Océ Technologies BV

ST-Océ Smart Imager-2.1

Security Target
The Océ Smart Imager 8.3.3.39
as used in the Océ VP 2090 3.3

Version	2.1
Date	16th February 2006

Certification ID	BSI-DSZ-CC-0326
Sponsor	Océ Technologies BV
File name	Oce Smart Imager Security Target 2.1.doc
No of pages	60

This Security Target was prepared for:
Océ Technologies BV
P.O. Box 101,
5900 MA Venlo,
The Netherlands

by TNO-ITSEF B.V.

Document information

Date of issue	16th February 2006
Author(s)	Rob Hunter
Version number report	2.1
Certification ID	BSI-DSZ-CC-0326
Scheme	BSI
Sponsor	Océ Technologies BV P.O. Box 101, 5900 MA Venlo, The Netherlands
Evaluation Lab	TNO-ITSEF B.V. *IT Security Evaluation Facility* Delftechpark 1 2628XJ Delft The Netherlands
Sponsor Project leader	Christophe Soriano
Target of Evaluation (TOE)	The Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 3.3
TOE reference name	Océ Smart Imager
CC-EAL number	2+ (augmented with ALC_FLR.1)
Classification	None
Report title	Security Target The Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 3.3
Report reference name	ST-Océ Smart Imager-2.1

Document history

Version	Date	Comment
0.1	14-04-05	Initial draft
0.2	17-05-05	Incorporated Océ comments
0.3	30-05-05	Incorporated Océ and BSI comments
0.4	24-11-05	Incorporated Océ comments
1.0	06-02-06	Incorporated BSI comments
2.0	10-02-06	Incorporated BSI comments
2.1	16-02-06	Incorporated BSI comments

Signature

The project leader has signed for technical correctness.

Christophe Soriano
Project leader

Contents

1. Security Target Introduction

1.1 ST Identification

Name of the TOE:
The Océ Smart Imager 8.3.3.39
as used in the Océ VP 2090 3.3

Name of the Security Target:
Security Target
The Océ Smart Imager 8.3.3.39
as used in the Océ VP 2090 3.3

ST evaluation status: Non-evaluated release
ST version number: 2.1
ST publication date: 16th February 2006
ST authors: Rob Hunter

This Security Target was prepared for:
Océ Technologies BV
P.O. Box 101,
5900 MA Venlo,
The Netherlands

by TNO-ITSEF B.V. IT Security Evaluation Facility
Delftechpark 1
2628XJ Delft
The Netherlands

.

1.2 ST Overview

The firm Océ produces a wide range of multifunctional devices for copying, printing and scanning (MFDs) for various purposes. One of these MFDs: the VP 2090, uses PC hardware based controller, the Smart Imager.

- The Océ Smart Imager V8.3.3.39, is used with the Océ VP 2090 R3.3

These VarioPrint products are referred to collectively in this Security Target as MFDs

A Océ VP2090 with embedded Smart Imager controller.	

The Smart Imager is a PC-based MFD-controller. The Smart Imager provides a wide range of printing, scanning and copying functionality to the MFD peripherals to which it is connected. The Smart Imager provides security functionality to the MFD.

This Security Target describes the Smart Imager and the specific security problem that it addresses. The Target of Evaluation (TOE) is a collection of software components (Océ developed software, 3rd party printer language interpreters, Operating System) that use the underlying hardware platform. The TOE is a subset of the complete Smart Imager.

1.3 CC Conformance

The evaluation is based upon:

- Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 1: General model, August 1999, annotated with interpretations as of 2003-12-31.
- Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 2: Security functional requirements, August 1999, annotated with interpretations as of 2003-12-31.
- Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 3: Security assurance requirements, August 1999, annotated with interpretations as of 2003-12-31.
- Common Methodology for Information Technology Security Evaluation, Version 1.0, Part 2: Evaluation Methodology, August 1999, annotated with interpretations as of 2003-12-31.

The chosen level of assurance is:

EAL2 (Evaluation Assurance Level 2 augmented with ALC_FLR.1**)**

This Security Target claims the following conformance to the CC:

CC Part 2 conformant
CC Part 3 conformant

2. TOE Description

2.1 TOE Overview

This section presents an overview of the TOE.

2.1.1 TOE physical scope and boundary

The firm Océ produces a wide range of multifunctional devices for copying, printing and scanning (MFDs). For the purpose of this evaluation, the MFD consists of two main parts: (1) the Smart Imager controller and (2) the Digital Printer and Scanner/Copier and Local User Interface peripherals that together form the VP2090 product.

The Smart Imager is a PC-based MFD-controller that provides a wide range of printing, scanning and copy functionality to the Digital Printer, Scanner and Copier and Local User Interface peripherals to which the Smart Imager is connected. The Smart Imager provides security functionality to the MFD.

The Smart Imager can operate in two different security modes: ‘High’ and ‘Normal’. This Security Target covers the Smart Imager operating in the security mode ‘High’ as delivered by Océ to the customer. This mode provides a restricted set of functionality that is configured to meet the Security Target claim. Changing the operational mode invalidates the claim made in this Security Target

The Smart Imager is connected between a network and the MFD. This is depicted in Figure 1.

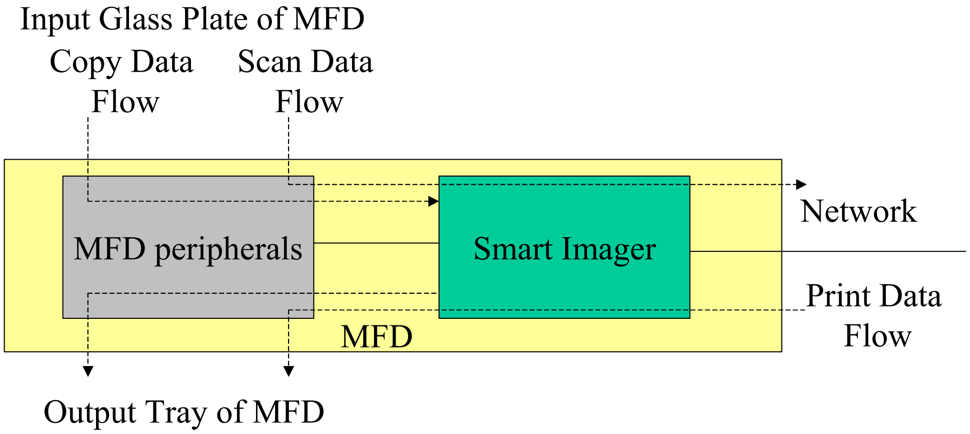


Figure 1: Relation between the Smart Imager and MFD.

The Smart Imager is located internally in the MFD. This physical configuration is depicted in Figure 2.

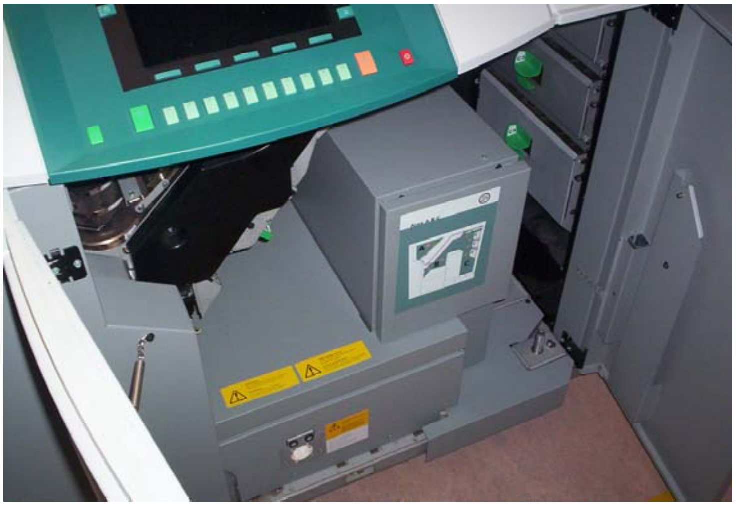


Figure 2: Front view of the Smart Imager controller.

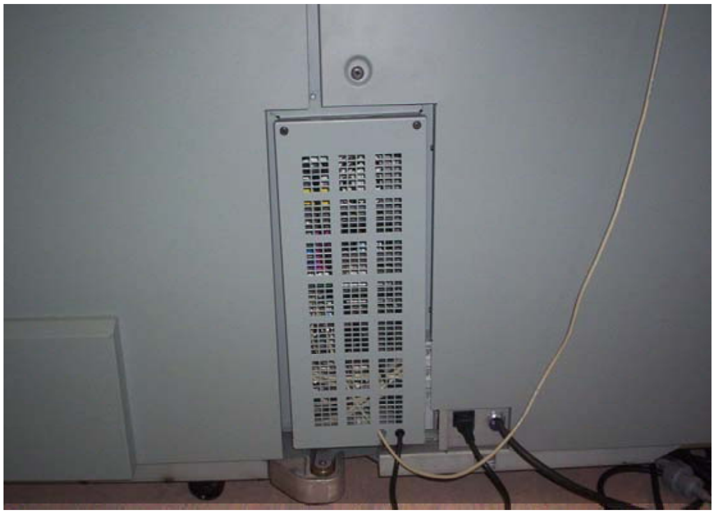


Figure 3: Rear view of the Smart Imager controller.

The internal configuration helps prevent theft of the Smart Imager, but prevention of theft of the Smart Imager is outside the scope of this evaluation[1]. All logical access points (CD-Rom, floppy drives, network ports, USB/serial/parallel ports etc. are protected from physical access in the internal configuration by a metal casing.

