PP-Office Photocopier-1.3

Low Assurance Protection Profile for an Office Based Photocopier Device

Version	1.3
Date	6th April 2005
Author(s)	Rob Hunter Dirk-Jan Out

Certification ID	BSI-PP-0015
Sponsor	TNO-ITSEF BV
File name	Photocopier Low Assurance Protection Profile
No of pages	8

FINAL

Document information

Date of issue	6th April 2005
Author(s)	Rob Hunter Dirk-Jan Out
Version number report	1.3
Certification ID	BSI-PP-0015
Scheme	BSI
Sponsor	TNO-ITSEF BV
Sponsor address	Delftechpark 1 2628XJ Delft The Netherlands
Evaluation Lab	SRC
Evaluation Lab address	Graurheindorferstrasse 149a D-53117 Bonn Germany
Project leader	Rob Hunter
Target of Evaluation (TOE)	Office Based Photocopier Device
TOE reference name	Office Photocopier
CC-EAL number	1
Classification	Final
Report title	Low Assurance Protection Profile for an Office Based Photocopier Device
Report reference name	PP-Office Photocopier-1.3

Document history

Version	Date	Comment
0.1	27-Jan-04	Initial version
0.2	01-Feb-04	Initial review comments included
0.3	27-Feb-04	Strengthened compliance with CCv2.4
0.4	8-Apr-04	Added results from 6/7 April meeting
1.0	13-Apr-04	Added BSI comments
1.1	14-Apr-04	Added more BSI comments, submitted to SRC
1.2	26 Apr 04	Processed comments from SRC, final version
1.3	6 Apr 05	Incorporated Raised Interpretations, added certification ID

1.   PP Introduction

1.1   PP Reference

This is the Low Assurance Protection Profile for an
Office Based Photocopier Device 1.3, TNO-ITSEF BV, 6th April 2005

1.2   TOE overview

The TOE is a photocopier device, as it is typically used in a typical office
environment.

The TOE is used for copying: a piece of paper is placed upon its scanning
mechanism, the information on that paper is converted into data, and stored on an
intermediate storage device. From this intermediate storage device it is
transformed, and reproduced one or multiple times on paper. The TOE may be
connected to a network for the purpose of monitoring and/or managing the TOE.

As the information being copied may be confidential in nature, it is important that:
- The TOE does not retain residual information after use, in the intermediate
  storage device or otherwise;
- The TOE does not leak this information to the outside world (except by
  printing it on paper by request of the user).

The TOE is stand-alone, and hence does not require any non-TOE
hardware/software/firmware.

2.   Conformance claims

2.1   Conformance claim

This Protection Profile:
- claims conformance to CC version 2.4 release 256 and v2.4Draft Interpretation[1] #1-#17
- is CC Part 2 conformant and CC Part 3 conformant.
- does not claim conformance to any other PP.
- is EAL 1 conformant

2.2   Conformance claim rationale

PP-related conformance claim rationale
This PP does not claim conformance to another PP, so there is no rationale related to this.

Package-related conformance claim rationale
This PP is EAL1 conformant. The EAL1 package contains no uncompleted operations. As no SARs were added to EAL1, the SARs in this PP are consistent with EAL1.

2.3   Conformance statement

Security targets or other PPs wishing to claim conformance to this PP can do so as *strict-PP-conformance*. Demonstrable-PP-conformance is not allowed for this PP.

---

[1] V2.4 Draft Interpretation #n are interpretations that are made during the v2.4 Trial Period. They address problems with CC v2.4 as they occur.

3. Definition of terms

3.1 Definition of subjects, information and operations

This section is added to define the terms that are used in the Security Objectives of the Operational Environment and SFRs.

3.2 Subjects

S.USER   A person that makes copies with the TOE

S.OUTSIDE   Any entity outside the TOE (except S.USER)

All subjects have a single security attribute, which is identical to its name.

3.3 Information

I.COPY_INFO   Information that is derived by the TOE by scanning its input

I.COPY_INFO has a single security attribute, which is identical to its name.

3.4 Operations

The operations that are performed by the TOE are (in alphabetical order):

R.COPY   S.USER makes a copy with the TOE.

4.   Security Objectives for the Operational Environment

The operational environment of the TOE shall conform to the following objectives:

OE.OFFICE   The operational environment of the photocopier shall be a general office-type environment. This means low-to medium physical security measures.

Application Note: The goal for OE.OFFICE is to ensure that any PP or ST claiming compliance to this PP cannot add objectives for the operational environment that are inconsistent with this objective, such as "The printer shall be guarded for 24 hours a day".

OE.PAPER   S. USER shall be responsible for the confidentiality of the original paper input and all paper copies. This includes paper input and copies that remain in the copier when the copier fails.

5.   Security Requirements

5.1   Extended components definition

As this PP does not contain extended security requirements, there are no extended components.

5.2   SFRs

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1   The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from all objects containing I.COPY_INFO**[2]

FDP_RIP.1.2[3]   **The TSF shall deallocate the resources of all objects containing I.COPY_INFO:**
  - **immediately after completion of R.COPY**
  - **and on start-up of the TOE**[4]

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1   The TSF shall enforce the **NoLeakagePolicy**[5] on **S.OUTSIDE, I.COPY_INFO, and R.COPY**.

---

[2] The requirement was refined to make it more readable.

[3] Added an element (refinement) to show when the de-allocation is to take place. In our opinion the lack of this element is an error in FDP_RIP.1

[4] Photocopiers can experience errors and sometimes require restarting to handle these errors (or users restart the photocopier anyway in an attempt to handle these errors). It is therefore important that the photocopier also deletes data whenever it is restarted.

[5] The NoLeakagePolicy consists of the element FDP_IFF.1.6.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **NoLeakagePolicy[6]**.

FDP_IFF.1.6[7] The TSF shall explicitly deny an information flow based on the following rules: **R.COPY shall not cause I.COPY_INFO to flow to S.OUTSIDE (except in the form of a regular photocopy as requested by S.USER)**.

5.3 SARs

The SARs for this PP are the package EAL 1.

---

[6] The rest was refined away as this TOE uses no security attributes

[7] The second through fifth elements were refined away because no other rules and capabilities apply.