SMI : SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

Table 9. Operational Environment B SFR Package Conformance:

Functions Implemented by the TOE	SFR Conformance Package
PRT (printing)	IEEE Std 2600.2-PRT: SFR Package for Hardcopy Device Print Functions, Operational Environment B
SCN (scanning)	IEEE Std 2600.2-SCN: SFR Package for Hardcopy Device Scan Functions, Operational Environment B
CPY (copying)	IEEE Std 2600.2-CPY: SFR Package for Hardcopy Device Copy Functions, Operational Environment B
FAX (faxing)	IEEE Std 2600.2-FAX: SFR Package for Hardcopy Device Fax Functions, Operational Environment B.
DSR (document storage and retrieval)	IEEE Std 2600.2-DSR: SFR Package for Hardcopy Device Data Storage and Retrieval Functions, Operational Environment B.
NVS (removable nonvolatile storage)	IEEE Std 2600.2-NVS: SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B.
SMI (shared-medium interface)	IEEE Std 2600.2-SMI: SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B.

Table 10. Operational Environment C SFR Package Conformance:

Functions Implemented by the TOE	SFR Conformance Package
SMI (shared-medium interface)	IEEE Std 2600.3-SMI: SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment C.

Table 11. Operational Environment D SFR Package Conformance:

Functions Implemented by the TOE	SFR Conformance Package
SMI (shared-medium interface)	IEEE Std 2600.4-SMI: SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment D.

Notice that in Operational Environment C or D, even if the TOE has implemented or supported one or more of the functions that follows -PRT, CPY, SCN, FAX, DSR, NVS - the ST does not need to claim conformance to any additional SFR package.

4. Conformance Rationale:

The ST should demonstrate the ST is equivalent or more restrictive than the PP to which it is claiming demonstrable conformance. This is explained in more detail in the following clauses:

- Security Problem Definition: see 6.8.4.
- Security Objectives: see 6.8.5.
- Extended Components: see 6.8.6.
- SFRs: see 6.6.
- SARs: see 6.10.

Things To Avoid:

The ST should not claim conformance to any SFR package for a function not implemented or supported by the TOE.

6.8.4 ST Security Problem Definition

The ST should define the security problem to be addressed by both the TOE and its operational environment. The security problem definition has to include the threats, OSPs and assumptions about the TOE's operational environment.

In the case of an ST written against IEEE Std 2600.4, the security problem definition is not needed for conformance to IEEE Std 2600.4. If the ST Author wants to make a Low Assurance ST (i.e., an ST with reduced content) as described in CC Part 1 [B2], Section A.12, the ST Author should not include a security problem definition. Otherwise, if the ST Author wants to create a regular ST the ST Author should include a security problem definition.

Some specific guidance on what should be included in the security problem definition is:

1. Threat Agents :

The threat agents in the ST's environment **should be either exactly the same** as those defined in the PP from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, **or stronger**; they **should not be weaker** than those defined in the PP selected from the IEEE Std 2600 series of Protection Profiles the ST claims conformance to.

2. Assumptions :

The assumptions made in the ST's environment **should be either exactly the same** as those made by the PP from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, **or less**; they **should not be more** than those made by the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to.

3. Organizational Security Policies (OSPs):

The OSPs that are to be enforced by the TOE, its operational environments, or a combination of the two **should be either exactly the same** as those defined by the PP from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, **or more restrictive**. However, these OSPs **should not be less restrictive** than those defined by the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to.

4. Threats:

Threats defined by the ST are either to be countered by the TOE or the operational environment.

In the ST the threats defined for the TOE **should be either exactly the same** as those defined by the PP from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, **or more** because either (1) less assumptions are made in the ST's environment or (2) less restrictive OSPs are to be enforced by the operational environment. **The threats defined for the TOE, however, should not be less than** those defined by the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to.

6.8.5 ST Security Objectives

The ST should define the security objectives consisting of a concise statement of how the TOE and its operational environment will respond to the security problem as defined in the ST. Some specific guidance on what should be included in the security objectives given below:

1. Security Objectives for the TOE

The security objectives for the TOE should counter all threats defined for the TOE. If the ST has defined more threats for the TOE than those defined in the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, because there are less OSPs to be enforced in the TOE environment, then there should be more security objectives defined for the TOE to address the additional threats. Therefore the security objectives for the TOE in the ST should be **either be equivalent, or more restrictive than** those defined by the Protection Profile selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to, and each SFR package the ST claims to conform for the applicable operational environment.

Each security objective for the TOE should map to at least one threat or OSP.

Things To Avoid:

- The security objectives for the TOE should never be less strict than the security objectives defined in the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to.
- There should not be any objective for the TOE that does not map to any threat, or OSP.

2. Security Objectives for the IT environment

The security objectives for the IT operational environment of the TOE described in ST should be **either the same as or less strict than** those defined in the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST claims conformance to. The important point to keep in mind here is that when you make the security objectives for the IT Environment less strict than those defined in the applicable PP that means the security objectives for the TOE must be **greater than** those defined in the PP to cover the security objectives no longer being performed by the IT environment.

Each security objective for the environment should trace to at least one threat, OSP, or assumption.

Things To Avoid:

- The security objectives for the operational environment should never have more, or stricter objectives than those defined in the applicable PP selected from the IEEE 2600 Std Series of Protection Profiles for the ST to claim “demonstrable conformance” to that PP.

- There should not be any objective for the environment that does not map to any threat, OSP, or assumption.

3. Security Objectives for the Non-IT Environment

Security objectives for the Non-IT environment typically apply to issues like policies and procedures to ensure the secure installation and operation of the TOE or education and training of users and/or administrators to ensure secure installation and operation of the TOE.

The same guidance specified above for the security objectives for the IT environment of the TOE applies to the security objectives for the non-IT operational environment of the TOE.

6.8.6 Extended Components Definitions

The common Protection Profile that is part of the IEEE Std 2600 Series of Protection Profiles for a given operational environment does not define or use any extended SFR component. However, there are two extended components defined in two SFR packages in the IEEE Std 2600 Series of Protection Profiles:

1. FPT_CIP_EXP (Confidentiality and Integrity of Stored Data) in NVS SFR package that is defined as a SFR family extended from the FPT components that protects both confidentiality and integrity of stored TSF and user data on any removable nonvolatile storage.
2. FPT_FDI_EXP (Restricted Forwarding of Data to External Interfaces) in SMI SFR package that is defined as a SFR family extended from the FPT components that provides restricted direct forwarding of information from one external interface to another external interface.

Note that the statement of the FPT_FDI_EXP extended component in the IEEE Std 2600 Series of Protection Profiles refers to data from one external interface being restricted from further “processing” by the TSF to another external interface. The concept of “processing” in this context means that the TOE performs some type of function on data that is input to the TOE via one external interface before that same data is exported from the TOE via an external interface. An example of such a function that would be prohibited (and the situation that initially prompted this extended component) is that the TSFs are able to take data input to the HCD via a public telephone line and, using the internal interfaces in the HCD, output that same data via the network interface to that HCD.

The requirement in the FPT_FDI_EXP extended component is not intended to apply to any normal processing of data input from one external interface that might cause outputs to another external interface. For example, the FPT_FDI_EXP extended component does not preclude the case where a Fax might be over a public telephone line, processed by the HCD to convert it to an electronic form and then sent via a scan function to another user or stored in a directory in an external server. What the FPT_FDI_EXP extended component is intended to prohibit is the situation where data input from one external interface is directly transferred to another external interface without any of the “normal” processing occurring first. For the example in this paragraph, that would mean that the TSF must restrict Faxes input from a telephone line from being sent directly out over the network interface without any type of processing by the HCD.

The ST should use exactly *the same* extended components definitions defined in the two packages the ST claims to conform, *or* modify to a *stricter* definition due to weaker OSP(s) to be enforced or less assumptions in the operational environment.

Things To Avoid:

- If the ST claims conformance to the package(s) requiring the extended components, the ST should not modify the extended component definitions to be less restrictive than that defined in the PP selected from the IEEE Std 2600 Series of Protection Profiles the ST conforms to.

6.8.7 TOE summary specification

The *TOE Summary Specification* is the section in an ST that defines the IT security functions provided by the TOE to meet the specified security functional requirements, and finally any assurance measures claimed to satisfy the specified security assurance requirements. The *TOE Summary Specification* typically covers

the IT security functions, security mechanisms or techniques referenced by the ST (such as encryption) and assurance measures to be applied for the TOE in question.

Things To Do:

- The *TOE Summary Specification* should be written primarily for evaluators and consumers of the TOE to understand the IT security functions that are being claimed to meet the *ST Security Objectives*. The *TOE Summary Specification* should be self-contained; if not it should explicitly indicate that it depends on *ST Security Objectives* or indicate which other PP sections and which other documents (e.g. referenced encryption standards) are necessary for a full and accurate understanding of the SFRs included in the *ST Security Objective*.
- Provide only a high-level description of the IT security functions in the *TOE Summary Specification*. The goal should be to define at a high level what the TOE provides to satisfy the SFRs in the *ST Security Objectives* and thereby meet the TOE's security objectives.
- Whenever possible write the *TOE Summary Specification* making appropriate use of TOE-specific terminology. This will help in relating the IT security functions to TOE documentation and facilitate a better understanding of the IT security functions by evaluators and consumers.
- Ensure that every SFR is mapped to at least one IT security function in the *TOE Summary Specification*, and that each IT security function in the *TOE Summary Specification* is mapped to at least one SFR.

Things To Avoid:

- Supply a detailed specification for each IT security function in the *TOE Summary Specification*.

6.9 Guidance on PP Application Notes

Each of the four Protection Profiles that this Guide covers contains a set of PP Application Notes. These Application Notes are included in the appropriate spots to provide guidance to the ST Author on how to understand, and in some cases interpret, the applicable text. Although each PP Application Note is written to be self-contained, some but not all of the PP Application Notes require further explanations.

Each PP Application Note discussed below is paraphrased from the specific text of the PP Application Note included in the applicable PP. When appropriate the SFR associated with each PP Application Note is provided. IEEE Std 2600.1 ([B8]), IEEE Std 2600.2 [B9], IEEE Std 2600.3 [B10] and IEEE Std 2600.4 [B11] generally have a subset of the PP Application Notes included in IEEE Std 2600.1, although there are some unique PP Application Notes that are addressed in this clause.

The following are some points to help the reader understand the differences in the PP Application Notes described in 6.9.1 - 6.9.10 among IEEE Std 2600.1, IEEE Std 2600.2, IEEE Std 2600.3 and IEEE Std 2600.4:

1. Unless otherwise specifically stated any PP Application Note number, clause or SFR references included in this clause refer to the applicable clause or SFR in IEEE Std 2600.1 and not to a clause in this document.
2. The PP Application Notes described below, unless otherwise explicitly stated, are taken from the set of PP Application Notes included in IEEE Std 2600.1 and use the PP Application Note number from IEEE Std 2600.1.
3. The actual wording of each PP Application Note may be slightly different among the four PPs, but that will not be indicated in 6.9.1 - 6.9.10.
4. Any unique PP Application Note will indicate the PP or PPs that PP Application Note applies to and will use the PP Application Note number as it appears in the applicable PP. As a result, there may be a few instances in 6.9.1 - 6.9.10 where there are two or more PP Application Notes with the same PP Application Note number.

5. Starting with PP APPLICATION NOTE 13 for FAU_GEN.1 in 6.9.2 the number of the corresponding PP Application Note in IEEE Std 2600.2 will be two more than the number shown in this document (and thus in IEEE Std 2600.1). For example, PP APPLICATION NOTE 13 in 6.9.2 is PP APPLICATION NOTE 15 in IEEE Std 2600.2.
6. The following PP Application Notes in IEEE Std 2600.1 are not included in IEEE Std 2600.3 because the corresponding SFRs or SFR Packages are not included in IEEE Std 2600.3 – PP APPLICATION NOTES 15 – 31, 45 – 69 and 73 - 109. The remaining PP Application Notes in IEEE Std 2600.3 are renumbered accordingly, but this renumbering will not be indicated in 6.9.1 - 6.9.10.
7. The following PP Application Notes in IEEE Std 2600.1 are not included in IEEE Std 2600.4 because the corresponding SFRs or SFR Packages are not included in IEEE Std 2600.4 – PP APPLICATION NOTES 5 – 32, 46 – 58, 66 – 69, 73 - 112. The remaining PP Application Notes in IEEE Std 2600.4 are renumbered accordingly, but this renumbering will not be indicated in 6.9.1 - 6.9.10.

6.9.1 General PP Application Notes

1. PP Introduction (PP Clause 3)
 - a). **PP APPLICATION NOTE 1** — Addresses how the ST Author determines whether the ST claims “Part 2 conformant” or “Part 2 extended”.
Additional Guidance: No additional guidance is deemed necessary.
2. TOE Overview (PP Clause 5)
 - a). **PP APPLICATION NOTE 2** — Addresses the cases when User Data and TSF Data are either generated outside of the TOE and transmitted to the TOE or are generated and/or processed by the TOE and exported from the TOE.
Additional Guidance: The ST Author needs to make sure that any discussion in the ST of security measures for protecting User and TSF Data takes into account any User or TSF Data that is either transmitted to the TOE from a source in the TOE environment or transmitted from the TOE to a destination in the TOE environment.