The Smart Imager consists of:

1. A generic off-the-shelf PC comprising at a minimum a 1.5Ghz Celeron processor, 512MB internal RAM, a DVI output (graphical I/O), Two 40GB hard drives, two USB ports, one serial port, internal floppy and CDROM drive.
2. Generic graphics card and network card supporting 10/100/1000Mbs Ethernet UTP.
3. An Océ DP1 card for communication between the Smart Imager and it's attached peripherals.
4. Drivers for the PC, graphics card and network card
5. The Microsoft Windows 2000 operating system with service pack 4 (operating system version 5.00.2195) plus the following patches:
   Q823559 (MS03-023)
   Q828749 (MS03-049)
   Q835732 (MS04-011)
   Q828741 (MS04-012)

[1] Note that the SmartImager protects print, copy, and scan data stored in it against theft through e-shredding, but the SmartImager itself may be stolen.

Q837001 (MS04-014)
Q893066 (MS04-010) v2

6. Océ Smart Imager-specific software release 8.3.3.39.
7. Third-party developed software: Adobe PS3-PDF Interpreter, Version 3016.103 build #03; PCL5 interpreter, Version ME6.0.1/4; Microsoft IIS web server with SSL support, Version 5.0.

Of these 7, the first four are not part of the TOE and together form the underlying hardware platform that the TOE makes use of. The underlying hardware platform does not provide any specific security related functionality for the TOE. The TSF is mediated by the last three software components that are part of the TOE. This is depicted in Figure 4.

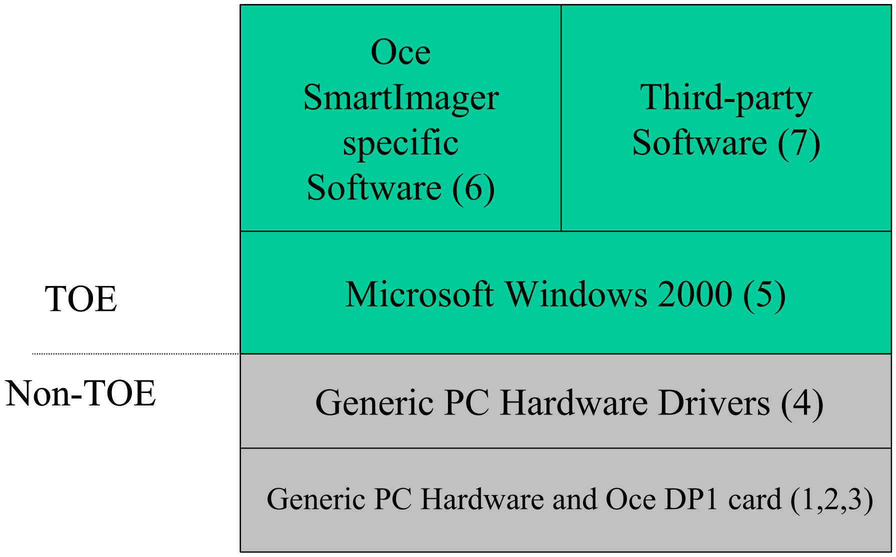

Oce SmartImager specific Software (6)
Third-party Software (7)
TOE
Microsoft Windows 2000 (5)
Non-TOE
Generic PC Hardware Drivers (4)
Generic PC Hardware and Oce DP1 card (1,2,3)

Figure 4: Division of the Smart Imager into TOE and non-TOE.

The physical interfaces through which the TOE communicates are:

- A USB port through which a service engineer can administer the TOE.
- A network card through which print and scan jobs can pass and a remote system administrator can administer the TOE
- A RS-232 interface. The data that flows between the TOE and the MFD for printing control purposes passes through this interface.
- A DP1 board with an RS-232 interface. The data that flows between the TOE and the MFD for all printing, scanning and copying purposes (other than printer control) passes through this interface.
- A USB port through which the local user can communicate with the TOE via the Local User Interface (LUI).

The user guidance for the TOE consists of:

- Océ VP2090 User manual
- Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39.

The administrator guidance for the TOE consists of:

- Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39
- The Smart Imager administration guidance for the customer system administrator takes the form of HTML pages. These are part of the Océ Smart Imager-specific software, Version 8.3.3.39.

The Smart Imager administration guidance for the Océ service engineer takes the form of an application called the Technical Service Manual that is installed on the service engineer's laptop. The guidance contains an appendix that is identified as:

- VP 2090 Smart Imager Security Service documents in the TSM: System Software - Installation

and is a frozen version of the Océ service engineer application made at the time of product release.

2.1.2 TOE logical scope and boundary

The TOE protects two assets: itself and the copy, print and scan job data that it receives:
Firstly, the TOE protects it's own integrity against threats from the LAN to which it is attached through use of a firewall.

Secondly, the TOE protects the confidentiality of print, copy and scan job data after they are no longer needed. The Smart Imager does this by shredding the data after they are deleted.

In order to protect these two assets, it offers the following functionality:

The TOE controls printing from the network
The TOE accepts Postscript, PDF and PCL5e print jobs from remote users on the network (lpr over TCP/IP) and provides these as images to the attached MFD printing peripheral. The TOE can print these jobs in two different ways. The remote users can select the way in which each of his jobs is printed from a printer settings dialog box on the screen of their PC.

Automatic printing
The TOE receives a print job from a remote end-user, and stores it in a queue. Once this job is the first one in the queue, the TOE processes this print job into images, and sends these images to the attached MFD peripheral for printing.

Mailbox printing

The TOE receives a print job from a remote end-user and stores it internally. The end-user then has to go physically to the VP2090 (become a local end-user) and identify himself at the Local User Interface (LUI). Only after this, will the TOE process the job. The resulting images are sent for printing.

Secure printing

This is similar to mailbox printing, with two differences:

- When submitting the print job, the remote end-user adds a job-specific PIN code that has a length of either 4 or 5 digits to the job.[2]
- The PIN code is stored in the Smart Imager.

When identifying himself at the LUI, the local end-user also has to provide the job-specific PIN code. The Smart Imager verifies the validity of the PIN. If correct, the print job data is released by the Smart Imager and rendered on paper. A replay attack with an intercepted PIN is countered by shredding the print job data after the print job is deleted from the mailbox.

The end-users and interfaces they interact with are depicted in Figure 5.

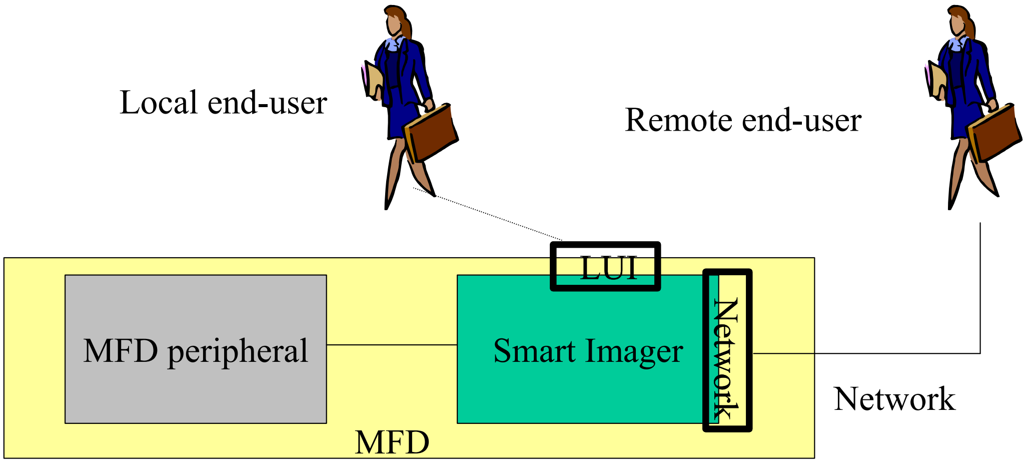


Figure 5: End-users and interfaces for printing

The TOE is configured to destroy the data relating to print jobs, scan jobs, copy jobs and temporary files[3].

[2] The TOE software allows a minimum PINcode length of 1 digit but there is a policy that is described in the user guidance that requires to the user to specify at least 4 digits.

[3] Job data is deleted when the job is completed or deleted from the mailbox. Temporary files (swap file) are shredded during system restart.

This is achieved by writing over the job related data with other data, thereby making it difficulty to retrieve the original data.

The TOE administrators can select the number of write iterations. The first iteration starts after the data is deleted (and is referred to further in this document as synchronous shredding). The remaining iterations take place with low priority in the background (and is referred to further in this document as asynchronous shredding).

Additionally, the TOE is also configured to shred all data at the end of each working day by specifying a specific time interval no greater than once every 24 hours.[4]

The TOE administers scan jobs that are exported to the network
Local end-users can scan documents on the VP2090, and the resulting images will then be submitted to the TOE. The TOE can process the images to a variety of file formats and then transfer the resulting files by ftp to an ftp-server, or by SMTP to an e-mail server on the network.

The end-users and interfaces they interact with are depicted in Figure 6.

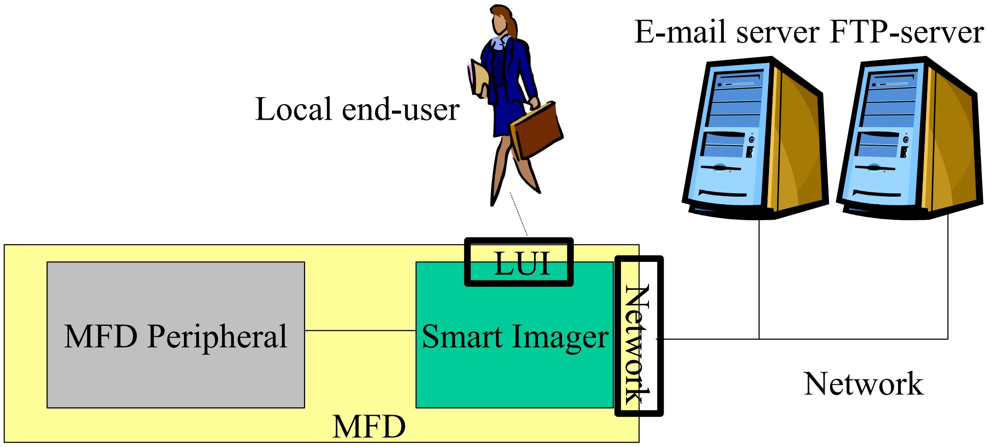


Figure 6: End-users and interfaces for scanning

[4] The setting to shred the data at a particular time interval is not enabled by default. The administrator guidance describes a policy, defined later in this Security Target, that requires the customer administrator to do this.

The TOE can be managed

As indicated in the previous sections, the MFD (of which the TOE is a part) supports local and remote end-users. The MFD also supports various administrators, which are described briefly here:

Remote Key Operator: These are typically administrators or secretaries from the organization owning/renting the TOE. They can interact with the Smart Imager through a Web interface that communicates with the TOE via the LAN. Through this interaction they have access to a limited amount of non-security related settings of the TOE.

Remote System administrator (HTTPS): These are remote administrators, typically a network administrator from the organization owning/renting the TOE. They can read and write a limited set of settings of the TOE through an SSL over HTTP connection (HTTPS). The remote administrator can identify the TOE via a certificate. Help files for the administrator are also delivered via the HTTPS connection. Web pages that are delivered via the HTTPS connection are ‘non-cacheable’.

Remote System administrator (SNMP): These are remote administrators, typically a network administrator from the organization owning/renting the TOE. They can read and write a limited set of settings of the TOE through a SNMP connection. None of the settings that the remote system administrator can access through SNMP are security related in the sense that they provide access to the assets that the TOE protects or allow changes to be made to the TOE security functionality.

Service engineer: These are local administrators, and are typically employed by Océ. They have access through an USB connection to a wide range of settings on the TOE. The TOE connection is PIN code protected and service license protected and access to the management functions provided to the Service engineer require specific hardware and software. It is not possible to access the management functions made available to the service engineer without the software that is installed on the service engineer laptop.

The various administrators and the interfaces through which they interact with the TOE are depicted in Figure 7.

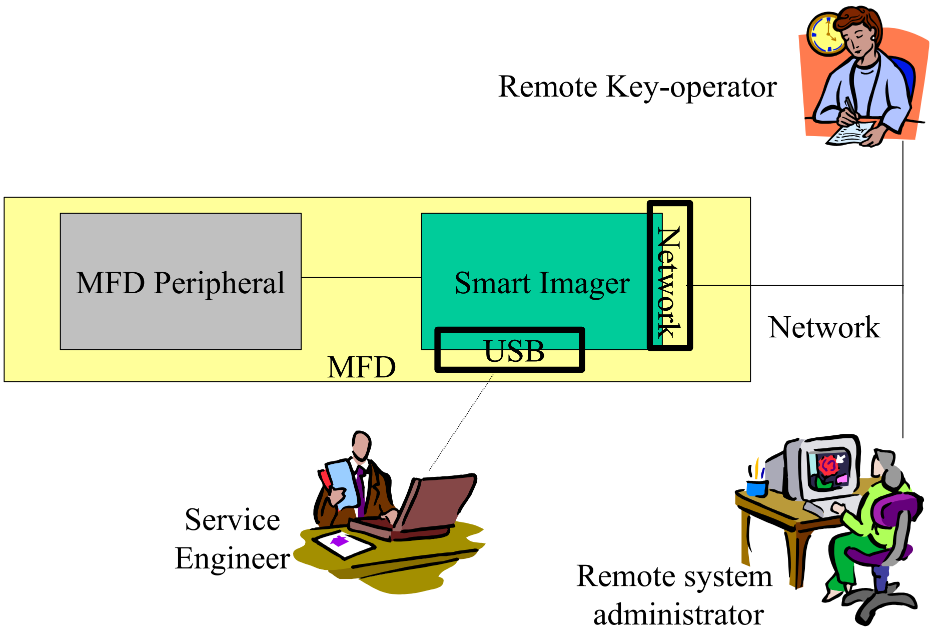


Figure 7: MFD Administrators and interfaces

The TOE has minimized all other functionality

The TOE supports the following network protocols:

- TCP/IP, UDP/IP and ICMP;

No other network protocols are enabled. The TOE manufacturer has filtered all network ports so that only data that is essential to the operation of the TOE can enter the TOE through the network interface. The TOE has further restricted the functionality behind each open network port to that which is absolutely necessary to its functioning. This is done to maximize the integrity of the TOE itself and minimize the risk of the TOE being infected or hacked and subsequently being used as a stepping-stone to damage the network.

The availability of security related functionality

As depicted in Figure 7, The Remote Key Operator is not able to influence the security of the TOE as they have no access to security settings via the Smart Imager LUI.

Because the Remote Key Operator and Local End-User cannot access security related settings on the Smart Imager LUI, they cannot affect the TOE. For the sake of clarity, Figure 8 shows the interfaces to the TOE and the subjects that can access and manage TOE security settings.

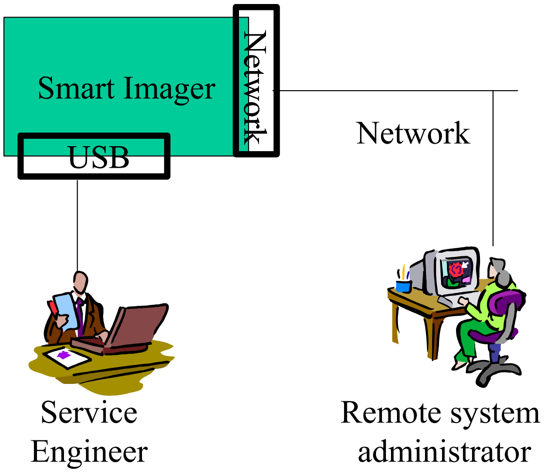


Figure 8: TOE Administrators and interfaces

3. TOE Security Environment

The TOE is intended to provide scan, print and copy functionality to users requiring a low to moderate level of security assurance. Additional environmental and organisational requirements support the security functionality provided by the TOE.

3.1 Definition of subjects, objects and operations

To facilitate definition of threats, OSPs, assumptions, security objectives and security requirements, we define the subjects, objects and operations to be used in the ST first.

3.1.1 Non-human subjects

The systems (equipment) that will be interacting with the TOE (in alphabetical order):

S.DIGITAL_PRINTER A device that is part of the MFD peripheral that physically renders a print job and is attached to the TOE via a cable.

S.DIGITAL_SCANNER A device that is part of the MFG peripheral that scans in a copy or scan job and is attached to the TOE via a cable.

S.LUI A device that provides a User Interface to S.LOCAL_USER.

S.NETWORK_DEVICE An unspecified network device that is logically connected to the TOE and is located in the same operating environment (office building).

3.1.2 Human subjects

The users (or subject acting on behalf of that user) that will be interacting with the TOE are:

S.REMOTE_USER A person located within the operational environment of the TOE who is aware of how the TOE should be used. They are not malicious towards the TOE but are capable of making mistakes when operating it. S.REMOTE_USER typically sends print jobs from their desktop PC to the TOE.

S.LOCAL_USER A person located within the operational environment of the TOE who is aware of how the TOE should be used.

They are not malicious towards the TOE but are capable of making mistakes when operating it. S.LOCAL_USER typically interacts indirectly with the TOE via S.LUI

S.REMOTE_SYSADMIN A person who can change some TOE settings using a Océ supplied interface accessed remotely over a network connection. They are trusted by the customer and are adequately trained. They are capable of making mistakes. They access the TOE via its network card from a remote location on the customer LAN. They do not access the TOE locally via a USB connection .

S.SERVICE_ENGINEER A person with elevated privileges above those of S.LOCAL_USER and S.REMOTE_SYSADMIN. This person is an Océ representative and accesses the TOE locally through a USB interface that is separate to the customer LAN interface. They do not access the TOE remotely via the customer LAN interface. They are not malicious towards the TOE but are capable of making mistakes when operating it.

S.THIEF S.THIEF (cleaning staff, burglar, visitor, in rare cases a user) will have no moral issues in stealing the TOE or parts of it. Once S.THIEF has stolen the TOE or parts of it he may attempt to retrieve earlier printer, scanner and copy jobs from the TOE. S.THIEF is opportunistic and is not a recurring visitor to the environment in which the TOE operates.

Note that the key operator is not included as a subject that interacts with the TOE as he is not able to make changes to the security settings of the TOE and is therefore equal to S.REMOTE_USER with respect to security.