The ST Author should determine whether the protection of such data is performed by the TOE itself, by the TOE environment, or by both. The ST Author should then ensure that the assumptions, OSPs, threats, security objectives and SFRs associated with all protections of User and TSF Data provided by the TOE, regardless of the data’s source or destination, are covered in the ST.
 - b). **PP APPLICATION NOTE 2 (IEEE Std 2600.4 Only)** — Indicates IEEE Std 2600.4 was written in a way so that it can be elevated to an EAL above Low Assurance Level.
Additional Guidance: If the TOE is conforming to IEEE Std 2600.4 at the EAL1 Low Assurance Level, the ST Author does not have to include the Security Problem Definition (see 6.8.4) in the ST.
 - c). **PP APPLICATION NOTE 3** — Advises the ST Author when defining the TSF Data assets for the TOE.
Additional Guidance: See the discussion in 6.4 on how to determine what the TSF Data is for a given TOE and how to determine whether that TOE data is protected or confidential data.
 - d). **PP APPLICATION NOTE 3 (IEEE Std 2600.3 Only)** — Indicates that IEEE Std 2600.3 does not provide any access controls for User Data.
Additional Guidance: No additional guidance is deemed necessary.

3. Conformance Claims (PP Clause 6)

- a). **PP APPLICATION NOTE 4** — Suggests how the ST Author should reference one of the Protection Profiles and associated SFR Packages that is part of the IEEE Std 2600 Series of Protection Profiles.

Additional Guidance: See 6.3 for additional guidance on claiming conformance to a PP in an ST.

- b). **PP APPLICATION NOTE 6 (IEEE Std 2600.4 Only)** — Indicates IEEE Std 2600.4 was written in a way so that it can be elevated to an EAL above Low Assurance Level.

Additional Guidance: As was the case for PP APPLICATION NOTE 2, if the TOE is conforming to IEEE Std 2600.4 at the EAL1 Low Assurance Level the ST Author does not have to include the Security Problem Definition in the ST.

4. Security Problem Definition (PP Clause 7)

PP APPLICATION NOTE 6 (IEEE Std 2600.3 Only) — Suggests how in an ST the ST Author can address authorization of Normal Users to perform non-administrative functions by adding the appropriate security objectives, threats, assumptions and SFRs, since in IEEE Std 2600.3 this authorization is not specified.

Additional Guidance: Since IEEE Std 2600.1 [B8] requires user authorization to access TOE functions, the ST Author should look at the security objectives (e.g., O.USER_AUTHORIZED and OE.USER_AUTHORIZED), associated threats (e.g., T.DOC.DIS), OSPs (P.USER.AUTHORIZATION) and SFRs that map to these objectives in IEEE Std 2600.1 Clauses 7, 8 and 10 to determine what should be added to the ST to address authorization of Normal Users to perform non-administrative functions. The ST Author should keep in mind that when doing this make sure to include the proper wording to restrict required authorization only to U.NORMAL (i.e., Normal Users) performing non-administrative functions.

See the Additional Guidance to the PP Application Notes for the FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 SFRs in for more information on how to specify this authentication in the ST.

5. Security Objectives (PP Clause 8)

- a). **PP APPLICATION NOTE 5** — Discusses what the ST Author should consider if the TOE provides an internal capability to provide access to audit records.

- b). **PP APPLICATION NOTE 6** — Discusses what the ST Author should consider if both the TOE and an IT product external to the TOE (e.g., an audit server) provide audit storage capabilities.

Additional Guidance: This PP APPLICATION NOTE as worded in [B8] is fairly self-explanatory. The guidance in 6.6 on specifying SFRs applies here also. The ST Author should just review the ST before submittal to make sure that access to and storage of audit records are adequately covered in both the security objectives and SFRs to the extent that these are done by the TOE.

The ST Author should keep in mind that if the TOE provides audit record access to only an authorized administrator that can be address in one of the security management SFRs such as FMT_SMR. Also, if the TOE only allows downloading of audit records for storage on an external server or client then no security objectives or SFRs associated with audit storage are needed in the ST because this function is being addressed by the TOE's IT environment.

6.9.2 Common SFR PP Application Notes (PP Clause 10)

1. Class FAU: Security Audit

- a). **PP APPLICATION NOTE 7** -- Discusses what the ST Author should consider in terms of additional SFRs if the TOE provides an internal capability to store and provide access to audit records.

PP APPLICATION NOTE 8 -- Discusses what the ST Author should consider in terms of additional SFRs if audit storage capabilities are provided both internally (by the TOE) and externally (by a trusted IT product).

Additional Guidance: An example of additional SFR requirements that can be added to address storing and providing access to audit records is:

FAU_SAR.1	Audit review
FAU_SAR.1.1:	The TSF shall provide [U.ADMINISTRATOR] with the capability to read [all information] from the audit records.
FAU_SAR.1.2:	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	Restricted audit review
FAU_SAR.2.1:	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAU_STG.1	Protected audit trail storage
FAU_STG.1.1:	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2:	The TSF shall be able to <u>prevent</u> unauthorized modifications to the stored audit records in the audit trail.
FAU_STG.4	Prevention of audit data loss
FAU_STG.4.1:	The TSF shall <u>overwrite the oldest stored audit records</u> and [no other actions to be taken] if the audit trail is full.

This example is for a case where the audit records are stored on the TOE but then must be downloaded from the TOE to an external client to be reviewed and analyzed.

- b). **PP APPLICATION NOTE 9** – Indicates that any additional audit requirements and recommendations that exist in SFR Packages to which a Security Target conforms do not supersede the requirements and recommendations in PP Clause 10.1.

Additional Guidance: See the Additional Guidance in 6.9.2, Item 1.a.

- c). **PP APPLICATION NOTE 10 (FAU_GEN.1)** — Suggests what the ST Author should do when, for a specified Common Criteria defined audit level (minimum, basic, or detailed), there are conflicts among the SFRs and the requirements listed in the applicable Audit data requirements table.

Additional Guidance: The phrase “the greater of those requirements” in PP APPLICATION NOTE 10 refers to the fact that per CC Part 2 [B3] auditable events are hierarchical. This means that if a Basic audit level (which is considered a more stringent audit level than Minimal) is chosen the auditable events for both the Basic and Minimal auditable levels specified in CC Part 2 for the SFRs included in the ST must be collected. This creates the conflict mentioned in PP APPLICATION NOTE 10 because selected SFRs documented in Common Criteria Part 2 [B3] provide required audit requirements based on the level specified (see Common Criteria Part 2,

Appendix C.3 in [B3] for a description of what the Common Criteria defined audit levels mean). The ST Author has to be aware of these conflicts when creating the ST.

As an example of this potential conflict, consider the FIA_UAU.1, Timing of authentication SFR. Table 14 in IEEE Std 2600.1 [B8] requires for FIA_UAU.1 that “Both successful and unsuccessful use of the authentication mechanism” be a recorded auditable event to satisfy the Basic audit level requirement. If the ST specified that auditable events require only that the Minimum audit level be satisfied, Common Criteria Part 2, Section 12.4 [B3] indicates that for FIA_UAU.1 at the Minimum audit level only “Unsuccessful use of the authentication mechanism” be the recorded auditable event in the audit log. The ST would still have to indicate that the TOE records both successful and unsuccessful use of the authentication mechanism for the ST to be able to state conformance to IEEE Std 2600.1 [B8].

- d). **PP APPLICATION NOTES 11 & 12** (FAU_GEN.1) — Indicates that additional required and recommended auditable events are included in PP Clause 10.1.

Additional Guidance: The ST Author should keep in mind that any auditable events listed in the [the applicable Audit data recommendations table] in any of the IEEE Std 2600 Series of Protection Profiles ([B8]-[B11]) are not required so the ST Author is free to not included them in the ST. However, for any “recommended” item it is good practice on the part of the ST Author to include some rationale as to why that item (the recommended auditable events in this case) is not applicable or is not included in the ST; an Evaluation Lab is likely to ask for such rationale.

- e). **PP APPLICATION NOTE 13** (FAU_GEN.1) (IEEE Std 2600.2 Only) – Indicates that FAU_GEN.1 is a principal SFR for fulfilling the listed security objective and is a dependency of the indicated SFR.

Additional Guidance: No additional guidance is deemed necessary.

- f). **PP APPLICATION NOTE 14** (FAU_GEN.1) (IEEE Std 2600.2 Only) – Indicates that the FAU_GEN.1 SFR performs audit functions for the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- g). **PP APPLICATION NOTE 13** (FAU_GEN.2) – Indicates that FAU_GEN.2 is a principal SFR for fulfilling the listed security objective.

Additional Guidance: No additional guidance is deemed necessary.

- h). **PP APPLICATION NOTE 14** (FAU_GEN.2) – Indicates that the FAU_GEN.2 SFR performs audit functions for the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

2. Class FDP: User data protection

- a). **PP APPLICATION NOTE 15** – Indicates when the access control rules apply to the specified object in the applicable SFR Package attributes table.

PP APPLICATION NOTE 16 — Defines what it means for a User to “own” a document .

PP APPLICATION NOTE 17 — Discusses adding appropriate Access control rules for the “Create” Operation in a conforming TOE.

Additional Guidance: As an example of the type of additional rules that could be added here (using the format of the applicable table in any of the PPs from the IEEE Std 2600 Series of Protection Profiles) suppose the goal is to document in the ST preventing an authorized System Administrator from reading or modifying anyone else’s documents, while still permitting the Administrator to delete others’ documents. The Common Access Control SFP could be changed to look as follows:

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	attributes from [applicable SFR Package attributes table]	Delete	U.NORMAL	Denied, except for his/her own documents
		Read; Modify	U.ADMINISTRATOR	Denied, except for his/her own documents
D.FUNC	attributes from [applicable SFR Package attributes table]	Modify; Delete	U.NORMAL	Denied, except for his/her own documents

Keep in mind that any items added to the existing Common Access Control SFP must only further restrict access; otherwise the Common Access Control SFP will be violated.

- b). **PP APPLICATION NOTE 18** — Indicates that conformance to one or more of the named SFR Packages in a PP may expand the rules by adding access controls for additional objects, security attributes, or roles.

Additional Guidance: This applies not only to objects, security attributes and roles but to security objectives, threats, assumptions and SFRs – if an ST claims conformance to any of the SFR packages that means that the ST conforms to the union of the objects, security attributes, roles security objectives, threats, assumptions, SFRs, etc. specified in the main body of the PP and the objects, security attributes, roles security objectives, threats, assumptions, SFRs, etc. specified in the applicable SFR package.

- c). **PP APPLICATION NOTE 19** — Indicates when an ST Author may refine these rules by adding additional security attributes or additional roles.

PP APPLICATION NOTE 20 — Discusses when an ST Author may define additional objects and access control rules for those objects.

Additional Guidance: The example in 6.9.2, Item 2.a shows how the current access control policy rules can be amended in a case where there is no violation of the access control policy.

As an example of where there would be a violation, if the TOE allows anyone to delete anyone's document as is the case on many digital copiers, the access control policy table would then be:

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	attributes from [applicable SFR Package attributes table]	Delete	U.NORMAL	Authorized
D.FUNC	attributes from [applicable SFR Package attributes table]	Modify; Delete	U.NORMAL	Denied, except for his/her own documents

If the intent is to conform to IEEE Std 2600.1[B8], this would clearly violate the Common Access Control Policy specified in IEEE Std 2600.1 [B8].

The ST Author needs to make sure that any additional access control rules added are truly additive to the access control rules specified in the PP being conformed to.

- d). **PP APPLICATION NOTE 21** (FDP_ACC.1(a)) – Indicates that FDP_ACC.1(a) is a principal SFR for fulfilling the listed security objectives and a dependency of the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- e). **PP APPLICATION NOTE 22** (FDP_ACC.1(b)) — States what comprises the TOE Function Access Control SFP.

Additional Guidance: The sum of the various assignments and selections in the ST for TOE functions, security attributes and associated actions in the FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b), and FMT_MSA.3(b) SFRs should include all of the security functions that the ST Author wants to claim for the TOE.

- f). **PP APPLICATION NOTE 23** (FDP_ACC.1(b)) — Provides more information about the TOE Function Access Control SFP for the FDP_ACC.1(b) SFR.

Additional Guidance: See the Additional Guidance for PP APPLICATION NOTE 24.

- g). **PP APPLICATION NOTE 24** (FDP_ACC.1(b)) — Indicates how the TOE Function Access Control SFP may be defined for the FDP_ACC.1(b) SFR.

Additional Guidance: An example of stating a policy between users and objects is:

FDP_ACF.1.1(b)	The TSF shall enforce the TOE Function Access Control SFP to objects based on the following: users and [Objects: functions accessible by authorized users].
-----------------------	---

An example of stating a policy between subjects and objects is:

FDP_ACF.1.1(b)	The TSF shall enforce the TOE Function Access Control SFP to objects based on the following: users and [Subjects: users acting in the role U.ADMINISTRATOR ; Objects: functions accessible by users acting in the role U.ADMINISTRATOR].
-----------------------	--

- h). **PP APPLICATION NOTE 25** (FDP_ACC.1(b)) – Indicates that FDP_ACC.1(b) is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- i). **PP APPLICATION NOTE 26** (FDP_ACC.1(b)) – Indicates that FDP_ACF.1(a) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- j). **PP APPLICATION NOTES 27, 51 & 56** – Indicates that the TOE Function Access Control SFP is composed of the listed SFRs.