3.1.3 Objects

The (data) objects for the TOE that the TOE will operate upon are:

D.SECURE_PRINT_JOB A secure print job submitted by S.REMOTE_USER to the TOE. D.SECURE_PRINT_JOB has the Security Attribute *Username/PIN* associated with them.

D.PRINT_JOB A print job submitted by S.REMOTE_USER to the TOE.

D.SCAN_JOB Data that is scanned in via the S.DIGITAL_SCANNER peripheral attached to the Smart Imager. Data is sent from the TOE to a FTP or e-mail server located elsewhere on the network.

D.COPY_JOB Data that is scanned in via the S.DIGITAL_SCANNER peripheral attached to the Smart Imager. Data is returned from the TOE to the printer peripheral for rendering.

D.INBOUND_TRAFFIC TCP/IP, UDP/IP or ICMP network packets received by the TOE. D.INBOUND_TRAFFIC has the Security Attributes *Port* and *Protocol* associated with it.

3.1.4 Operations

The operations that are performed by the TOE are:

R.RELEASE_JOB The TOE processes and releases a D.SECURE_PRINT_JOB to the attached S.DIGITAL_PRINTER peripheral.

R.PRINT_JOB The TOE processes and releases a D.PRINT_JOB to the attached S.DIGITAL_PRINTER peripheral.

R.SCAN_JOB The TOE processes and releases a D.SCAN_JOB to the attached network though S.NETWORK_DEVICE.

R.COPY_JOB The TOE processes and releases a D.COPY_JOB to the attached S.DIGITAL_PRINTER peripheral.

R.SHRED_JOB The TOE shreds redundant D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D_COPY_JOB data objects from the TOE’s hard disk.

R.ENTER_TOE The TOE allows D.INBOUND_TRAFFIC from S.NETWORK_DEVICE to enter its boundary.

3.2 Assumptions

A.DIGITAL_PRINTER It is assumed that the TOE has a S.DIGITAL_PRINTER device attached to it. S.DIGITAL_PRINTER is part of the Océ VarioPrint 2090 MFD. For all print jobs that are sent to the mailbox, whether the job is printed or not, the job will be deleted on the same workday. Employees are aware of this requirement. It is assumed that for EAL2, that the interface from the Smart Imager to the S.DIGITAL_PRINTER will not be used to mount an attack and that the interface is only used for the purposes of printing.

A.DIGITAL_SCANNER It is assumed that the TOE has a S.DIGITAL_SCANNER device attached to it.

S.DIGITAL_SCANNER is part of the Océ VarioPrint 2090 MFD. It is assumed that for EAL2, that the interface from the Smart Imager to the S.DIGITAL_SCANNER will not be used to mount an attack and that the interface is only used for the purposes of scanning.

A.LUI
It is assumed that the TOE has a S.LUI device attached to it. S.LUI is part of the Océ VarioPrint 2090 MFD. It is assumed that for EAL2, that the interface from the LUI to the Smart Imager will not be used to mount an attack and that the interface is only used for the purposes of printing, scanning and copying.

A.ENVIRONMENT
The TOE assumes that its operational environment is a regular office environment. Physical access to the operational environment is restricted. The environment contains non-threatening office personnel (S.LOCAL_USER, S.REMOTE_USER, S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER). S.THIEF is only rarely present in this environment and not on a recurring basis.

A.SECURITY_POLICY
It is assumed that the customer will have a Security Policy governing the use of IT products by employees in the customer organisation. The TOE assumes that the network to which it is attached is protected by security measures that are intended to prevent mal-ware, viruses and network traffic, not related to the working of the operational environment, entering the network to which it is attached. Although the Virus database files and various patches are kept up to date, the policy recognises that new threats emerge over time and that occasionally they may enter the environment from outside and provides measures to help limit the damage. The Policy will define how IT products are protected against threats originating from outside the customer organisation. The organisation's employees are aware of, are trained in and operate according to the terms and conditions of the policy. The policy also covers physical security and the need for employees to work in a security aware manner including the usage of the TOE. The Security Policy describes and requires a low to medium level of assurance (EAL2) for the TOE.

A.SLA It is assumed that any security flaws discovered in the TOE will be repaired by Océ (possibly as part of an agreed service level agreement).

3.3 Threats

T.RESIDUAL_DATA S.THIEF steals the TOE or parts thereof and retrieves stored or deleted D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB. The motivation for S.THIEF to attack the TOE is low because it requires sophisticated data recovery equipment that can recover data even after the shredding mechanism has executed to recover data that has little value to the attacker.

T.NOSY_USER S.LOCAL_USER accesses a D.SECURE_PRINT_JOB that does not belong to him/her that is stored in the Smart Imager. The motivation to carry out this attack is low.

T.MALWARE A S.NETWORK_DEVICE is used by malware that may have entered the TOE's operational environment to launch an attack on the integrity of the TOE. The motivation to carry out this attack is low.

3.4 Organisational Security Policies

P.JOB_DELETE When D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB objects are no longer needed by the TOE, they will be deleted by the TOE at the earliest available opportunity in a manner that meets a recognised standard.

P.TOE_ADMINISTRATION The modification of TOE security settings shall be restricted to S.SERVICE_ENGINEER and S.REMOTE_SYSADMIN.

4. Security Objectives

4.1 TOE Security Objectives

This section consists of two groups of objectives:

- Functional Security Objectives for the TOE, that deal with what the TOE must do;
- Assurance Security Objectives for the TOE, that deal with how much assurance one should have in that the TOE does what it is expected to.

4.1.1 Functional Security Objectives for the TOE

O.F.INBOUND_FILTER The TOE will only support TCP/IP, UDP/IP and ICMP as a network protocol. D.INBOUND_TRAFFIC shall only enter the TOE (R.ENTER_TOE) if its Port is specified as being open in Appendix D.

O.F.JOB_RELEASE The TOE shall only perform R.RELEASE_JOB once S.LOCAL_USER has successfully identified and authenticated himself as owner of D.SECURE_PRINT_JOB.

O.F.JOB_SHRED The TOE shall delete all D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB data as soon as it is no longer required. During the start-up procedure, any residual D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB located in the TOE's hard disk (including the swap file) is deleted. The first write cycle occurs after the job has been deleted and the other remaining cycles occur once the TOE enters an idle state. The data shall be deleted according to a recognised standard so that it cannot be reconstituted.

O.F.AUTHENTICATE The TOE ensures that S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER must authenticate themselves to the TOE before allowing them to modify the TOE security settings.

4.1.2 Assurance Security Objectives for the TOE

O.A.SLA The TOE shall be evaluated to ALC_FLR.1

4.2 Security Objectives for the environment

O.E.ENVIRONMENT The environment into which the TOE will be introduced is protected by physical measures that limit access S.LOCAL_USER, S.REMOTE_USER, S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER. The physical measures are adequate to prevent all other persons but not a determined S.THIEF who deliberately wants to steal part of or all of the TOE by methodically planning an attack on the TOE over a period of time.

O.E.NETWORK_POLICY The network to which the TOE is attached shall be adequately protected so that the TOE is not visible outside the network. In addition, measures shall be implemented to only allow connections to the TOE from devices situated on the same network. No inbound connections from external networks are allowed. The network scans data for mal-ware (viruses and worms). This type of data may originate from either inside or outside the network to which the TOE is attached and includes the TOE itself.

O.E.DEPLOYMENT The network (LAN) to which the TOE is attached is well managed with established procedures for introducing and attaching new devices to the network.

O.E.DIGITAL_COPIER The environment into which the TOE will be introduced shall contain an Océ VarioPrint 2090 MFD that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE (selecting username). When sending a D.SECURE_PRINT_JOB to the Smart Imager, S.REMOTE_USER shall specify a PIN that consists of a minimum of 4 and a maximum of 5 digits and, whether or not it is printed, will ensure the print job is deleted from the TOE during the same workday that the job is sent. When sending a D.SECURE_PRINT_JOB or D.PRINT_JOB to the Smart Imager, S.REMOTE_USER will ensure the print job is deleted from the TOE during the same workday that the job is sent either by printing it or deleting it from the queue.

	The Smart Imager MFD peripheral provides a glass plate and LUI with which S.LOCAL_USER can perform print, scan and copy jobs. The ST claim is not valid when the TOE is used with any other type of Océ MFD. The TOE will not work with any other device (including Digital MFD Products from any other manufacturers).
O.E.SHREDDING	The customer requires the shredding of D.SECURE_PRINT_JOB, D.PRINT_JOB D.SCAN_JOB and D,COPY_JOB data objects

5. IT Security Requirements

5.1 TOE Security Functional Requirements

5.1.1 SFRs for Filtering

FDP_ACC.1 Subset access control

FDP_ACC1.1 The TSF shall enforce the **NETWORK_POLICY** on:

- **D.INBOUND_TRAFFIC**

Dependencies: FDP_ACF.1 (included)

FDP_ACF.1 Security attribute based access control

FDP_ACF1.1 The TSF shall enforce the **NETWORK_POLICY** to objects based on **the following**:

- **Port;**
- **Protocol.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The TOE shall perform R.ENTER_TOE on D.INBOUND_TRAFFIC only if Port(D.INBOUND_TRAFFIC) = ICMP, DNS, DHCP, LPR, HTTP, HTTPS, FTP, SNMP, IPSEC and Protocol = TCP/IP or UDP/IP**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **none**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **none**

Dependencies: FDP_ACC.1 (included)
FMT_MSA.3 (included)

5.1.2 SFRs for Job Release

FIA_UID.1 Timing of identification (Secure Printing)

FIA_UID.1.1 The TSF shall allow **R.PRINT_JOB, R.COPY_JOB and R.SCAN_JOB** on behalf of the **S.LOCAL_USER** to be performed before **S.LOCAL_USER** is identified.