Additional Guidance: PP APPLICATION NOTE 23 describes what the TOE Function Access Control SFP actually is. For additional guidance see 6.9.2, Item 2.g.

- k). **PP APPLICATION NOTE 28** (FDP_ACF.1(b)) — Provides guidance on what the list of functions for the FDP_ACF.1(b) SFR should include.

Additional Guidance: One approach to listing all the applicable functions would be to state SFR component FDP_ACF.1.2(b) as follows:

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: <i>[a user that is authorized to use the TOE is automatically authorized to use the functions accessible via the management interfaces]</i> .
-----------------------	---

and then include in the FMT_SMF.1 SFR the list of TSF management functions (e.g., access to certain non-System Administrator machine features such as the ability to make color copies) an authorized user would be able to use.

In the case where you had a TOE and only an authorized system administrator could access the TSF management functions, FDP_ACF.1.2(b) might be stated something like:

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: [a user acting in the role of U.ADMINISTRATOR will be granted access to the TOE security relevant functions accessible via the management interfaces].
-----------------------	--

and then include in the FMT_SMF.1 SFR the list of TSF management functions (e.g., enabling/disabling security features on the device, downloading an audit log) an authorized System Administrator would be able to use.

- l). **PP APPLICATION NOTE 29** (FDP_ACF.1(b)) — Suggests what functions the ST Author may specify depending on which combination of selections are made in the FDP_ACF.1(b) SFR.

Additional Guidance: See the example in 6.9.2, Item 2.k.

- m). **PP APPLICATION NOTE 30** (FDP_ACF.1(b)) — Indicates that for the FDP_ACF.1(b) SFR the ST author may define access control rules common for all functions.

Additional Guidance: An example of the type of additional access control rules (italicized) the ST Author can add⁴⁷ for FDP_ACF.1 is:

FDP_ACF.1.1(a)	The TSF shall enforce the Common Access Control SFP in Table 10 to objects based on the following: [the list of users as subjects and objects controlled under the Common Access Control SFP in Table 16, and for each, the indicated severity attributes in Table 16; <i>Subjects: Authorized users – role; Objects: functions accessible via User Interface – role</i>].
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 16 governing access among controller users as subjects and controlled objects using controlled operations on controlled objects; <i>authorized user(s) in System Administrator role will be granted access to the TOE security relevant functions accessible via the management interfaces</i>].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [<i>no additional access rules</i>].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [<i>no denial of access rules</i>].

- n). **PP APPLICATION NOTE 31** (FDP_ACF.1(b)) – Indicates that FDP_ACF.1(b) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- o). **PP APPLICATION NOTE 32** (FDP_RIP.1) – Indicates that FDP_RIP.1 is a principal SFR for fulfilling the listed security objective.

Additional Guidance: No additional guidance is deemed necessary.

- p). **PP APPLICATION NOTE 7** (IEEE Std 2600.4 Only) – Indicates that in Operational Environment D User Data is not protected from unauthorized disclosure or alteration.

Additional Guidance: No additional guidance is deemed necessary.

⁴⁷ In this example, the access control rules govern access to device security features by an authorized System Administrator and by other “Normal” users.

3. Class FIA: Identification and authentication

- a). **PP APPLICATION NOTE 33** (FIA_ATD.1) – Indicates that FIA_ATD.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- b). **PP APPLICATION NOTES 34 & 39** (FIA_UAU.1 & FIA_UID.1) — Suggests what the ST Author should consider if certain functions are desired in the ST’s TOE that do not require user identification and authorization.

Additional Guidance: An example of TSF-mediated actions for FIA_UAU.1.1 and FIA_UID.1 where a user is allowed no action until being identified and authenticated (which might be the case for a secure system under Operational Environment A) is:

FIA_UAU.1.1	The TSF shall allow [<i>None</i>] on behalf of the user to be performed before the user is authenticated.
FIA_UID.1.1	The TSF shall allow [<i>None</i>] on behalf of the user to be performed before the user is identified.

- c). **PP APPLICATION NOTES 35 & 40** (FIA_UAU.1 & FIA_UID.1) — States that user I&A may be performed internally by the TOE or externally by a trusted IT product in the operational environment.

PP APPLICATION NOTE 36 (FIA_UAU.1) — Suggest what the ST Author should add if user authentication or identification is performed internally.

PP APPLICATION NOTES 37 & 41 (FIA_UAU.1 & FIA_UID.1) — Suggests how the ST Author should express I&A if user authentication or identification can be performed internally (by the TOE) or externally (by a trusted IT product).

Additional Guidance: The important thing for the ST Author here is that the ST only has to cover user identification and authentication mechanisms done all or in part by the TOE. An example of what might go into FIA_AFL.1 and FIA_UAU.7 to document user I&A requirements is:

FIA_AFL.1.1	The TSF shall detect when <n> ⁴⁸ unsuccessful authentication attempts occur related to [authentication at the Graphical User Interface].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been <i>met</i> , the TSF shall [lockout user login for a period of 3 minutes on the Graphical User Interface].
FIA_UAU.7.1	The TSF shall provide only [obscured feedback] to the user while the authentication is in progress.

- d). **PP APPLICATION NOTE 38** (FIA_UAU.1) – Indicates that FIA_UAU.1 is a principal SFR for fulfilling the listed security objectives.

Additional Guidance: No additional guidance is deemed necessary.

- e). **PP APPLICATION NOTE 42** (FIA_UID.1) – Indicates that FIA_UID.1 is a principal SFR for fulfilling the listed security objectives and a dependency of the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- f). **PP APPLICATION NOTE 43** — States that the PP assumes there is no difference between Users and Subjects.

Additional Guidance: See the discussion in 4.2.2.2 for further guidance.

⁴⁸ <n> is the number of unsuccessful authentication attempts

- g). **PP APPLICATION NOTE 44** (FIA_USB.1) – Indicates that FIA_USB.1 is a principal SFR for fulfilling the listed security objective.

Additional Guidance: No additional guidance is deemed necessary.

4. Class FMT: Security management

- a). **PP APPLICATION NOTE 45** — Indicates that the ST Author should identify the specific TSF protected and TSF confidential data in the TOE and define how those data are initialized and managed.

Additional Guidance: This relates to the discussion in 6.5.1 about determining the confidential and protected TSF Data for a TOE; the protected data becomes the data that comprises D.PROT and the confidential data becomes the data that comprises D.CONF; this data would be documented in the ST in the equivalent of Table 4 in IEEE Std 2600.1 [B8], for example.

An example of how this might be documented iteratively in an ST for FMT_MSA.1 and FMT_MSA.3 is:

FMT_MSA.1.1(a)	The TSF shall enforce the TOE Function Access Control Policy, [User Data Protection SFP ⁴⁹] to restrict the ability to <u>change default, modify, delete [all security attributes]</u> to [Nobody].
FMT_MSA.3.1(a)	The TSF shall enforce the TOE Function Access Control Policy, [User Data Protection SFP] to provide [<u>fixed</u>] default values for security attributes that are used to enforce the SFPs.
FMT_MSA.3.2(a)	The TSF shall allow [Nobody] to specify alternative initial values to override the default values when an object or information is created.
FMT_MSA.1.1(b)	The TSF shall enforce the TOE Function Access Control Policy, [Information Flow Control SFP ⁵⁰] to restrict the ability to <u>change default, query, modify, delete [all security attributes]</u> to [nobody].
FMT_MSA.3.1(b)	The TSF shall enforce the TOE Function Access Control Policy, [Information Flow Control SFP] to provide [<u>fixed</u>] default values for security attributes that are used to enforce the SFPs.
FMT_MSA.3.2(b)	The TSF shall allow [Nobody] to specify alternative initial values to override the default values when an object or information is created.

An example of an iterative use of FMT_MTD.1 for TSF Data is:

FMT_MTD.1.1(a)	The TSF shall restrict the ability to <u>clear, delete, [create, read [download]]</u> the [Audit log] to [U.ADMINISTRATOR].
FMT_MTD.1.1(b)	The TSF shall restrict the ability to <u>query, modify, delete, [create]</u> the [IP filter rules] to [U.ADMINISTRATOR].

- b). **PP APPLICATION NOTE 46** (FMT_MSA.1(a)) — Provides further direction on security attributes and how the ST Author should define them.

PP APPLICATION NOTE 49 (FMT_MSA.1(b)) — Discusses the security attribute(s) that need to be instantiated by the ST Author for the FMT_MSA.1(b) SFR.

Additional Guidance: An example of how security attributes can be defined in the FMT_MSA.1 SFR is:

⁴⁹ The User Data Protection SFP in this case could be a policy added to the Common Access Control SFP in the ST that addresses protection of User and TSF Data stored in nonvolatile storage.

⁵⁰ The Information Flow Control SFP in this case could be a policy added to the Common Access Control SFP in the ST that addresses information sent to the TOE from an external trusted IT product.

FMT_MSA.1.1(a)	The TSF shall enforce the Common Access Control SFP to restrict the ability to <i>change default, modify, delete</i> [<i>Security Relevant Roles, Authentication Data, User Identifier</i>] to [U.ADMINISTRATOR].
FMT_MSA.1.1(b)	The TSF shall enforce the Common Access Control SFP to restrict the ability to <i>query</i> [<i>Authentication Data, User Identifier</i>] to [U.NORMAL].

- c). **PP APPLICATION NOTE 47** (FMT_MSA.1(a)) – Indicates that FMT_MSA.1(a) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- d). **PP APPLICATION NOTE 48** (FMT_MSA.1(a)) – Indicates that FMT_MSA.1(a) performs management functions recommended for the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- e). **PP APPLICATION NOTE 50** (FMT_MSA.1(b)) — Indicates what should be done if the TOE function access control policy does not allow anyone to change a user’s ability to execute a function.

Additional Guidance: See 6.9.2, Item 4.a for an example on how to use ‘Nobody’ in the context of access control policy in an SFR.

- f). **PP APPLICATION NOTE 52** (FMT_MSA.1(b)) – Indicates that FMT_MSA.1(b) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- g). **PP APPLICATION NOTE 53** (FMT_MSA.1(b)) – Indicates that FMT_MSA.1(b) performs management functions recommended for the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- h). **PP APPLICATION NOTE 54** (FMT_MSA.3(a)) — Discusses restrictions on how User and object security attributes are initialized when the user or object is created.

Additional Guidance: This PP APPLICATION NOTE is associated with the FMT_MSA.3 SFR. Using the same security attributes as in 6.9.2, Item 4.b an example of how initialization can be documented in FMT_MSA.3 is:

FMT_MSA.3.1(b)	The TSF shall enforce the TOE Function Access Control Policy, [Attribute Initialization SFP] to provide [<i>fixed</i>] default values for security attributes that are used to enforce the SFPs.
FMT_MSA.3.2(b)	The TSF shall allow [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

where the Attribute Initialization SFP could be something as simple as:

Attribute	Operation(s)	Subject	Access control rule
All Security Attributes	Initialize	U.ADMINISTRATOR	Authorized
		U.NORMAL	Denied

- i). **PP APPLICATION NOTE 55** (FMT_MSA.3(a)) – Indicates that FMT_MSA.3(a) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- j). **PP APPLICATION NOTE 57** (FMT_MSA.3(b))— Discusses the default values for the access to TOE functions assigned to a user when that user is defined.

Additional Guidance: See 6.9.2, Item 4.h above for an example of defining roles to define default values in FMT_MSA.3.2; 6.9.2, Item 4.a provides an example of the ‘Nobody’ case.

- k). **PP APPLICATION NOTE 58** (FMT_MSA.3(b)) – Indicates that FMT_MSA.3(b) is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- l). **PP APPLICATION NOTE 59** (FMT_MTD.1) — Provides ST Author guidance on the iterations of FMT_MTD.1.1 SFR component.

Additional Guidance: No additional guidance is deemed necessary.

- m). **PP APPLICATION NOTE 60** (FMT_MTD.1(a) & (FMT_MTD.1(b)) – Indicates that FMT_MTD.1(a) & FMT_MTD.1(b) are both principle SFRs to fulfill the listed security objectives.

Additional Guidance: No additional guidance is deemed necessary.

- n). **PP APPLICATION NOTE 61** (FMT_SMF.1) — Suggests that the ST Author should consider specifying other management functions that support administrative functionality of the ST TOE beyond those indicated in the FMT_SMF.1 SFR.

Additional Guidance: Some of the types of management functions that can be specified are:

- Enable / Disable / Invoke / Configure security functions and security protocols
- Read / store / download / analyze Audit Logs
- Create / upload / download X.509 certificates
- Create / delete user accounts
- Create / change security-related passwords/PINs
- Create/delete security-related keys (e.g., authentication keys)
- Enable / Disable / Configure internal firewalls or IP filtering
- Network configuration

- o). **PP APPLICATION NOTE 62** (FMT_SMF.1) – Indicates that FMT_SMF.1 is a dependency of the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- p). **PP APPLICATION NOTE 63** (FMT_SMF.1) – Indicates that FMT_SMF.1 performs management functions recommended for the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

- q). **PP APPLICATION NOTE 64** (FMT_SMR.1) — Discusses the role “Nobody” included in FMT_SMR.1.1 SFR component.

Additional Guidance: The ST Author should make sure the role “Nobody” is properly used within the ST to meet the definition included in this PP Application Note.

- r). **PP APPLICATION NOTE 65** (FMT_SMR.1) – Indicates that FMT_SMR.1 is a dependency of the listed SFRs.

Additional Guidance: No additional guidance is deemed necessary.

5. Class FPT: Protection of the TSF

- a). **PP APPLICATION NOTE 66** (FPT_STM.1) — Provides explanation on how the PPs interprets FPT_STM.1 to be satisfied.

PP APPLICATION NOTE 67 (FPT_STM.1) — Provides suggestions on what SFRs the ST Author should consider including in the ST if reliable time stamps are generated outside of the TOE.

PP APPLICATION NOTE 68 (FPT_STM.1) — Provides ST Author guidance if a product can use either internal or external time stamp sources.

Additional Guidance: The intent is that if the TOE receives its time from a centralized time server (e.g., via the Network Time Protocol) which is outside of the TOE, the ST Author should make sure that any requirements on the TOE associated with accepting time input from the external time server are added to the basic FPT_STM.1 requirement.

For example, assuming the TOE uses Network Time Protocol to obtain its time there is the problem that a time skew could be required to allow for minor variances in machine time to that which is received from the time server such that if the received time is outside the allowable skew time, the system will reset the time to the received value. The ST Author might want to consider in this case either extending the FPT_STM.1.1 SFR to read something like “The TSF shall be able to provide reliable time stamps *that are within [x] seconds of the time value obtained from a time server*” (where x can be whatever value is appropriate for the TOE).

- b). **PP APPLICATION NOTE 69 (FPT_STM.1)** – Indicates that FPT_STM.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- c). **PP APPLICATION NOTE 70 (FPT_TST.1)** — Explains the intent of the FPT_TST.1.3 SFR component.

Additional Guidance: No additional guidance is deemed necessary.

- d). **PP APPLICATION NOTE 71 (FPT_TST.1)** – Indicates that FPT_TST.1 is a principle SFR to fulfill the listed security objective.

Additional Guidance: No additional guidance is deemed necessary.

6. Class FTA: TOE access

PP APPLICATION NOTE 72 (FTA_SSL.1) – Indicates that FTA_SSL.1 is a principle SFR to fulfill the listed security objectives.

Additional Guidance: No additional guidance is deemed necessary.

6.9.3 SFR Package Usage

PP APPLICATION NOTE 73 - Indicates that the ST Author can define additional subjects, objects, security attributes or rules as long as these added entities do not contradict the entities listed in both Clause 10.4 and the access control SFRs in the PP from the IEEE Std 2600 Series of Protection Profiles that the ST is to conform to.

Additional Guidance: As an example of an additional subjects, objects, security attributes or rules that could be added, assume the ST is to conform to IEEE Std 2600.1 [B8] and that the TOE should enforce a policy that all print jobs initiated from a print client must be encrypted via IPSec when it is submitted to the TOE. In that case, the ST Author might define an additional “Print User Data Protection” Security Function Policy in the PRT SFR Package that could look something like:

The security function “Print User Data Protection” requires that network traffic to and from the TOE will be encrypted when the printing client initiates IPSec encryption. This policy will be enforced on:

- SUBJECTS: Printing clients.
- INFORMATION: All Port 9100 traffic to and from that destination.
- OPERATIONS: Print jobs.

Such a policy would be permissible because it doesn’t contradict (in fact, it provides further restrictions to) any policies or access control SFRs required by IEEE Std 2600.1.

6.9.4 PRT SFR Package PP Application Notes

Class FDP: User data protection

- a). **PP APPLICATION NOTE 74** – Provides explanation as to what the “Read” operation refers to in the PRT Access Control SFP.

PP APPLICATION NOTE 75 – Provides further explanation on when a User needs to authenticate using the Operator Panel on the TOE to perform the “Read” operation for the PRT Access Control SFP.

PP APPLICATION NOTE 76 – Indicates what the ST Author should add if a conforming TOE provides a feature for modifying a submitted document before printing.

Additional Guidance: An example of such an additional rule (allowing only a user to modify his/her own document before printing) is:

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

PP APPLICATION NOTES 74 and 75 are included to qualify what is meant by “read” in the context of the PRT SFR Package and when user re-authentication might be needed to “read” a submitted print job. Neither the PRT Access Control SFP itself or either of these two PP Application Notes explicitly indicates how a submitted print job is released to the Hardcopy Output Handler, but there is an implicit assumption here that it is done for each submitted print job one-at-a-time.

In the case where the TOE supports allowing submitted jobs to be queued for processing and release to the Hardcopy Output Handler, the ST Author should extend the definition of “read” in the PRT SFR Package to allow for jobs to be queued and then “read” together rather than one-at-a-time.

Finally, PP APPLICATION NOTE 75 should not be interpreted to mean that every time a user wants to view the status of a print job or view the job data associated with a submitted print job the user has to do this from the Operator Panel, even if the job was submitted from the user’s PC. The intent here of the authors of the IEEE Std 2600 Series of Protection Profiles is to deal with the situation where a user is authenticated in some way to access services or features of the HCD (in this case the print function) and under what circumstances the user might have to re-authenticate to get access to the print function; it was not the intent to apply to authenticating the user each time to do normal user functions like checking job status.

The intent of the PRT Access Control SFP, however, is to apply only to any “read” operation being performed by the user on the TOE itself ; it does not apply to any “read” operation performed by a user externally to the TOE (such as on a PC). Thus, it is no violation of the PRT Access Control SFP if a user who submits the job allows anyone else to view the submitted print job.

- b). **PP APPLICATION NOTE 77 (FDP_ACC.1)** – Indicates that FDP_ACC.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- c). **PP APPLICATION NOTE 78 (FDP_ACF.1)** — Suggests how the ST Author can address the FMT_MSA.3 SFR being a dependency of the FDP_ACF.1 SFR with respect to the PRT Access Control SFP.

Additional Guidance: The additional management of attributes and roles for the PRT function could be specified in an FMT_MSA.3 in the PRT SFR Package as follows:

FMT_MSA.3.1	The TSF shall enforce the PRT Access Control SFP to provide <i>[permissive]</i> default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow <i>[U.NORMAL]</i> to specify alternative initial values to override the default values when an object or information is created.

where in this example a security attribute for the print function might be a secure password that allows the user access to modify his/her document.

- d). **PP APPLICATION NOTE 79** (FDP_ACF.1) – Indicates that FDP_ACF.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

6.9.5 SCN SFR Package PP Application Notes

Class FDP: User data protection

- a). **PP APPLICATION NOTE 80** – Provides explanation as to what the “Read” operation refers to in the SCN Access Control SFP.

PP APPLICATION NOTE 81 – Suggests what the ST Author should add if a conforming TOE provides a feature for modifying a scanned document before transmission.

Additional Guidance: An example of such an additional rule (allowing only a user to modify his/her own document before transmission) is:

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

- b). **PP APPLICATION NOTE 82** (FDP_ACC.1) – Indicates that FDP_ACC.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- c). **PP APPLICATION NOTE 83** (FDP_ACF.1) — Suggests how the ST Author can address the FMT_MSA.3 SFR being a dependency of FDP_ACF.1 SFR with respect to the SCN Access Control SFP.

Additional Guidance: The additional management of attributes and roles for the SCN function could be specified in an FMT_MSA.3 in the SCN SFR Package as follows:

FMT_MSA.3.1	The TSF shall enforce the SCN Access Control SFP to provide [<i>permissive</i>] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [<i>U.NORMAL</i>] to specify alternative initial values to override the default values when an object or information is created.

where, similar to the PRT function, in this example a security attribute for the SCN function might also be a secure password that allows the user access to modify his/her document before transmission.

- d). **PP APPLICATION NOTE 84** (FDP_ACF.1) – Indicates that FDP_ACF.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

6.9.6 CPY SFR Package PP Application Notes

Class FDP: User data protection

- a). **PP APPLICATION NOTE 85** – Provides explanation as to what the “Read” operation refers to in the CPY Access Control SFP.

PP APPLICATION NOTE 86 – Suggests that the ST Author can create more restrictive access control rules because there are no access control requirements for release of User Document Data to the Hardcopy Output Handler in the CPY Access Control SFP.

PP APPLICATION NOTE 87 – Suggests what the ST Author should add if a conforming TOE provides a feature for modifying a scanned document before printing a copy.

Additional Guidance: An example of a CPY Access Control SFP allowing only a user to modify his/her own document before copying is:

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

- b). **PP APPLICATION NOTE 88** (FDP_ACC.1) – Indicates that FDP_ACC.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- c). **PP APPLICATION NOTE 89** (FDP_ACF.1) — Suggests how the ST Author can address the FMT_MSA.3 SFR being a dependency of the FDP_ACF.1 SFR with respect to the CPY Access Control SFP.

Additional Guidance: The additional management of attributes and roles for the CPY function could be specified in an FMT_MSA.3 in the CPY SFR Package as follows:

FMT_MSA.3.1	The TSF shall enforce the SCN Access Control SFP to provide <i>[permissive]</i> default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow <i>[U.NORMAL]</i> to specify alternative initial values to override the default values when an object or information is created.

where, similar to the PRT and SCN functions, in this example a security attribute for the CPY function might also be a secure password that allows the user access to modify his/her document before copying.

- d). **PP APPLICATION NOTE 90** (FDP_ACF.1) – Indicates that FDP_ACF.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

6.9.7 FAX SFR Package PP Application Notes

Class FDP: User data protection

- a). **PP APPLICATION NOTE 91** – Provides explanation as to what the “Read” operation refers to in the FAX Access Control SFP.

PP APPLICATION NOTE 92 – Provides explanation as to whom the “owner” of a received fax job is and when the ST Author may refine this role.

Additional Guidance: See 6.9.7, Item b.

- b). **PP APPLICATION NOTE 93** – Suggests what the ST Author should consider adding if a conforming TOE provides a feature that allows an administrator to manage ownership of a received fax job.

PP APPLICATION NOTE 94 – Suggests what the ST Author should consider adding if a conforming TOE provides a feature that allows an administrator to manage the transmission of or delete outgoing fax documents.

PP APPLICATION NOTE 95 – Suggests what the ST Author should consider adding if a conforming TOE provides a feature for modifying a document before creating hardcopy output or transmission.

PP APPLICATION NOTE 96 – Suggests what the ST Author should consider adding if a conforming TOE provides a feature for modifying a document before creating hardcopy output or transmitting outgoing fax documents.

Additional Guidance: Similar to the example presented above for PP APPLICATION NOTE 81, an example of an additional rule (allowing only the owner of a sending FAX to modify his/her own document before transmission) that takes into account PP APPLICATION NOTES 93-96 above is:

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

Similarly, the case of an additional rule for the owner of a received Fax document to be able to modify the received Fax document prior to printing would be similar to the example for PP APPLICATION NOTE 56 (taking into account the PP APPLICATION NOTES 93-96 above):

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+FAXIN	Read, Modify	U.NORMAL	Denied, except if authorized by U.ADMINISTRATOR.
D.DOC	+FAXIN	Modify	U.ADMINISTRATOR	Denied, except for his/her own documents ⁵¹

Note that in the case of a received Fax document, the Administrator is considered the “owner” of the received Fax document unless the Administrator assigns ownership to a user; that accounts for the difference between this example and the Printing example for PP APPLICATION NOTE 56.

- c). **PP APPLICATION NOTE 97** (FDP_ACC.1) – Indicates that FDP_ACC.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- d). **PP APPLICATION NOTE 98** (FDP_ACF.1) — Suggests how the ST Author can address the FMT_MSA.3 SFR being a dependency of the FDP_ACF.1 SFR with respect to the FAX Access Control SFP.

Additional Guidance: The additional management of attributes and roles for the FAX function could be specified in an FMT_MSA.3 in the FAX SFR Package as follows:

FMT_MSA.3.1	The TSF shall enforce the FAX Access Control SFP to provide [<i>permissive</i>] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [<i>U.ADMINISTRATOR, U.NORMAL</i>] to specify alternative initial values to override the default values when an object or information is created.

where, similar to the PRT and SCN functions, in this example a security attribute for the FAX function might be a secure password that allows the user or Administrator access to print a received Fax document.

- e). **PP APPLICATION NOTE 99** (FDP_ACF.1) – Indicates that FDP_ACF.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

⁵¹ The ST Author would have to state somewhere that U.ADMINISTRATOR is considered the owner of a received Fax document unless the U.ADMINISTRATOR assigns another user to be the owner.

6.9.8 DSR SFR Package PP Application Notes

Class FDP: User data protection

- a). **PP APPLICATION NOTE 100** – Provides explanation as to what the “Read” operation refers to in the DSR Access Control SFP.

PP APPLICATION NOTE 101 – Suggests what the ST Author should consider adding if a conforming TOE provides a feature for modifying a document that has been stored in the TOE.

Additional Guidance: An example of such an additional rule allowing only a user to read and modify his/her own document that has been stored in the TOE is:

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+DSR	Read, Modify	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
D.DOC	+DSR	Read, Modify	U.ADMINISTRATOR	Denied

- b). **PP APPLICATION NOTE 102** – Provides ST Author guidance on specifying access control rules for the DSR function.

PP APPLICATION NOTE 103 – Indicates what the ST Author should specify if the conforming TOE provides for authorization of users to read or modify another user’s documents.