FIA_UID.1.2 The TSF shall require **S.LOCAL_USER** to be successfully identified before allowing **R.RELEASE_JOB** on behalf of **S.LOCAL_USER**.

Dependencies: No dependencies.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **R.PRINT_JOB, R.COPY_JOB and R.SCAN_JOB** on behalf of the **S.LOCAL_USER** to be performed before **S.LOCAL_USER** is authenticated.

FIA_UAU.1.2 The TSF shall require **S.LOCAL_USER** to be successfully authenticated before allowing **R.RELEASE_JOB** on behalf of **S.LOCAL_USER**.

Dependencies: FIA_UID.1 (included)

5.1.3 SFRs for Shredding

FDP_RIP.1 Subset residual; information protection

FDP_RIP.1.1[5] The TSF shall ensure that any previous information content of a resource is made unavailable upon the

deallocation of the resource from the following objects: **D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB, D_COPY_JOB**

- **on deletion of R.RELEASE_JOB, R.PRINT_JOB, R.COPY_JOB and R.SCAN_JOB by S.LOCAL_USER, S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER**
- **on start-up or reboot of the TOE.**[6]

Dependencies: No dependencies.

5.1.4 SFRs for Management

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require **S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER** to identify **themselves** before allowing any other TSF-mediated actions on the behalf of that user.

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require **S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER** to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user.

Dependencies: FIA_UID.1 (included)

[5] This is a refinement to show when the de-allocation is to take place. When you delete a file, the OS modifies the relevant entry from the file allocation table. The data remains on the hard disk and can be retrieved with suitable tools. This is why the TOE shreds the data. What is happening is that:

- When the job manager discards data, it moves the data reference in the file allocation table to a location that is dedicated to the E-shred subsystem.
- The E-shred subsystem then erases the data (makes the data unavailable) by overwriting the data several times.
- The E-shred service then removes the reference to the erased data from the file allocation table so that the erased disk resources can be re-used.

[6] The SmartImager 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.

FMT_MOF.1 Management of security functions behaviour (S.REMOTE_SYSADMIN)[7]

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour of** the functions **described in appendix E for S.REMOTE_SYSADMIN** to **S.REMOTE_SYSADMIN.**

Dependencies: FMT_SMF.1 (included)
FMT_SMR.1 (included)

FMT_MOF.1 Management of security functions behaviour (S.SERVICE_ENGINEER)

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour of** the **functions described in appendix E for S.SERVICE_ENGINEER** to **S.SERVICE_ENGINEER.**.

Dependencies: FMT_SMF.1 (included)
FMT_SMR.1 (included)

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **NETWORK_POLICY** to restrict the ability to **change the default** [8] security attributes **Port and Protocol** to **nobody.**[9]

Dependencies: FDP_ACC.1 (included)
FMT_SMF.1 (included)
FMT_SMR.1 (included)

FMT_MSA.3 Static Attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **NETWORK_POLICY** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **nobody**[10] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 (included)
FMT_SMR.1 (included)

[7] Note that this SFR relates to administration via the HTTPS connection. There are no TSF mediated actions that can be managed via the SNMP connection.

[8] For grammatical and clarity reasons, the underscore between change and default was removed and the word 'the' before security attributes was moved to between 'change' and 'default'.

[9] The TOE does not allow any users to change any security attributes in the evaluated configuration.

[10] The word 'the' before 'nobody' was removed for grammatical reasons.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions **as described in appendix E**:

Functions related to R.SHRED_JOB that are available to S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER

- **Set the number of shred runs**[11]

Dependencies: No dependencies.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **S.REMOTE_SYSADMIN, S.SERVICE_ENGINEER, S.REMOTE_USER and S.LOCAL_USER**.

FMT_SMR1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 (included)

5.1.5 SFRs for Protection of the TSF itself

FPT_SEP.1 TSF domain separation

FPT_SEP1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

[11] Note that this is the only setting which is available in security mode high, the evaluated configuration.

5.1.6 Strength-of-function claim

The Strength of function claim for all the probabilistic functions and mechanisms provided by the TOE is SOF-basic.

5.2 TOE Security Assurance Requirements

The TOE security assurance requirements are conformant to the CC Evaluation Assurance Level EAL2 +ALC_FLR.1. In detail the following Security Assurance Requirements are chosen for the TOE:

Components for Configuration management (**Class ACM**)
- ACM_CAP.2 Configuration Items

Components for Delivery and operation (**Class ADO**)
- ADO_DEL.1 Delivery procedures
- ADO_IGS.1 Installation, generation, and start-up procedures

Components for Development (**Class ADV**)
- ADV_FSP.1 Informal functional specification
- ADV_HLD.1 Descriptive high-level design
- ADV_RCR.1 Informal correspondence demonstration

Components for Guidance documents (**Class AGD**)
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance

Components for Life cycle support (**Class ALC**)
- ALC_FLR.1 Basic flaw remediation

Components for Tests (**Class ATE**)
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing – sample

Components for Vulnerability assessment (**Class AVA**)
- AVA_SOF.1 Strength of TOE security function evaluation
- AVA_VLA.1 Developer vulnerability analysis

5.3 Security Requirements for the IT Environment

None[12].

[12] The ST defines security objectives for the IT environment in which the TOE will operate. In accordance with the Common Criteria Standard, these objectives are not mapped to Security Requirements for the IT Environment.

5.4 Explicitly stated requirements

None.

6. TOE Summary Specification

6.1 IT Security Functions

SF.FILTERING
The TOE uses a built-in firewall to block ports that are not needed for the operation of the TOE. In addition no network protocols that are not supported by the evaluated configuration are enabled.

By default no traffic is permitted to enter the TOE from the network to which it is attached, except for the supported network packets via the ports defined in the rule table described in Appendix D.

SF.JOB_RELEASE
The TOE verifies the identity and associated PIN code that was sent with the print job when submitted by S.REMOTE_USER with Username/PIN received from S.LOCAL_USER via the Smart Imager interface. If verification is successful, the secure print job is released for printing.

SF.SHREDDING
Once a print, copy or scan job has been deleted, the data is overwritten. It is possible to perform multiple write cycles, with various patterns being applied. At least three write cycles will always take place. The first write cycle starts after the job has been deleted and to improve job throughput performance, all other remaining cycles are done once the TOE enters an idle state. The shredding mechanism supports US DOD 5220-22m and Gutmann algorithms[13].

SF.MANAGEMENT
The TOE can be managed in relation to SF.SHREDDING. In order to gain access, the S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER must authenticate themselves to the TOE. S.SERVICE_ENGINEER does this by entering a PIN. S.REMOTE_SYSADMIN authenticates himself by entering a password. The TOE is delivered by Océ with the most restrictive set of operational settings.

6.1.1 Probabilistic functions and mechanisms

The TOE contains probabilistic functions and mechanisms in the form of passwords and PIN numbers that are used for the authentication of S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER respectively.

[13] See Appendix B – References for more information relating to these algorithms

Subject	Function	Mechanism
S.REMOTE_SYSADMIN	SF.MANAGEMENT, SF.SHREDDING	For the HTTPS connection, an alpha-numeric password (ASCII characters 32-127) ranging in length between 8 and 50 characters is required. After the first failed attempt, a delay mechanism is invoked. There are no security management functions or access to the assets that the TOE protects that are accessible via the SNMP connection.
S.SERVICE_ENGINEER	SF.MANAGEMENT, SF.SHREDDING	A fixed length numeric pin code of 6 digits.
S.LOCAL_USER	SF.JOB_RELEASE	A numeric pin code varying in length between 4 and 5 digits.

6.1.2 Strength of function claim

The SFRs FIA_UID.1, FIA_UID.2, FIA_UAU.1 and FIA_UAU.2 require the TOE to provide security functions that provide identification/authentication functionality that meets a SOF claim of ‘SOF basic’.

A strength of function claim of ‘SOF basic’ is made for the security functions SF.JOB_RELEASE and SF.MANAGEMENT. These are the security functions that implement FIA_UID.1, FIA_UID.2, FIA_UAU.1 and FIA_UAU.2.

6.2 Assurance Measures

Appropriate assurance measures are employed to satisfy the security assurance requirements. The following list gives a mapping between the assurance requirements and the documents containing the information needed for the fulfillment of the respective requirement.

Configuration Management (ACM) assurance measures
The documents containing the description of the configuration management system as required by ACM and how it is used are is:
Océ-Technologies B.V., Configuration Management for the SI R8.3.3.39.doc

Delivery and Operation (ADO) assurance measures
The document containing the description of all steps necessary for secure installation, generation and start-up of the TOE is:
Océ Engineering Venlo, Delivery and developer security for SI R8.3.3.39.doc

Development (ADV) assurance measures
The developer documentation for ADV functional specifications can be found in:

- Océ-Technologies B.V., Functional Specification for SI R8.3.3.39.doc
- Océ-Technologies B.V., High Level Design for SI R8.3.3.39.doc

Guidance (AGD) assurance measures
The document containing the guidance for Océ service engineers is maintained on the service engineers laptop with the reference:

- VP 2090 Smart Imager Security Service documents in the TSM system software - installation,

and is not a publicly available document.