Additional Guidance: Similar to 6.9.4, Item a, an additional access control rule allowing a System Administrator and anyone authorized by the System Administrator (e.g., someone delegated by the System Administrator to act in the role of a System Administrator) to read or modify another user’s documents while it is being stored in the TOE would be something like:

Object	Attribute(s)	Operation	Subject	Access control rule
D.DOC	+DSR	Read, Modify	U.NORMAL	Denied, except when authorized by U.ADMINISTRATOR

- c). **PP APPLICATION NOTE 104 (FDP_ACC.1)** – Indicates that FDP_ACC.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- d). **PP APPLICATION NOTE 105 (FDP_ACF.1)** — Suggests how the ST Author can address the FMT_MSA.3 SFR being a dependency of the FDP_ACF.1 SFR with respect to the DSR Access Control SFP.

Additional Guidance: The additional management of attributes and roles for the DSR function could be specified in an FMT_MSA.3 in the DSR SFR Package as follows:

FMT_MSA.3.1	The TSF shall enforce the DSR Access Control SFP to provide <i>[fixed]</i> default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [<i>U.ADMINISTRATOR</i>] to specify alternative initial values to override the default values when an object or information is created.

where in this example a security attribute for the DSR function might be some type of secure password that allows the System Administrator to retrieve files stored in the TOE.

- e). **PP APPLICATION NOTE 106 (FDP_ACF.1)** – Indicates that FDP_ACF.1 is a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

6.9.9 NVS SFR Package PP Application Notes

Class FPT: Protection of the TSF

- a). **PP APPLICATION NOTE 107** (FPT_CIP_EXP.1) — Provides guidance on what the ST Author should define with respect to the methods used to protect the confidentiality and integrity of the data stored in NVS.

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

Additional Guidance: Although the PPs do not imply a specific method for protecting the confidentiality and integrity of data stored in nonvolatile storage, the primary method being used today for this purpose is to encrypt data stored in nonvolatile storage as indicated in PP APPLICATION NOTE 107. If encryption is to be used the ST Author should make sure that the proper SFRs from the FCS Class (Cryptography) as also included in the ST.

Typically, the minimum SFRs that should be included if encryption of nonvolatile storage is used are FCS_CKM.1, Cryptographic key generation; FCS_CKM.2, Cryptographic key distribution; FCS_CKM.4, Cryptographic key destruction and FCS_COP.1, Cryptographic operation.

An example of how these four SFRs could be stated in the case where AES is the encryption algorithm with a 256 bit key size is:

FCS_CKM.1	Cryptographic key generation
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [256 bit] that meet the following: [FIPS ⁵² Pub 197].
FCS_CKM.4	Cryptographic key destruction
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [semiconductor memory state loss at power-down, semiconductor memory zeroization at power-up] that meets the following: [None].
FCS_COP.1	Cryptographic operation
FCS_COP.1.1	The TSF shall perform [encryption and decryption] on User Data stored on nonvolatile storage in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256 bit] that meet the following: [None].

Note that [None] is used as the selection in both FCS_CKM.4 and FCS_COP.1 to indicate that no standards for cryptographic key destruction or cryptographic operation, respectively; are deemed applicable to cryptographic key destruction and cryptographic operation.

In some cases, the choice of country Scheme used to certify the TOE can be a factor in what is specified in the FCS SFRs. Some Schemes have scheme-specific cryptographic requirements that should be reflected in the SFRs. For example, the US Scheme requires that any cryptography that is used in a TOE being certified must be FIPS Pub 140-2 certified cryptography; that standard would have to be included in the list of standards applicable to cryptographic key generation, destruction and

⁵² FIPS – Federal Information Processing Standards

operation in an ST for a TOE being certified in the US. Other country Schemes may have similar requirements that the ST Author should take into account.

Concerning actions to be taken in case the TOE detects an integrity error when reading data that has been previously stored with confidentiality and integrity protection, the ST Author should keep in mind that the NVS SFR Package covers nonvolatile storage that is designed to be removed from the TOE and then, by implication, returned and reinstalled in the TOE. So PP APPLICATION NOTE 108 is really stating that the ST Author should make sure that any relevant SFRs (and possibly security objectives) should be added to indicate how the TOE protects the confidentiality and integrity of data stored in nonvolatile storage when the nonvolatile storage (and by extension the data) is outside of the TOE.

The ST Author should consult appropriate experts to determine exactly which SFR is appropriate for the particular TOE in question.

- b). **PP APPLICATION NOTE 109** (FTP_CIP_EXP.1) – Indicates that FTP_CIP_EXP.1 is a principal SFR for fulfilling the listed security objectives.

Additional Guidance: No additional guidance is deemed necessary.

6.9.10 SMI SFR Package PP Application Notes

1. Class FDP: User data protection

- a). **PP APPLICATION NOTE 110** (FAU_GEN.1) — Suggests what the ST Author should do when, for a specified Common Criteria defined audit level (minimum, basic, or detailed) there are conflicts among the SFRs and the requirements listed in the applicable Audit data requirements table.

Additional Guidance: This PP APPLICATION NOTE is equivalent to the corresponding PP APPLICATION NOTE for the Common FAU_GEN.1 SFR. See 6.9.2, Item 1.c for guidance on what this PP APPLICATION NOTE implies.

- b). **PP APPLICATION NOTE 111** (FAU_GEN.1) – Discusses FPT_STM dependency of FAU_GEN.1.

Additional Guidance: The dependency of FAU_GEN.1 on FPT_STM.1 is addressed in this case by the FAU_GEN.1 SFR documented in Clause 10.1 of the applicable PP from the IEEE Std 2600 Series of Protection Profiles.

- c). **PP APPLICATION NOTE 112** (FAU_GEN.1) – Indicates that FAU_GEN.1 is a principal SFR for fulfilling the listed security objective and a dependency of the listed SFR.

Additional Guidance: No additional guidance is deemed necessary.

- d). **PP APPLICATION NOTE 113** (FAU_GEN.1) – Indicates that FAU_GEN.1 performs audit functions for the indicated SFRs.

Additional Guidance: No additional guidance is deemed necessary.

2. Class FPT: Protection of the TSF

- a). **PP APPLICATION NOTE 114** (FPT_FDI_EXP.1) — PP APPLICATION NOTE 114 as stated in IEEE Std 2600.1 is incorrect. The correct wording for PP APPLICATION NOTE 114, which can be found in 13.1, Item #4, provides guidance on when the FMT_SMF.1 and FMT_SMR.1 SFRs need to be employed in support of the FPT_FDI_EXP.1 SFR.

PP APPLICATION NOTE 115 (FPT_FDI_EXP.1) — Discusses how the FMT_SMF.1 SFR being a dependency of the FPT_FDI_EXP.1 SFR is addressed in the SMI SFR Package.

PP APPLICATION NOTE 116 (FPT_FDI_EXP.1) — Discusses how the FMT_SMR.1 SFR being a dependency of the FPT_FDI_EXP.1 SFR is addressed in the SMI SFR Package.

Additional Guidance: PP APPLICATION NOTE 114 refers to defining roles that are permitted to allow forwarding of data without further processing by the TSF. The actual text of the FPT_FDI_EXP.1 SFR in the four PPs does not directly deal with roles or security functions; rather it depends on the FMT_SMF.1 SFR as indicated in PP APPLICATION NOTES 115 and 116. The ST Author should note that in the case where forwarding without further processing is never allowed:

- There is no need for any type of Administrator role or function associated with allowing such forwarding
- There is no need to specify in the ST any SFRs associated with forwarding without further processing, because specifying an SFR in the ST here might imply that some type of active technical mechanism, rather than the TOE’s architectural design, exists in the TOE that prohibits this forwarding.

In those cases where forwarding of data without further processing by the TSF is allowed, the ST must clearly indicate such forwarding is under Administrator control and should add the appropriate flow control policy associated with this Administrator control.

An example of a flow control policy based on defining flow control SFRs would be:

FDP_IFC.1	Subset information flow control
FDP_IFC.1.1	The TSF shall enforce the [assignment: <i>Information Flow SFP</i>] on [assignment: <i>list of users/subjects, list of operations</i>].
FDP_IFF.1	Simple security attributes
FDP_IFF.1.1	The TSF shall enforce the [assignment: <i>Information Flow SFP</i>] based on the following types of subject and information security attributes: [assignment: <i>list of users/subjects and informations, with an attribute that permits the operation for each user/subject-information pair</i>].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: <i>list of users/subjects and informations, with an attribute value that permits the operation for each user/subject-information pair</i>]
FDP_IFF.1.3	The TSF shall enforce the [assignment: <i>additional information flow SFP rules</i>].
FDP_IFF.1.4	The TSF shall provide the following: [assignment: <i>list of additional SFP capabilities</i>].
FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: [assignment: <i>rules, based on security attributes, that explicitly authorise information flows</i>].
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: [assignment: <i>rules, based on security attributes, that explicitly deny information flows</i>].

If, for example, it were desired that the ST allow bridging between a wired LAN adapter and a Wi-Fi⁵³ adapter the FDP_IFC.1 and FDP_IFF.1 SFRs would look something like:

FDP_IFC.1	Subset information flow control
FDP_IFC.1.1	The TSF shall enforce the [Wired-Wi-Fi® Bridging IFC SFP] on [Wired Users and Wi-Fi® Users, any information, any communication].

⁵³ The Wi-Fi® trademark is owned by the Wi-Fi Alliance [C5]

FDP_IFF.1	Simple security attributes
FDP_IFF.1.1	The TSF shall enforce the [Wired-Wi-Fi® Bridging IFC SFP] based on the following types of subject and information security attributes: [Wired Users and Wi-Fi® Users, any information, BridgeEnabled attribute].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [Wired Users and Wi-Fi® Users, any information, BridgeEnabled attribute has the value “True”].
FDP_IFF.1.3	The TSF shall enforce the [assignment: <i>additional information flow SFP rules</i>].
FDP_IFF.1.4	The TSF shall provide the following: [assignment: <i>list of additional SFP capabilities</i>].
FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: [assignment: <i>rules, based on security attributes, that explicitly authorise information flows</i>].
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: [assignment: <i>rules, based on security attributes, that explicitly deny information flows</i>].

Any rules governing the BridgeEnabled attribute in terms of what operations can be done and which roles can do those operations would have to be defined in the FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 SFRs, and the applicable roles would have to be defined in the FMT_SMR.1 SFR.

- b). **PP APPLICATION NOTE 117** (FPT_FDI_EXP.1) – Indicates that FPT_FDI_EXP.1 is a principal SFR for fulfilling the listed security objective.

Additional Guidance: No additional guidance is deemed necessary.

3. Class FTP: Trusted paths/channels

PP APPLICATION NOTE 118 (FTP_ITC.1) – Indicates that FTP_ITC.1 is a principal SFR for fulfilling the listed security objectives.

Additional Guidance: No additional guidance is deemed necessary.

6.10 Security Assurance Requirements (SARs) Guidance

ISO/IEC TR 15446 [B7], Section 6.3 provides good guidance on how to determine what Evaluation Assurance Level (EAL) and SARs to use for a given TOE. Typically, certification of hardcopy devices has been at either EAL 2 or EAL 3.

However, there are two factors that are not mentioned in ISO/IEC TR 15446 but are equally important in making the decision as to what EAL to certify a hardcopy device:

1. The EAL at which competitor products are being certified.
2. Any policies or requirements the Common Criteria Scheme the product will be certified in that suggest or mandate an EAL.

Make sure that these two factors are taken into consideration when the ST Author determines at what EAL to certify a product.

Another consideration for the ST Author is to determine whether to certify the product at an extended EAL, meaning that additional SARs not required by Common Criteria Part 3 [B4] for the EAL chosen are included in the certification. That choice becomes a combination of a business and a technical decision. The “business” part of the decision relates to what other competitors are doing – if they are certifying with one of the Flaw remediation (ALC_FLR) SAR components (which are not required at EALs 1-4) then you probably should also. The “technical” part of the decision is whether you can meet the requirements of the extended SAR. Like the choice of EAL, the choice of any extended components should be made on a case-by-case basis.

Three of the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles are Part 3 extended, by inclusion of one of the three components from the ALC_FLR (Flaw Remediation) Assurance Class described in Common Criteria Part 3 [B4] Section 14.5 – specifically, ALC_FLR.2, Flaw reporting procedures for IEEE Std 2600.1 [B8] and IEEE Std 2600.2 [B9] and ALC_FLR.1, Basic flaw remediation for IEEE Std 2600.3 [B10]. It was the intent of the authors of the IEEE Std 2600 Series of Protection Profiles that the applicable ALC_FLR assurance component in the case of these three PPs applies only to any security flaws that are found in the software or firmware included within the TOE boundary. Also, in the case of ALC_FLR.2 for IEEE Std 2600.1 and IEEE Std 2600.2 this SAR requires that a procedure for addressing security flaws and reporting their resolution back to TOE users be provided; however, this procedure can be completely manual and does not have to be automated in any way.

6.11 Additional ST Author Guidance

This subclause contains additional guidance ST Authors should be aware of that does not fit into any of the above categories.

1. In the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles the descriptions of the FAX and DSR SFR Packages state that each package may be used for specifying roles, mechanisms or rules for authorizing users to access documents. The two SFR packages, however, differ in their implementation of this and the ST Author should be aware of this difference. In the case of the DSR SFR package the intent is to let a user store a document and retain control over that document while still granting ‘read’ and possible ‘modify’ permissions to other users. In that way the ST Author can handle the instance where documents may be stored by a user in some type of volatile or nonvolatile memory in the TOE where they can be accessed by another application for some type of processing; this other application can be thought of as the other user in this case. That is why the DSR Access Control SFP table is written to deny read access to anyone except the document “owner” unless such access is authorized via another role or mechanism. The permission of this other application to access the stored document by the user constitutes the authorization in this instance.

Contrast this with the FAX DSR Package where if a Fax Administrator transfers control of an incoming fax document to another user, ownership of that incoming Fax document transfers from the Fax Administrator to this other user. That is why the Fax Access Control SFP is written to not include the case where read access is authorized via another role or mechanism – only the current owner of an incoming Fax document can read an incoming Fax document.

2. As indicated in 4.2.1.4 and 6.3, the intent of the IEEE Std 2600 Series of Protection Profiles is to require vendors to evaluate all product functionality that is identified in clause 12.3 of each PP if such functionality is present in the end product. For example, if the product has a fax interface, then the Fax SFR package should be included in the product's ST whether or not the Fax interface can be disabled by an administrator. Other functionality, as long as that functionality is not SFR-supporting (as defined in CC Part 3 [B4], Chapter 12.2), can be excluded from evaluation if it is disabled in the evaluated configuration.

Take the case where the end product has a USB flash memory interface into which a user can insert a USB flash drive to perform some kind of document operations. If that were the case, the USB flash memory interface would be considered to be “other functionality”. In many end products the USB flash memory interface is disabled to prevent someone from uploading unauthorized software into the device. Being “other functionality”, the USB flash memory interface could be excluded from the ST as long as it is disabled in the evaluated configuration.

7 IEEE STD 2600 SERIES OF PROTECTION PROFILES – CUSTOMER USAGE GUIDELINES

7.1 Introduction

This clause provides some detailed guidance from the perspective of a customer who wants to purchase a product that has been or is in the process of being certified against a PP selected from the IEEE Std 2600 Series of Protection Profiles. This guidance also discusses what Common Criteria certification can mean to a security-conscious customer and on proper use of Common Criteria certifications.

The general conventions that applied to Clause 5 apply to this clause also.

7.2 What Common Criteria Certification Means

The Common Criteria provides a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products. It addresses protection of assets from unauthorized disclosure, modification, or loss of use.

For a CC evaluation, the maker of an IT product describes security functions that the product claims to perform in the Security Target. A CC certification, along with the Security Target used in the CC evaluation, tells potential consumers of an IT product that the product was found to satisfactorily perform the security functions described in the Security Target. It also lets them know that the assurance measures applied to the product were evaluated and determined to meet CC requirements. This may help consumers to determine whether the IT product fulfills their security needs.

A Security Target may claim conformance to a Protection Profile. A Protection Profile is a high-level expression of desired security properties (i.e., security environment, security objectives, and security requirements). Consumers can specify their security requirements by selecting or creating a Protection Profile.

Purchasing a Common Criteria certified product provides a level of confidence to customers that the product being purchased has met the standards of an internationally recognized security certification. It should not be interpreted to mean that there are no security vulnerabilities in the products purchased, though efforts are taken in the certification process to ensure that as many vulnerabilities as possible are fixed.

When considering the purchase of products that have been Common Criteria certified, it is important to remember that comparable products from different manufacturers may not have certified the same security features. One of the purposes of Protection Profiles is to specify a common set of security features that must be Common Criteria certified in order to claim a defined level of security conformance. Common Criteria certification based on conformance with a Protection Profile helps put manufacturers of similar products at the same level, so that customers can compare products more effectively from a security perspective.

7.2.1 Common Criteria As It Relates to HCDs

If HCDs from multiple manufacturers are evaluated based on Security Targets that claim conformance to one or more of the Protection Profiles from the IEEE Std 2600 Series of Protection Profiles, then it becomes easier for a customer to compare HCDs based on evaluation results.

It is also important to note here that claiming conformance to one of the PPs from the IEEE Std 2600 Series of Protection Profiles is based on demonstrable conformance (see 6.3). This means that each HCD

manufacturer must provide adequate documentation for an HCD that is to be Common Criteria certified so that the ST Author can prove in the ST that the HCD aligns with the required security features. However, this also means that different HCD manufacturers can use different approaches or methodologies to show conformance to the SFRs in the applicable PP from the IEEE Std 2600 Series of Protection Profiles.

7.3 Identifying the Appropriate Operational Environment

An organization’s IT security needs depend on many factors, such as the value of its assets, the organizational impact of compromising those assets, the likelihood of a threat being carried out, various assumptions about the IT environment and about individuals in the organization, and externally mandated security requirements. By choosing a generalized environment that most closely matches a particular organization’s specific environment, the organization can identify the guidance and recommendations that are most applicable to its specific needs. Four Operational Environments (A, B, C, and D) are considered in IEEE Std 2600, and there are four Protection Profiles in the IEEE Std 2600 Series of Protection Profiles. Those four Operational Environments are summarized in Clause 3 of this document and described in more detail in IEEE Std 2600 [B1] Clause 4.

Operational Environment A has the highest security requirements of the four. Operational Environments B, C, and D have progressively less stringent security requirements. A product certified for any one of these environments can also be considered adequate for an environment with less stringent security requirements. If, for example, a product is certified for Operational Environment B, it is adequate for Operational Environments C and D as well, but it may not be adequate for Operational Environment A.

When choosing the most applicable environment to use as a guide for particular security needs, the reader should look beyond the simple description of the environment and instead consider both the totality of the Operational Environment and the value of the most valuable assets to be protected. The following table summarizes those factors for each environment.

Table 12. Factors Affecting Security

Effect on Security Requirements

Operational Environment	A	B	C	D
Element of Security				
Value of Asset	High	Moderate	Moderate – Low	Low
Physical Security	High	Moderate	Low	Low
Network Protection	High	Moderate	Moderate	Low
Laws and Regulations	High	Moderate – Low	Low	Low
Personnel Trust	High	Moderate	Low	Low

Because many security requirements can be considered environment-specific, it is important to match the intended product usage to the appropriate Operational Environment, its assets, and anticipated threats. This will serve as the basis for deciding which Protection Profile certification is the correct one for each customer.

It is important to note that “islands” or sub-sets of one Operational Environment may exist within the framework of larger Operational Environments. For example, a legal department or executive office may have more stringent security needs compared to an R&D engineer. In cases like these, it is important to balance the broader business need for certification based on the most prevalent Operational Environment, and compare that need to the pockets or islands of a particular Operational Environment.

Identifying security use cases and then assigning them to a particular Operational Environment is also a good way to determine which Operational Environment is most applicable to a particular business.

Here are some examples of how to choose an appropriate Operational Environment:

1. **Home Appliance Service Company** – This business typically has a network of computers to run their operation, which includes taking orders, dispatching trucks, general bookkeeping, and providing access to service documentation. Operational Environment B is the most applicable environment description. However, a few of the company’s routine functions involve private information such as credit card processing for customers and payroll and health insurance records for its employees. Systems that perform those functions are likely to be regulated by laws, and would therefore need to be considered as Operational Environment B with islands of Operational Environment A.
2. **Publicly-traded Pharmaceutical Manufacturer** – This business performs many functions that are regulated or involve highly valuable competitive information. For example, their bookkeeping is regulated by governance laws, their clinical trial data is regulated by privacy laws, and their research and patent data is so valued that its disclosure could result in the loss of significant future revenue. All of these activities would clearly require the precautions typical of Operational Environment A.
3. **Home User** – A typical home network often consists of two desktop computers, an HCD, which is connected via USB to one of the computers but its use is shared. Such a home network is often connected to the Internet by a combined DSL modem, firewall, and wireless access point. This environment is typical of Operational Environment D. However, one of the family members uses their laptop computer at home to connect to their employer’s corporate network so that they can work at home on product launch plans for the aforementioned pharmaceutical company. The laptop, the wireless connection, and the HCD and its host computer, would need to be able to operate as an Operational Environment A island within this typical Operational Environment D environment.

7.4 Configuring the Product

Note that a certified product does not necessarily achieve all of its security potential without appropriate configuration, installation, and setup. While this Guide cannot describe the appropriate procedures for all CC-certified HCD products, it should be stressed that vendor documentation must be followed to ensure proper levels of performance.

7.5 Understanding Product Compliance

Compliance with IEEE Std 2600 for a particular Operational Environment means that an HCD provides a level of security appropriate for that operational environment. Customers can look for HCDs that claim compliance in an operational environment comparable to their own. For a higher level of assurance, they can look for HCDs that are Common Criteria certified against a PP from the IEEE Std 2600 Series of Protection Profiles for the appropriate Operational Environment.

It should be cautioned here that Common Criteria certification is meant to apply to a known specific configuration of the HCD. This known configuration can either be the “out-of-box” HCD configuration, which is the typical situation, or in some cases to a different configuration that is not the “out-of-box” HCD configuration. If the HCD configuration to be certified is not the “out-of-box” configuration, then the HCD vendor has to provide clear directions that accompany the HCD as it is shipped “out-of-box” on how the certified HCD configuration is obtained from the “out-of-box” HCD configuration. Be aware, however, that if this known configuration is changed in any way the product security and the validity of the Common Criteria certification could be adversely affected.

It should be noted that a vendor can claim compliance without evaluation. If the vendor believes that its HCD meets the requirements of the IEEE Std 2600 in a particular operational environment, it can say that its product is “IEEE Std 2600 Compliant” in that environment. This gives some level of assurance that the product’s security features are appropriate and sufficient for the environment, and it may be useful for comparison of products.

To provide further assurance, a vendor can have a product evaluated against one of the IEEE Std 2600 Series of Protection Profiles by an accredited Common Criteria Testing Lab. If the product passes the evaluation, it is Common Criteria certified. This validates the vendor's compliance claim, providing a higher level of assurance that the HCD's security features are "IEEE Std 2600 compliant" in a particular environment. Thus, certification implies compliance but adds independent validation of the claim.

7.5.1 Specifying Certification Level in a Request for Proposal

Information on how to specify the certification level in a Request for Proposal will be provided here in a future version of this document.

7.6 Examples

Several examples on how to specify some of the SFRs that are part of the four Protection Profiles that comprise the IEEE Std 2600 Series of Protection Profiles have been included in the additional guidance provided for the various PP Application Notes in 6.9.

After a few HCD manufacturers create Security Targets against the four PPs that comprise the IEEE Std 2600 Series of Protection Profiles, additional examples of how the SFRs are actually worded in these STs will be included in this Clause as representative examples for other HCD Manufacturers and ST Authors to follow.

8 IEEE STD 2600 SERIES OF PROTECTION PROFILES FAQs

This clause provides a set of Frequently Asked Questions (FAQs) and answers about the content and use of the IEEE Std 2600 Series of Protection Profiles. The questions are organized by topic area for ease of use by readers of this guide.

8.1 General Interest Questions

1. **Question: What is the “packages” model used in the HCD Protection Profiles, and how do the packages fit together?**

Answer: There is a package of SFRs (Security Functional Requirements) for each of various common HCD functions:

- CPY (“Copy”) – This package covers the conversion of hardcopy input to hardcopy output.
- SCN (“Scan”) – This one covers the conversion of hardcopy input to digital output.
- FAX (“Fax”) – This covers the conversion of digital input to analog fax output and the conversion of analog fax input to digital output.
- PRT (“Print”) – This covers the conversion of digital input to hardcopy output.
- DSR (“Digital Storage & Retrieval”) – This covers the storage and retrieval of digital data.
- SMI (“Shared Medium Interface”) – This covers the transmission and receipt of data through an interface designed to allow the HCD to communicate with multiple users simultaneously.
- NVS (“Nonvolatile Storage”) – This covers the storage of data on nonvolatile storage media that is designed to be removable by authorized non-service personnel.

There are various other ways in which the functions corresponding with the SFR packages may interact to perform the tasks that an HCD is designed for. For example, when a user faxes a document, the operation typically involves a collaborative effort between the SCN and FAX functions. (If the document starts in hardcopy form, it is first converted to digital form by the scanner and then processed by the FAX functionality.) When a document is printed by a user, it may travel through a network (SMI) to get to the HCD, where it is then converted to hardcopy output by the PRT functionality.

2. **Question: Where can I find a list of threat descriptions that exist for HCDs?**

Answer: In IEEE Std 2600™-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security, Clause 6.

3. **Question: Why are some threats in IEEE Std 2600 not included in the PPs?**

Answer: IEEE Std 2600 was developed to define security requirements covering all aspects of security for manufacturers, users and IT professionals on the selection, installation, configuration and usage of HCDs. To cover all of this scope the standard addresses all the varied classes of potential threats that could apply to the installation, configuration and usage of HCDs.

The PPs, on the other hand, deal with defining security threats, objectives and requirements specifically needed to write STs for Common Criteria certification of HCDs and to write other conformant PPs. The CC limits what requirements, objectives and threats are covered in STs and PPs to those that meet certain criteria; this results in the set of threats covered in the PPs becoming a subset of the total set of threats covered in the IEEE Std 2600. That is why some threats in the IEEE Std 2600 are not included in the PPs.