The guidance for the customer administrators and users is in:

- Océ-Technologies B.V., Océ System Configuration On-line help.
- Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39.
- Océ VarioPrint 2090 User manual

Life Cycle (ALC) assurance measures
The physical, procedural, personnel and other security measures applied by the developer can be found in:
Océ-Technologies B.V., Flaw remediation for SI R8.3.3.39.doc

Test (ATE) assurance measures
The developer test documentation can be A test analysis showing that the tests cover the entire functional specification can be found in:

Océ-Technologies B.V., Test Documentation for the SI R8.3.3.39.doc

Vulnerability Assessment (AVA) assurance measures
An analysis of vulnerabilities can be found in:

- Océ-Technologies B.V., Strength of function analysis for SI R8.3.3.39.doc
- Océ-Technologies B.V., Vulnerability analysis for SI R8.3.3.39.doc

7. PP Claims

This Security Target TOE does not claim compliance to a Protection Profile.

8. Rationale

8.1 Security Objectives Rationale

For each assumption, threat and OSP we demonstrate that it is met by the security objectives. The tracings are provided in the following table.

	O.F.INBOUND_FILTER	O.F.JOB_RELEASE	O.F.JOB_SHREAD	O.F.AUTHENTICATE	O.A.SLA	O.E.ENVIRONMENT	O.E.NETWORK_POLICY	O.E.DEPLOYMENT	O.E.DIGITAL_COPIER	O.E.SHREDDING
A.DIGITAL_COPIER									X	
A.ENVIRONMENT						X				
A.SECURITY_POLICY							X	X	X	X
A.SHREDDING										X
A.SLA					X					
T.RESIDUAL_DATA			X							
T.NOSY_USER		X								
T.MALWARE	X									
P.TOE_ADMINISTRATION				X						
P.JOB_DELETE			X							

The individual rationales demonstrating that the threats, assumptions and organizational security policies are met are described as follows:

A.DIGITAL_COPIER
The assumption is met by the following TOE assurance objective:

O.E.DIGITAL_COPIER - The environment into which the TOE will be introduced shall contain an Océ VarioPrint 2090 MFD that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE.

When sending a D.SECURE_PRINT_JOB or D.PRINT_JOB to the Smart Imager, S.REMOTE_USER is aware that they must delete the job on the same workday that it is sent to the TOE, whether or not it is used. Requiring job data to be deleted from the TOE on the same workday it is sent reduces the time available to an attacker in which the data object is vulnerable. The MFD provides a glass plate and LUI with which S.LOCAL_USER can perform scan jobs. The ST claim is not valid when the TOE is used with any other type of Océ MFD. The TOE will not work with any other device (including Digital MFD Products from any other manufacturers).

Although the assumption states that a VarioPrint 2090 MFD from Océ will be used, the MFD is an un-trusted device.

A.ENVIRONMENT

The assumption is met by the following objectives for the environment:

O.E.ENVIRONMENT - The environment into which the TOE will be introduced is protected by physical measures that limit access S.LOCAL_USER, S.REMOTE_USER, S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER. The physical measures are adequate to prevent all other persons but a determined S.THIEF who deliberately wants to steal part of or all of the TOE by methodically planning an attack on the TOE over a period of time.

A.SECURITY_POLICY

The assumption is met by the following objectives for the environment:

O.E.NETWORK_POLICY - The network to which the TOE is attached shall be adequately protected so that the TOE is not visible outside the network. In addition, measures shall be implemented to only allow connections to the TOE from devices situated on the same network. No inbound connections from external networks are allowed. The network scans data for mal-ware (viruses and worms). This type of data may originate from either inside or outside the network to which the TOE is attached and includes the TOE itself.

O.E.DEPLOYMENT - The network (LAN) to which the TOE is attached is well managed with established procedures for introducing and attaching new devices to the network.

O.E.DIGITAL_COPIER - The environment into which the TOE will be introduced shall contain an Océ VarioPrint 2090 that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE. When sending a D.SECURE_PRINT_JOB or D.PRINT_JOB to the Smart Imager, S.REMOTE_USER is aware that they must delete the job on the same workday that it is sent to the TOE, whether or not it is printed. The MFD provides a glass plate and LUI with which S.LOCAL_USER can perform scan jobs. The ST claim is not valid when the TOE is used with any other type of Océ MFD. The TOE will not work with any other device (including Digital MFD Products from any other manufacturers).

O.E.SHREDDING – The customer requires the shredding of D.SECURE_PRINT_JOB, D.PRINT_JOB, D.COPY_JOB and D.SCAN_JOB data objects.

A.SHREDDING

The assumption is met by the following objectives for the environment:

O.E.SHREDDING – The customer requires the shredding of D.SECURE_PRINT_JOB, D.PRINT_JOB, D.COPY_JOB and D.SCAN_JOB data objects.

A.SLA

The assumption is met by the following TOE assurance objective:

O.A.SLA - The TOE shall be evaluated to ALC_FLR.1.There are measures in place to repair faults in the TOE when they occur.

T.RESIDUAL_DATA

The threat is met by the following TOE functional objective:

O.F.JOB_SHRED - The TOE shall delete all D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB data as soon as it is no longer required or during the start-up procedure if residual D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB is found on the TOE's hard disk (including the swap file). The first write cycle starts immediately after the job has deleted and the rest are completed once the TOE enters an idle state. The data shall be deleted according to a recognised standard so that it cannot be reconstituted.

'Scrubbing' the data from the hard disk when it is no longer needed helps prevent the data been accessed by unauthorised persons.

T.NOSY_USER

The threat is met by the following TOE functional objective:

O.F.JOB_RELEASE - The TOE shall only perform R.RELEASE_JOB once S.LOCAL_USER has successfully identified and authenticated himself as owner of D.SECURE_PRINT_JOB.

By first requiring a print job owner to identify an authenticate himself before printing can commence, observation of print job related data by casual users is prevented.

T.MALWARE

The threat is met by the following objectives for the environment:

O.F.INBOUND_FILTER - The TOE will only support TCP/IP, UDP/IP and ICMP as a network protocol. D.INBOUND_TRAFFIC shall only enter the TOE (R.ENTER_TOE) if the Port is specified as being open in Appendix D.

The chances of mal-ware being accidentally sent to the TOE and causing a security violation is limited by only opening the ports and enabling the protocols that are absolutely necessary for the operation of the TOE.

Although the TOE is designed, tested and configured with security as a main concern, it is possible that vulnerabilities will be discovered in the future that could be exploited in order to use the TOE as a launch pad for an attack. By only opening the ports and enabling the protocols that are absolutely necessary for the operation of the TOE, the chances of a successful attack launch are limited.

P.JOB_DELETE

The policy requirement is met by the following TOE functional objective:

The threat is met by the following TOE functional objective:

O.F.JOB_SHRED - The TOE shall delete all D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB data as soon as it is no longer required or if during the start-up procedure residual D.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB is found on the TOE's hard disk (including the swap file). The first write cycle starts immediately after the job has deleted and the remaining cycles are completed once the TOE enters an idle state. The data shall be deleted according to a recognised standard so that it cannot be reconstituted

'Scrubbing' the data from the hard disk when it is no longer needed helps prevent the data been accessed by unauthorised persons.

P.TOE_ADMINISTRATION

The policy requirement is met by the following TOE functional objective:

O.F.AUTHENTICATE - The TOE ensures that S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER must identify and authenticate themselves to the TOE before allowing them to modify the TOE security settings.

8.2 Security Requirements Rationale

The purpose of the Security Requirements Rationale is to demonstrate that the security requirements are suitable to meet the Security Objectives.

8.2.1 The SFRs meet the Security Objectives for the TOE

For each Security Objective for the TOE we demonstrate that it is met by the SFRs. The tracings are provided implicitly by the rationales.

	FDP ACC1.	FDP ACF.1	FIA UID.1	FIA UAU.1	FDP RIP.1	FIA UID.2	FIA UAU.2	FMT MOF.1	FMT MSA.1	FMT MSA.3	FMT SMF.1	FMT SMR.1	FPT SEP.1	FPT RVM.1
O.F.INBOUND_FILTER	X	X							X	X			X	X
O.F.JOB_RELEASE			X	X									X	X
O.F.JOB_SHREAD					X								X	X
O.F.AUTHENTICATE						X	X	X			X	X	X	X

The individual rationales demonstrating the objectives are met are described as follows:

O.F.INBOUND_FILTER

FDP_ACC.1 Subset access control

Inbound traffic is filtered so that only traffic relating to the operation of the TOE is allowed to enter the TOE. This SFR supports the security objective by restricting the TOE data flow to only that that is necessary for the operation of the TOE. This reduces the number of vulnerable entry points.

FDP_ACF.1 Security attribute based access control

All ports that are not necessary for the operation of the TOE as described in this document are blocked. This SFR supports the security objective by reducing the number of entry points that could be vulnerable to attack.

FMT_MSA.1 Management of security attributes

The TOE is delivered pre-configured to the customer. This SFR supports the objective by ensuring that it is not possible for any user (including S.SERVICE_ENGINEER and S.REMOTE_SYSADMIN) to change the settings of the firewall mechanism.

FMT_MSA.3 Static Attribute initialisation

In order to change the security attributes of the TOE the management interfaces provided for S.SERVICE_ENGINEER and S.REMOTE_SYSADMIN must be used. This SFR supports the objective by ensuring that the TOE provides restrictive default security related settings that require no additional modification by SERVICE_ENGINEER or S.REMOTE_SYSADMIN. Nobody is allowed to create new settings with alternative values.

FPT_RVM.1 Non-bypassability of the TSP
In order for data to enter or leave the TOE it must pass through the filtering mechanism. This SFR supports the security objective by ensuring that TSF cannot be bypassed, resulting in a direct line between the network to which the TOE is attached and the TOE being created.

FPT_SEP.1 TSF domain separation
Filtering of network traffic occurs is an area of the TOE that is separate to non-TSF related operation. This SFR supports the objective by ensuring that the filtering mechanism is protected by it not being exposed to non TSF mechanisms from which a possible attack could be made.

O.F.JOB_RELEASE
FIA_UID.1 Timing of identification (Secure Printing)
Printing will only commence once the TSF has validated the Username associated with the job by S.LOCAL_USER. The TSF receives the Username via the Smart Imager LUI interface. This SFR supports the security objective by requiring the S.LOCAL_USER to identify himself as part of the job release process.

FIA_UAU.1 Timing of authentication
Printing will only commence once the TSF has validated the PIN associated with the job by S.LOCAL_USER. The TSF receives the PIN via the Smart Imager LUI interface. This SFR supports the security objective by requiring the S.LOCAL_USER to authenticate himself as part of the job release process.

FPT_RVM.1 Non-bypassability of the TSP
Print jobs cannot be processed by any other mechanism than by the specified mechanism. This SFR supports the objective by ensuring that no other mechanisms can access the print job data.

FPT_SEP.1 TSF domain separation
Management of print jobs occurs in an area of the TOE that is separate to non-TSF related operation. This SFR supports the objective by ensuring that the job release mechanism is protected by it not being exposed to other non-TSF mechanisms from which a possible attack could be made.

O.F.JOB_SHRED
FDP_RIP.1 Subset residual; information protection
This SFR supports the objective by ensuring that once print, copy or scan job is no longer needed and during the startup procedure, if residual print or scan job data is

found then the related data will be electronically shredded from the hard disk. The SFR has been refined to describe the moment when the data will be shredded.

FPT_RVM.1 Non-bypassability of the TSP
Print and scan jobs must pass through the shredding mechanism. This SFR supports the objective by ensuring that print and scan jobs cannot leave the TOE except in the authorised manner.

FPT_SEP.1 TSF domain separation
Shredding occurs is an area of the TOE that in separate to non-TSF related operation. This SFR supports the objective by ensuring that the shredding mechanism is protected by it not being exposed to other non TSF-mechanisms from which a possible attack could be made.

O.F.AUTHENTICATE
FIA_UID.2 User identification before any action
S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER must identify themselves to the TOE before any TOE management actions can be performed.

FIA_UAU.2 User authentication before any action
S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER must authenticate themselves to the TOE before any TOE management actions can be performed.

FMT_SMF.1 Specification of Management Functions
The functions that can be performed by either the S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER are defined.

FMT_MOF.1 Management of security functions behaviour
Only TOE administrators and Océ technicians can use security related functions.

FMT_SMR.1 Security roles
The TOE shall make a distinction between administrators and ordinary users.

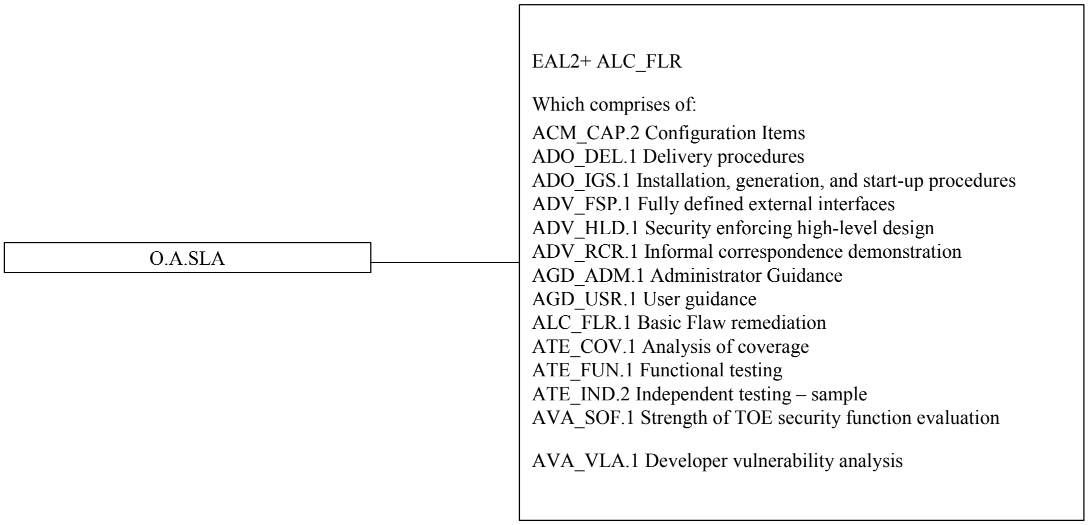
FPT_RVM.1 Non-bypassability of the TSP
Users other than S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER cannot gain access to security management functions of the TOE without begin first controlled by the mechanisms specified in this document.

FPT_SEP.1 TSF domain separation
Identification and authentication of users occurs in an area of the TOE that is separate to non-security related operation.

8.2.2 The security requirements for the IT environment meet the security objectives for the environment

The TOE does not make any security requirements on its environment.

8.2.3 The Assurance Requirements and Strength of Function Claim are appropriate



O.A.SLA

EAL2+ ALC_FLR

Which comprises of:

ACM_CAP.2 Configuration Items
ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Fully defined external interfaces
ADV_HLD.1 Security enforcing high-level design
ADV_RCR.1 Informal correspondence demonstration
AGD_ADM.1 Administrator Guidance
AGD_USR.1 User guidance
ALC_FLR.1 Basic Flaw remediation
ATE_COV.1 Analysis of coverage
ATE_FUN.1 Functional testing
ATE_IND.2 Independent testing – sample
AVA_SOF.1 Strength of TOE security function evaluation

AVA_VLA.1 Developer vulnerability analysis

The Assurance Requirements consist of EAL 2 requirements components. The TOE is a commercially available device produced by a well-known manufacturer and most importantly, provides a limited set of security related functionality. The TOE has been structurally tested by Océ and is suitable for environments that require a low to moderate level of independently assured security. The developer works in a consistent manner with good commercial practice.

Occasionally the TOE may develop a problem that requires S.SERVICE_ENGINEER to make a visit to the customer location in order to repair the TOE. Océ has procedures that support these processes and for this reason the assurance requirements have been augmented with the following assurance classes as the developer is able to meet them:

Components for Life cycle support (Class ALC)

- ALC_FLR.1 Basic Flaw Remediation

The evaluation of the TOE security mechanisms at AVA_VLA.1 is designed to provide assurance the exploit of obvious vulnerabilities by an attacker with a low attack potential. Therefore the SOF claim is SOF-basic. This strength of function claim is consistent with the security objectives for the TOE and the defined TOE assumptions that have been made.

8.2.4 All dependencies have been met

The following dependencies are identified and met: FDP_ACF.1, FDP_ACC.1, FMT_MSA.1, FMT_MSA.3, FIA_UID.1, FIA_UID.2, FMT_SMF.1, FMT_SMR.1.

8.2.5 The requirements are internally consistent

Because the assurance requirements form a package (EAL 2) they are internally consistent. The addition of ALC_FLR.1 does not cause inconsistencies with the EAL 2 package.

The functional requirements and assurance requirements do not have any dependencies between them, and are therefore completely independent of each other. Because both functional and assurance requirements are internally consistent, and they are independent, the requirements are internally consistent.

8.2.6 The requirements are mutually supportive

The requirements are complete and do not cause inconsistencies, therefore the requirements are considered to be mutually supportive. (This argument has been based on section 9.3.8 of Guide for the production of PPs and STs, PDTR 15446 N2449)

8.3 TOE Summary Specification Rationale

8.3.1 The functions meet the SFRs

For each SFR we demonstrate that it is met by the Security Functions. The tracings are provided implicitly by the rationales.

	FDP ACC1.	FDP ACF.1	FIA UID.1	FIA UAU.1	FDP RIP.1	FIA UID.2	FIA UAU.2	FMT MOF.1	FMT MSA.1	FMT MSA.3	FMT SMF.1	FMT SMR.1	FPT SEP.1	FPT RVM.1
SF.FILTERING	X	X							X	X			X	X
SF.JOB_RELEASE			X	X									X	X
SF.SHREDDING					X								X	X
SF.MANAGEMENT						X	X	X	X	X	X	X	X	X

FDP_ACC.1
This Security Functional Requirement ensures that only traffic is allowed to enter the TOE that is relevant to its operation. This SFR is supported by SF.FILTERING that restricts flow of network traffic and limits the supported network protocols.

FDP_ACF.1
This Security Functional Requirement ensures that all ports that are non-essential to the operation of the TOE are blocked. This SFR is supported by SF.FILTERING. SF.FILTERING expands on the restricted flow of network traffic and supported network protocols by defining which ports are open and which protocols are supported.

FIA_UID.1
This Security Functional Requirement ensures that the TSF verifies the identity of S.LOCAL_USER before allowing SF.JOB_RELEASE. This helps to ensure that access to confidential print jobs is restricted.