4. **Question: Where can I find a general description of PPs and STs?**

Answer: ISO/IEC⁵⁴ TR 15446, Information Technology – Security techniques - Guide for the production of Protection Profiles and Security Targets, First Edition, 2004-07-01 (<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>) [B7] is a good reference for helping to create a Protection Profile and/or Security Target.

5. **Question: If I have a question about a PP from the IEEE Std 2600 series of Protection Profiles, whom can I ask?**

Answer: A Distribution List/e-mail address exists for each PP in the IEEE Std 2600 Series of Protection Profiles – Stds-2600-1@ieee.org for IEEE Std 2600.1 [B8], Stds-2600-2@ieee.org for IEEE Std 2600.2 [B8], Stds-2600-3@ieee.org for IEEE Std 2600.3 [B10] and Stds-2600-4@ieee.org for IEEE Std 2600.4 [B11] - for questions about any of the PPs. A point of contact will forward the question to the appropriate person or group who can address the question.

If the question still isn't answered, for questions about the Evaluation Lab's report contact the Evaluation Lab listed in the Validation Report and for questions about the Validation Report itself contact the applicable Scheme.

Lastly you can submit the question to your applicable CCRA member⁵⁵, or more specifically, to one of the Certificate Authorizing Schemes to address. Only contact the CCRA Member of Scheme if the question involves general issues concerning the certification of an IT product, its international recognition, or technical matters related to the Common Criteria.

6. **Question: Where (and to whom) should we send questions or comments about this guide?**

Answer: Use the same Distribution List/e-mail address that exists for each PP in the IEEE Std 2600 Series of Protection Profiles – Stds-2600-1@ieee.org for IEEE Std 2600.1 [B8], Stds-2600-2@ieee.org for IEEE Std 2600.2 [B8], Stds-2600-3@ieee.org for IEEE Std 2600.3 [B10] and Stds-2600-4@ieee.org for IEEE Std 2600.4 [B11] - for questions or comments about this guide.

If the question or comment does not concern a specific PP in the IEEE Std 2600 Series of Protection Profiles, use the Stds-2600-1@ieee.org Distribution List/e-mail address for IEEE Std 2600.1. A point of contact will forward the question to the appropriate person or group who can address the question.

7. **Question: If there is an inconsistency or issue with a PP, how would that be resolved?**

Answer: Officially, the Scheme that performed Common Criteria certification of the two PPs from the IEEE 2600 Series of Protection Profiles (the US Scheme for IEEE Std 2600.1 [B8] and the German Scheme for IEEE Std 2600.2 [B8]) is responsible to resolve inconsistencies or issues with the two certified PPs. However, since all the PPs in the IEEE Std 2600 Series of Protection Profiles are IEEE Standards, it also becomes a problem for the IEEE to resolve. For IEEE Std 2600.1 and IEEE Std 2600.2 first go to the applicable Scheme to get resolution and then to the IEEE; for IEEE Std 2600.3 [B10] and IEEE Std 2600.4 [B11] any such inconsistencies or issues should be taken directly to the IEEE to resolve.

Another way ST Authors can deal with problems in one of the PPs is to make a note in the ST of which part of the applicable PP is not being followed and the rationale as to why it is not being followed. This could lead to the applicable Scheme issuing an interpretation that all STs must address the same issue.

8. **Question: Where can I find the full set of PPs?**

Answer: The IEEE Std 2600 Series of Protection Profiles will be available from the IEEE (see <http://ieeexplore.ieee.org/xpl/standards.jsp>). In addition, IEEE Std 2600.1 [B8] and IEEE Std 2600.2 [B8] will be available via the Common Criteria portal at URL <http://www.commoncriteriaportal.org/pp.html>.

⁵⁴ ISO – International Organization for Standardization; IEC – International Electrotechnical Commission

⁵⁵ The list of CCRA members and Schemes, including contacts, can be found at URL <http://www.commoncriteriaportal.org/members.html>.

9. **Question: Where (and to whom) should we send questions on PP text?**

Answer: Questions on PP text can be sent to the Secretary, IEEE-SA Standards Board, 445 Hoes Lane, Piscataway NJ 08854 USA.

10. **Question: Where can I find a list of certified and/or compliant products?**

Answer: The list of all Common Criteria certified products can be found in the Common Criteria Portal Certified Product List website at URL <http://www.commoncriteriaportal.org/products.html>.

Individual country Schemes may also maintain their own websites containing a list of Common Criteria certified products that have been certified under their specific country Schemes. For example:

- a). For products certified in the United States, see the NIAP⁵⁶ Common Criteria Evaluation and Validation Scheme (CCEVS) Validated Product List at <http://www.niap-ccevs.org/cc-scheme/vpl/>
- b). For products certified under the German Scheme see the BSI⁵⁷ Certification Report website at <http://www.bsi.bund.de/zertifiz/zert/reporte.htm>.
- c). For products certified under the Japanese Scheme see the IPA⁵⁸ Certified/Validated Products List at http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/certfy_list.html.

A complete list of all the country Schemes can be found on the Common Criteria portal at URL <http://www.commoncriteriaportal.org/schemes.html>.

8.2 Questions For ST Authors

1. **Question: Where can I find reference examples of STs written against one of the IEEE Std 2600 Series of Protection Profiles?**

Answer: Examples of sections taken from actual STs written against one of the IEEE 2600 Series of Protection Profiles are included in Clause 7.6 of this document.

2. **Question: If I want to include PIN printing in my HCD, which SFR packages should I include in the ST?**

Answer: In Operational Environments A and B, an HCD that implements either the FAX, DSR (“Digital Storage & Retrieval”) or PRT (“Print”) functions must provide some method of authentication before releasing jobs to hardcopy output for the applicable functions implemented. “PIN Printing” is one mechanism for satisfying this authentication requirement. Therefore, the Security Target for an HCD conforming to either IEEE Std 2600.1 [B8] or IEEE Std 2600.2 [B8] that provides PIN Printing that either the Fax, DSR or Print functions must include the corresponding SFR package for that function.

3. **Question: What does conformance to one of the four Protection Profiles from the IEEE Std 2600 Series of Protection Profiles mean and how can I demonstrate it?**

Answer: Per Common Criteria Part 1 [B2], a Common Criteria certification is an independent inspection by the Scheme in question of the results of a TOE evaluation by an accredited lab; the TOE evaluation is a review of the TOE and its associated documentation to make sure that the statement in all the Security Assurance Requirements (SARs) stated in the ST have been met, which in turn means that the TOE meets the SFRs as stated in the ST.

⁵⁶ NIAP (National Information Assurance Partnership) is the United States Common Criteria Authorization Scheme

⁵⁷ BSI (Bundesamt für Sicherheit in der Informationstechnik) is the German Common Criteria Authorization Scheme

⁵⁸ IPA (Information Security Certification Office Information Technology Promotion Agency) is the Japanese Common Criteria Authorization Scheme

Common Criteria Part 1 Annex D defines two levels of conformance – strict compliance (where the ST includes verbatim, as a minimum, all the statements that are in the PP) and demonstrable conformance (where the ST may contain different statements from the PP but provides a rationale demonstrating how the statements in the ST are “equivalent to or more restrictive than” the corresponding statements in the PP). The four PPs comprising the IEEE Std 2600 Series of Protection Profiles all require demonstrable conformance. This means that for these four PPs conformance means that the security problem definition, SFRs and security objectives included in the ST must be equivalent to or more restrictive than the corresponding security problem definition, SFRs and security objectives in the PP. This allows for ST Authors to provide alternate ways of meeting the PP SFRs depending on the TOE.

Conformance will be demonstrated through completion of the Common Criteria certification process where the evaluation lab will independently verify the SARs as stated in the ST have been met, and thus by implication that the TOE meets the SFRs stated in the ST that conform to their counterparts in the PP.

8.3 Questions for HCD Vendors

Question: How do I select which operational environment to have a product certified for (i.e., Which PP should I certify against?)

Answer: Clause 5.2 of this document provides several criteria a vendor can use to determine what operational environment (and thus which PP) to have a product certified under.

8.4 Questions for Common Criteria Evaluators

Question: Once any of the four Protection Profiles becomes certified, must an HCD that is to be certified against the applicable Operational Environment conform to the certified Protection Profile?

Answer: In general, an HCD that is to be certified against the applicable Operational Environment does not have to conform to the applicable certified PP, but there may be differences depending on the customer and requirements of the Scheme the HCD is to be certified in. Different customers may have different requirements as to what certification an HCD to be procured must meet, and this may include a requirement that the TOE conform to one an available PP for the TOE in question.

Although the Common Criteria Recognition Agreement (CCRA) states that a Protection Profile certified in one Scheme will be recognized by all other Schemes, each Scheme has a different policy about recognizing Protection Profiles certified in another Scheme. For example, the US Scheme requires that if there is a Government PP available for the TOE being certified the TOE must conform to that PP. In our case IEEE Std 2600.1 [B8] is being certified under the US Scheme as a Government PP, so any HCD certified in the US Scheme will have to conform to IEEE Std 2600.1; the same scenario will likely be true with an HCD to be certified using the German Scheme – it would have to conform to IEEE Std 2600.2 [B9] that is being certified under the German Scheme. However, the Australian Scheme may not require that an HCD certified under that Scheme conform to either IEEE Std 2600.1 or IEEE Std 2600.2.

It is best to check with Scheme the HCD is being certified under to ascertain what its policy is towards required conformance with the applicable Protection Profile.⁵⁹

⁵⁹ Many schemes have a policy, for example, that conformance to a Protection Profile is required for Protection Profiles that have been certified by that scheme; conformance to any other PPs is at the discretion of the sponsor but is not required.

9 Glossary (Informative)

For the purposes of this document, the following terms and definitions apply. Note that IEEE Std 100, *The Authoritative Dictionary of IEEE Standards, Seventh Edition*, and Annex A in normative references [B8] – [B11] should be referenced for terms not defined in this clause.

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 SFP. Administrators may possess special privileges that provide capabilities to override portions of the SFP.

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

Component: the smallest selectable set of elements on which requirements may be based.

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

Evaluation Scheme: the administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

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 products), MFDs (multifunction devices), “all-in-ones”, and other similar products. See also: multifunction device.

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.

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.

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

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.

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.

Package: a named set of either functional or assurance requirements.

Protection Profile (PP): an implementation-independent statement of security needs for a TOE type.

Security Assurance Requirement (SAR): a description of how assurance is to be gained that the TOE meets the SFRs in a standardized language to provide an exact description of what is to be evaluated.

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 that 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.

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 guidance⁶⁰.

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

TSF Confidential 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.

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

⁶⁰ Guidance in this context is defined as documentation that describes the delivery, preparation, operation, management and/or use of the TOE.

10 Acronyms (Informative)

Table 13. Acronyms

Acronym	Definition
BSI	Bondsman für Sicherheit in der Informationstechnik
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Method
C/IA	IEEE Computer Society Information Assurance
CIM	Consistency Instruction Manual
CPY	copy
DSR	document storage and retrieval
EAL	evaluation assurance level
ECD	extended component definition
FAQ	frequently asked question
FAX	facsimile
FIPS	Federal Information Processing Standards
HCD	hardcopy device
HIPAA	Health Insurance Portability and Accountability Act
HomePNA™	home phoneline networking alliance
I&A	identification and authentication
IASC	IEEE Information Assurance Standards Committee
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE-SA	IEEE Standards Association
IPA	Information Security Certification Office Information Technology Promotion Agency
IPSec	Internet Protocol Security
IrDA	Infrared Data Association
ISO	International Organization for Standardization
IT	information technology
MFD	multifunction device
HCD	multifunction product / peripheral / printer
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIC	network interface card
NIST	National Institute of Standards and Technology
NTP	network time protocol
NVS	nonvolatile storage
OSP	organizational security policy
PAR	Project Authorization Request
PCI DSS	Payment Card Industry Data Security Standard
PII	personally identifiable information
PIN	personal identification number
PP	protection profile
PPM	pages per minute
PRT	print
SA	system administrator
SAR	security assurance requirement
SCADA	supervisory control and data acquisition

Acronym	Definition
SCN	scan
SFP	security function policy
SFR	security functional requirement
SIG	special interest group
SMB	server message block
SMI	shared-medium interface
SNMP	Simple Network Management Protocol
SOHO	small office – home office
SSL	Secure Sockets Layer
ST	security target
Std	standard
TLS	Transport Layer Security
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TOE security functionality interface
TSP	TOE security policy
USB	universal serial bus

11 Informative References

- [C1]. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, 2001 May 25, available from <http://www.itl.nist.gov/fipspubs/by-num.htm>.
- [C2]. FIPS PUB 197, Advanced Encryption Standard (AES), 2001 November 26, available from <http://www.itl.nist.gov/fipspubs/by-num.htm>.
- [C3]. IEEE Std 1284-2000, IEEE Standard Signaling Method for a Bidirectional Parallel Peripheral Interface for Personal Computers
- [C4]. ISO/IEC 17799:2000: Code of Practice for Information Security Management
- [C5]. Wi-Fi Alliance, <http://www.wi-fi.org>
- [C6]. Bluetooth Special Interest Group, <https://www.bluetooth.org>

12 International Perspectives

Twenty-six countries now participate in the international Common Criteria program. Thirteen of the countries issue certificates that are recognized up to EAL4 by the other participating countries. While all countries involved use the same Common Criteria standard several of the leading players in the program have developed supplemental policies and local (national) requirements. An example is a requirement that if encryption is required the encryption implementation might have to be independently evaluated and certified as being acceptable using a different certification process in that country. Another example is a policy that requires that security audit trails be included as a required component of every security solution. These issues are not specifically addressed in the IEEE documents.