FIA.UAU.1
This Security Functional Requirement ensures that the TSF authenticates S.LOCAL_USER by correctly supplying the PIN associated with the secure print job before SF.JOB_RELEASE will commence. This helps to ensure that access to confidential print jobs is restricted.

FDP_RIP.1
This Security Functional Requirement ensures requires that residual information relating to D.SECURE_PRINT_JOB, D.PRINT_JOB, D.COPY_JOB and D.SCAN_JOB is deleted once they are no longer needed or during the startup procedure, if residual print or scan job data is found on the hard disk (including the swap file). The SFR has been refined to describe the moment when the data will be shredded. This SFR is supported by SF.SHREDDING that provides functionality that ensures the data objects detailed above are shredded in accordance with known standards. This SFR helps to reduce the amount of sensitive data present on the hard disk in the event of it being stolen.

FIA_UID.2
This Security Functional Requirement ensures that administrators correctly identify themselves to the TOE before security management functions can be used. This SFR is supported by SF.MANAGEMENT and provides functionality whereby administrators (S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER) can identify themselves to the TOE. This helps to restrict access to security management functions and thereby reduces the risk of modification being made to the TOE settings by unauthorised users.

FIA_UAU.2
This Security Functional Requirement ensures that administrators correctly authenticate themselves to the TOE before security management functions can be used. This SFR is supported by SF.MANAGEMENT and provides functionality whereby administrators (S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER) can authenticate themselves to the TOE. This helps to restrict access to security management functions and thereby reduces the risk of modification being made to the TOE settings by unauthorised users.

FMT_MOF.1
This Security Functional Requirement ensures that the TOE management functions are only used by either the Océ technician (S.SERVICE_ENGINEER) or customer system administrator (S.REMOTE_SYSADMIN). This SFR is supported by SF.MANAGEMENT and ensures that non-administrators cannot administer the TOE.

FMT_MSA.1
This Security Functional Requirement ensures that the TOE management functions related to the filter mechanism settings cannot be changed. This SFR is supported by SF.MANGEMENT that ensures that filter related settings cannot be changed by administrators.

FMT_MSA.3

This Security Functional Requirement ensures that the TOE management functions related to the filter mechanism settings are given default values. This SFR is supported by SF.MANAGEMENT that ensures that the filter related settings are pre-configured before delivery to the customer.

FMT_SMF.1

This Security Functional Requirement ensures that the TOE management functions are defined. This SFR is supported by functions made available by SF.MANAGEMENT and defines the set of operations that are available to the Océ technician (S.SERVICE_ENGINEER) or customer system administrator (S.REMOTE_SYSADMIN) that are needed to administrate the TOE.

FMT_SMR.1

This Security Functional Requirement ensures that the TOE makes a distinction between security related roles and normal users. This SFR is supported by SF.MANAGEMENT. This SFR is supported by SF.MANAGEMENT and ensures that non-administrators cannot administer the TOE.

FPT_SEP.1

This Security Functional Requirement ensures that the TSF operates in its own domain and cannot be influenced by external sources. This requirement is met by the physical characteristics of the TOE that comprises software that uses a generic PC hardware platform. The Smart Imager only provides functionality related to the operation of the TOE and does not have dual function, for example, as an office file server. The nature of the TOE is such that evaluation at EAL2 provides a suitable level of assurance that the TSF operates in it's own domain.

The operation of the TSF in its own domain provides the following:

1. The filtering mechanisms are in a separate domain to the rest of the non-security related operations that the TOE performs. This SFR is supported by SF.FILTERING. This protects the integrity of the filtering mechanism against un-authorised subjects and threat attacks.
2. The shredding mechanisms are in a separate domain to the rest of the non-security related operations that the TOE performs. This SFR is supported by SF.SHREDDING. This protects the integrity of the shredding mechanism against un-authorised subjects and threat attacks.
3. The TOE security management mechanisms are in a separate domain to the rest of the non-security related operations that the TOE performs. This SFR is supported by SF.MANAGEMENT. This protects the integrity of the security management mechanisms against un-authorised subjects and threat attacks.

FPT_RVM.1

This Security Functional Requirement ensures that no security related operations can be performed without being controlled by the TOE's security mechanisms. The Smart Imager provides a limited set of security functionality that is related to the operation of the TOE. The nature of the TOE is such that evaluation at EAL2 provides a suitable level of assurance that the only the TSF can perform security related operations.

This SFR is supported by SF.MANAGEMENT.
This Security Functional Requirement ensures that:

1. No filtering mechanisms can be performed without being controlled by the TOE's security mechanisms. This SFR is supported by SF.FILTERING.
2. No secure print job management mechanisms can be performed without being controlled by the TOE's security mechanisms. This SFR is supported by SF.JOB_RELEASE.
3. No shredding mechanisms can be performed without being controlled by the TOE's security mechanisms. This SFR is supported by SF.SHREDDING.
4. No security related operations can be performed without being controlled by the TOE's security mechanisms. This SFR is supported by SF.MANAGEMENT.

8.3.2 The assurance measures meet the SARs

The statement of assurance measures has been presented in the form of a reference to the documents that show that the assurance measures have been met (CC Part 3 paragraph 188). This statement can be found in section 6.2.

8.3.3 The SOF-claims for functions meet the SOF-claims for the SFRs

The SFRs FIA_UAU.1, FIA_UAU.2, FIA_UID.1 and FIA_UID.2 require the TOE to provide security functions that provide identification/authentication functionality that meets a SOF claim of 'SOF basic'.

This rational for this is that the claim must adequate to defend against the identified threats to the TOE that are identified in the TOE Security Environment for which a low attack potential exists

The Security Functions that are realised by probabilistic or permutational mechanisms are:

- SF.JOB_RELEASE
- SF.MANAGEMENT

The claim for these two Security Functions is 'SOF basic'. These Security Functions are traced back to the TOE SFRs they implement in 8.3.1

As the SOF claims for the three Security Functions are equal to the SOF claims for the TOE SFRs they implement, the SOF claims are consistent.

8.3.4 The functions are mutually supportive

The requirements are mutually supportive (see section 8.2.6) and the functions that implement theses requirements are complete (see section 8.3.1). The functions are mutually supportive. (This argument has been based on section 9.3.8 of Guide for the production of PPs and STs, PDTR 15446 N2449)

8.4 PP Claims Rationale

This Security Target TOE does not claim conformance to any Protection Profile.

Appendix A Abbreviations

BSI	Bundesamt für Sicherheit in der Informationtechnik
ITSEF	IT Security Evaluation Facility
LUI	Local User Interface (attached to the Smart Imager via a USB connection)
MFD	Multifunctional device for copying, printing and scanning, connected to a network
TNO	Netherlands Organization for Applied Scientific Research

Appendix B References

1. Secure Deletion of Data from Magnetic and Solid State Memory, Peter Guttman 1996 (http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)
2. US Department of Defence Military Standard DOD 5220-22m (http://www.dss.mil/isecnispom_0195.htm)

.

Appendix C Glossary of Terms

None.

Appendix D Firewall rule table

The firewall rule table that is used by the Smart Imager for controlling the inbound flow of data is given below:

By default no traffic is permitted to enter or leave to TOE except for the ports defined in the rule tables below.

ICMP(administration)

Protocol	*Destination Port*
ICMP	any

DNS (administration)[14]

Protocol	*Destination Port*
UDP	>1023

DHCP (administration)

Protocol	*Destination Port*
UDP	68

LPR (accepting print jobs)

Protocol	*Destination Port*
TCP	515

Web HTTPS server with HTTP redirect (administration)

Protocol	*Destination Port*
TCP	443
TCP	80

IPSEC (Windows 2000 port filtering)

Protocol	*Destination Port*
UDP	500

SNMP (non security functionality related administration)

Protocol	*Destination Port*
UDP	161

[14] Additionally the Smart Imager can filter on the IP address of the DNS server and block all DNS traffic from IP addresses that do not match the specified IP address

Appendix E Security Related Administration Functions

In this appendix the security related administration functions that are available to S.SERVICE_ENGINEER and S.REMOTE_SYSADMIN are detailed. The tables give the administration function name and a short description

S.SERVICE_ENGINEER

Administration Function	Description
ResetSASPassword	Resets the S.REMOTE_SYSADMIN password to its default value
Filtering of web server ports	Enable/disable web traffic on LAN interface (must not be disabled in the evaluated configuration)

S.REMOTE_SYSADMIN & S.SERVICE_ENGINEER

Administration Function	Description
Security\Security level\enable high level	Enable/disable switch for high security level (This must not be changed if the customer requires the CC evaluated configuration)
Security\E-shredding\Configure	On/off E-shredding switch (must be left on in the evaluated configuration)
Security\E-shredding\Method	Shredding method (Dod, Guttmann, custom)
Security\E-shredding\Number of runs	Number of runs from 1 to 35 (not allowed to be set to under 3 in the evaluated configuration)
Security\E-shredding\Sensitive jobs	definition job categories to shred (all job types are to be shred in the in the evaluated configuration and must be left enabled)
Security\Secure Protocols	selection HTTPs/HTTP (HTTPS must not be disabled in the evaluated configuration)
System\System administrator PIN	change S.REMOTE_SYSADMIN password
Protocols\ TCP/IP\Secure filtering of DNS ports	enable use of DNS server IP info for port filtering

Distribution list

1. BSI
2. Océ Technologies BV
3. TNO-ITSEF B.V