NIAP also posts a relatively large number of documents named Policy Letters. NIAP refers to its Policy Letters as guidance documents but compliance may be necessary. Nineteen Policy Letters were posted as of Oct 2008. Posted policies address issues such as limiting evaluations to Security Targets that NIAP judges to be “reasonable” (as opposed to frivolous) targets of evaluation. If FIPS certification in the US or Canada has not been secured by the product developer for their encryption implementation the vendor CC documentation must indicate that the encryption implemented has not been verified.

CC Schemes with unique add-ons may require that they be met before a certificate from that country is issued. Most CC Schemes, if not all, will recognize foreign certificates that do not specifically comply with their local policies. Local evaluations may require full compliance with local policies however so they should be carefully researched on the web sites of the countries where the evaluations will be done.

As indicated in 6.2 it was the intent of the authors of the IEEE 2600 Series of Protection Profiles that the TOE in all cases would be the entire HCD. The ST authors should be reminded, however, that each country Scheme might have different rules or policies governing what the allowable boundaries of a TOE can be. The ST Author must make sure that any such TOE boundary rules or policies for the country Scheme in which the HCD is being certified are followed when defining the TOE in the ST. The ST Author must also keep in mind when defining the TOE boundaries that any security-relevant component addressed in the applicable PP selected from the IEEE 2600 Series of Protection Profiles or in the ST itself must be included in the TOE boundary. For example, if the HCD includes removable nonvolatile storage such as a removable hard disk drive, that removable nonvolatile storage must be included within the TOE boundary.

13 IEEE 2600 Series of Protection Profiles Errata

This section will contain a list of errors found in any of the four IEEE Std 2600 Protection Profiles along with the associated corrected text once the Protection Profiles have been Common Criteria certified or have been approved by the IEEE Standards Board.

This list will be maintained “evergreen” so it will change as errors are found and are corrected in a published version of the applicable Protection Profile.

13.1 IEEE Std 2600.1 Errata

The errata listed below exist in IEEE Std 2600.1 [B8].

1. Clause 3.2, Page 3:

Discussion: The overall PP, which is designated as "IEEE Std 2600.1", includes both the common PP as described in Clauses 3 – 11 and the SFR packages as described in Clauses 12 – 19. A way was needed to designate just the common PP was needed. The decision was to use the convention "2600.1-PP" whenever it was desired to express conformance to just the common PP and not the overall PP. This convention, however, was not used in Clause 3.2 by mistake.

Change: The **Title** in Clause 3.2, Page 32, first line should read:

Title: 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A

2. Clause 8.4, Page 15, Table 14:

Discussion: In the listing of the sufficiency of the A.ADMIN.TRUST assumption in Table 14 on page 15 there is a reference in the ‘Objectives and Rationale’ column to the OE.ADMIN.TRUST Security Objective of the non-IT environment discussed in Clause 8.3 on Page 12. This is a typographical error – the name of this particular Security Objective was previously changed to OE.ADMIN.TRUSTED, but that change was not carried through into Table 14.

Change: The row for the A.ADMIN.TRUST assumption in Table 14 should read:

Threats, policies, and assumptions	Summary	Objectives and rationale
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.

3. Clause 10.1, Page 18:

Discussion: There is a misspelling in the wording of the last sentence of PP APPLICATION NOTE 9 on page 18.

Change: PP APPLICATION NOTE 9 should read:

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 not supersede the requirements and recommendations in this clause.

4. Clause 10.1, Page 19, Table 15:

Discussion: The auditable event listing for the FTA_SSL.3 SFR in Page 19, Table 15 - “Locking of an interactive session by the session locking mechanism” - is actually the auditable event for the FTA_SSL.2 SFR. The proper auditable event for the FTA_SSL.3 SFR is “Termination of an interactive session by the session locking mechanism”.

Change: Table 15 should read:

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
Termination of an interactive session by the session locking mechanism	FTA_SSL.3	Minimum	None required

See the additional guidance in 6.9.2, Item 1.c for more about the Audit Levels listed in Table 15 and what they will mean to the ST Author.

5. Clause 10.1, Page 19:

Discussion: The two lines on page 19 after Table 16 should have been marked as separate PP APPLICATION NOTES, but were not.

Change: The two lines on page 19 after Table 16 should read:

PP APPLICATION NOTE 12.1. FAU_GEN.1 is a principal SFR to fulfill O.AUDIT.LOGGED and is a dependency of FAU_GEN.2.

PP APPLICATION NOTE 12.2. 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.

6. Clause 10.4, Page 20

Discussion: In Table 17, Common Access Control SFP, the 'Attribute' column for both the D.DOC and D.FUNC objects currently says 'attributes from Table 22; see PP APPLICATION NOTE 15". However, Table 22 is the SFR Package functions table in this standard; the reference in Table 17 in both cases should instead be to Table 23, which is the SFR Package attributes table in this standard.

Change: Table 17 --Common Access Control SFP in Clause 10.4, page 20 should read:

Table 17 —Common Access Control SFP

Object	Attribute	Operation(s)	Subject	Access control rule
D.DOC	attributes from Table 23; see PP APPLICATION NOTE 15	Delete	U.NORMAL	Denied, except for his/her own documents
D.FUNC	attributes from Table 23; see PP APPLICATION NOTE 15	Modify; Delete	U.NORMAL	Denied, except for his/her own function data

7. Clause 10.4, Page 22:

Discussion: There is a minor error in the typographical notation in the FDP_ACF.1.1(b) SFR component. Where it says "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]**", the intention is that "users and" is a refinement that is separate from the assignment that follows. The correct notation is "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]**".

Change: FDP_ACF.1.1(b) SFR component definition in Clause 10.4, page 22 should read:

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*].

8. Clause 10.6, Page 27:

Discussion: The FMT_MTD.1 SFR should have been iterated as a component. Instead, the elements within the FMT_MTD.1 SFR were iterated within FMT_MTD.1. ST Authors may correctly iterate the components, but in any case evaluators should be aware that the intention was to iterate the component and should allow conforming STs to either correct or repeat this structural iteration error.

No change to the FMT_MTD.1 SFR definition in Clause 10.6, Page 27 is required at this time. A possible suggestion on how this SFR can be iterated by the ST Author is included in clause 6.6.9 of this document.

9. Clause 13.2, Page 36:

Discussion: The definition of the FDP_ACC.1.1 SFR component in Clause 13.2 does not completely follow the Notational Conventions listed in Clause 1.4, Page 2.

Change: The FDP_ACC.1.1 SFR component in Clause 13.2 should read:

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.**

10. Clause 14.2, Page 38:

Discussion: The definition of the FDP_ACC.1.1 SFR component in Clause 14.2 does not completely follow the Notational Conventions listed in Clause 1.4, Page 2.

Change: The FDP_ACC.1.1 SFR component in Clause 14.2 should read:

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.**

11. Clause 16.2, Pages 41 and 42:

Discussion: There is a typographical error in the wording of the last sentence of PP APPLICATION NOTE 93 on page 42. This PP APPLICATION NOTE refers to “User Documents” when it should correctly refer to “User Document Data”.

Change: PP APPLICATION NOTE 93 should read:

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 Document Data and User Function Data associated with such documents.

12. Clause 16.2, Page 42:

Discussion: The definition of the FDP_ACC.1.1 SFR component in Clause 16.2 does not completely follow the Notational Conventions listed in Clause 1.4, Page 2.

Change: The FDP_ACC.1.1 SFR component in Clause 16.2 should read:

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.**

13. Clause 19.3, Page 48:

Discussion: PP APPLICATION NOTE 114 is incorrectly worded. An earlier draft of the FPT_FDI_EXP.1 SFR included a requirement to specify an authorized role, and PP APPLICATION NOTE 114 referred to that requirement. When that requirement was eventually removed (deferring to dependencies on FMT_SMR.1 and FMT_SMF.1), PP APPLICATION NOTE 114 should have been reworded so that it referred to the dependencies and not to FPT_FDI_EXP.1 itself.

Change: PP APPLICATION NOTE 114 should read:

PP APPLICATION NOTE 114. The ST Author may use FMT_SMF.1 and FMT_SMR.1 to specify the management function and authorized role for allowing data to be forwarded without further processing by the TSF from an external interface to a shared-medium interface. If such forwarding is never allowed by the TOE, then FMT_SMF.1 and FMT_SMR.1 do not need to be employed in support of this FPT_FDI_EXP.1.

14. Front matter, Page v:

Discussion: Under the heading "Patents", there are several instances in which the standard is referred to as a "draft standard". It is an approved standard, not a draft standard.

Change: In each instance, "draft standard" should be changed to "standard"

13.2 IEEE Std 2600.2 Errata

The following errata exists in IEEE Std 2600.2 [B9]:

1. Clause 10.6, Page 28:

Discussion: The FMT_MTD.1 SFR should have been iterated as a component. Instead, the elements within the FMT_MTD.1 SFR were iterated within FMT_MTD.1. ST Authors may correctly iterate the components, but in any case evaluators should be aware that the intention was to iterate the component and should allow conforming STs to either correct or repeat this structural iteration error.

No change to the FMT_MTD.1 SFR definition in Clause 10.6, Page 28 is required at this time. A possible suggestion on how this SFR can be iterated by the ST Author is included in clause 6.6.9 of this document.

2. Clause 16.2, Page 43:

Discussion: There is a typographical error in the wording of the last sentence of PP APPLICATION NOTE 94 on page 42. This PP APPLICATION NOTE refers to "User Documents" when it should correctly refer to "User Document Data".

Change: PP APPLICATION NOTE 94 should read:

PP APPLICATION NOTE 94. 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 Document Data and User Function Data associated with such documents.

3. Clause 19.3, Page 50:

Discussion: PP APPLICATION NOTE 115 is incorrectly worded. An earlier draft of the FPT_FDI_EXP.1 SFR included a requirement to specify an authorized role, and PP APPLICATION NOTE 115 referred to that requirement. When that requirement was eventually removed (deferring to dependencies on FMT_SMR.1 and FMT_SMF.1), PP APPLICATION NOTE 115 should have been reworded so that it referred to the dependencies and not to FPT_FDI_EXP.1 itself.

Change: PP APPLICATION NOTE 115 should read:

PP APPLICATION NOTE 115. The ST Author may use FMT_SMF.1 and FMT_SMR.1 to specify the management function and authorized role for allowing data to be forwarded without further processing by the TSF from an external interface to a shared-medium interface. If such forwarding is never allowed by the TOE, then FMT_SMF.1 and FMT_SMR.1 do not need to be employed in support of this FPT_FDI_EXP.1.

13.3 IEEE Std 2600.3 Errata

The following erratum exists in IEEE Std 2600.3 [B10]:

1. Clause 13.3, Page 29:

Discussion: PP APPLICATION NOTE 51 is incorrectly worded. An earlier draft of the FPT_FDI_EXP.1 SFR included a requirement to specify an authorized role, and PP APPLICATION NOTE 51 referred to that requirement. When that requirement was eventually removed (deferring to dependencies on FMT_SMR.1 and FMT_SMF.1), PP APPLICATION NOTE 51 should have been reworded so that it referred to the dependencies and not to FPT_FDI_EXP.1 itself.

Change: PP APPLICATION NOTE 51 should read:

PP APPLICATION NOTE 51. The ST Author may use FMT_SMF.1 and FMT_SMR.1 to specify the management function and authorized role for allowing data to be forwarded without further processing by the TSF from an external interface to a shared-medium interface. If such forwarding is never allowed by the TOE, then FMT_SMF.1 and FMT_SMR.1 do not need to be employed in support of this FPT_FDI_EXP.1.

13.4 IEEE Std 2600.4 Errata

The following erratum exists in IEEE Std 2600.4 [B11]:

2. Clause 13.3, Page 24:

FPT_FDI_EXP.1 SFR included a requirement to specify an authorized role, and PP APPLICATION NOTE 31 referred to that requirement. When that requirement was eventually removed (deferring to dependencies on FMT_SMR.1 and FMT_SMF.1), PP APPLICATION NOTE 31 should have been reworded so that it referred to the dependencies and not to FPT_FDI_EXP.1 itself.

Change: PP APPLICATION NOTE 31 should read:

PP APPLICATION NOTE 31. The ST Author may use FMT_SMF.1 and FMT_SMR.1 to specify the management function and authorized role for allowing data to be forwarded without further processing by the TSF from an external interface to a shared-medium interface. If such forwarding is never allowed by the TOE, then FMT_SMF.1 and FMT_SMR.1 do not need to be employed in support of this FPT_FDI_EXP.1.

14 Future Considerations

Items to be considered in future versions of this guide:

1. Guidance on how to evaluate a TOE based on one of the IEEE Std 2600 Series of Protection Profiles
2. Scheme-specific policies and interpretations that cross multiple Schemes
3. Certification issues in specific countries (e.g., unique Scheme policies)
4. How to deal with updates of CC and the relation to existing PPs and current / new STs
5. ST evaluators and PP validator guidance
6. CC and the relation to existing PPs and current / new STs

0