Océ Technolgies B.V.

ST-Océ DAC-1.6

Security Target
The Océ Digital Access Controller (DAC) v7.3.6, as used in the Océ VarioPrint 2045, 2050, 2055, 2060, 2065, 2070, 3145, 3155, 3165 printer/copier/scanner products

Version	1.6
Date	1st December 2004

Certification ID	BSI-DSZ-CC-0268
Sponsor	Océ Technologies B.V.
File name	Oce Venlo DAC Security Target 1.6.doc
No of pages	64

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

by TNO-ITSEF B.V.

Document information

Date of issue	1st December 2004
Author(s)	Rob Hunter, Dirk-Jan Out
Version number report	1.6
Certification ID	BSI-DSZ-CC-0268
Scheme	BSI
Sponsor	Océ Technologies B.V. 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
Target of Evaluation (TOE)	The Océ Digital Access Controller (DAC) v7.3.6, as used in the Océ VarioPrint 2045, 2050, 2055, 2060, 2065, 2070, 3145, 3155, 3165 printer/copier/scanner products
TOE reference name	Océ DAC
CC-EAL number	2+ (augmented with ALC_FLR.1)
Classification	None
Report title	Security Target The Océ Digital Access Controller (DAC) v7.3.6, as used in the Océ VarioPrint 2045, 2050, 2055, 2060, 2065, 2070, 3145, 3155, 3165 printer/copier/scanner products
Report reference name	ST-Océ DAC-1.6

Document history

Version	Date	Comment
0.2	14-10-03	Initial draft
0.3	17-10-03	Added initial comments from TNO-ITSEF BV
0.4	28-10-03	Added comments from Océ
0.5	06-11-03	Added comments of Océ resulting from meeting
0.6		Added telephone comments from JB
0.7	17-11-03	Further expansion of versions 0.5 and 0.6
0.8	1-12-03	SFR's added and comments from Océ included
0.9	20-2-04	Added comments from Océ
1.0	2-3-04	Initial release (unevaluated)
1.1	28-5-04	Modified after initial CC evaluation round with comments from evaluators and from BSI
1.2	17-6-04	Modified after second CC evaluation round
1.3	25-08-04	Modified after comment BSI (Rev Prot 3)
1.4	23-09-04	Modified after comment BSI (Rev Prot 12)
1.5	30-11-04	Modified after comment BSI (Rev Prot 23)
1.6	01-12-04	Modified after comment BSI (Rev Prot 23)

Contents

1. Security Target Introduction

1.1 ST Identification

Name of the TOE:
The Océ Digital Access Controller (DAC) v7.3.6,
as used in the Océ VarioPrint
2045, 2050, 2055,
2060, 2065, 2070,
3145, 3155, 3165 printer/copier/scanner products

Name of the Security Target:
Security Target
The Océ Digital Access Controller (DAC) v7.3.6,
as used in the Océ VarioPrint
2045, 2050, 2055,
2060, 2065, 2070,
3145, 3155, 3165 printer/copier/scanner products

ST evaluation status: Evaluated Release
ST version number: 1.6
ST publication date: 1st December 2004
ST authors: Rob Hunter, Dirk-Jan Out

This Security Target was prepared for:
Océ Technologies B.V.
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. A number of these MFDs: the 2045/55/65 series, the 2050/60/70 series and the 31x5 series, use the same Digital Access Controller (DAC).

The Océ Digital Access Controller (DAC) v7.3.6, is used with the Océ VarioPrint

- 2045, 2050, 2055,
- 2060, 2065, 2070,
- 3145, 3155, 3165.

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

A digital copier from the Océ 2045/55/65 series with optional embedded DAC or external DAC.	
A digital copier from the Océ 2050/60/70 series with either an embedded or external DAC.	

A digital copier from the Océ 31x5 series pictured with optional external DAC	

For external DACs, an optional ‘removable hard disk’ is available.

The DAC is a PC-based MFD-controller that provides a wide range of printing and scanning functionality to the Digital Copier (DC) of the MFD to which the DAC is connected. The DAC provides security functionality to the DC, the DAC does not provide copy functionality.

This Security Target describes the DAC and the specific security problem that it addresses. The Target of Evaluation (TOE) is a collection of software components (printer drivers, OS) that use the underlying hardware platform. The TOE is a subset of the complete DAC.

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, MFDs consist of two main parts: a controller and a Digital Copier (DC).

A number of these MFDs use the same controller: the Digital Access Controller (DAC).

The DAC is a PC-based MFD-controller that provides a wide range of printing and scanning functionality to the Digital Copier (DC) of the MFD to which the DAC is connected. The DAC provides security functionality to the DC. It does not provide copy functionality.

The DAC can operate in three different security modes: ‘high’, ‘normal’ and ‘low’. This Security Target covers the DAC 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 DAC is connected between a network and the DC. This is depicted in Figure 1.

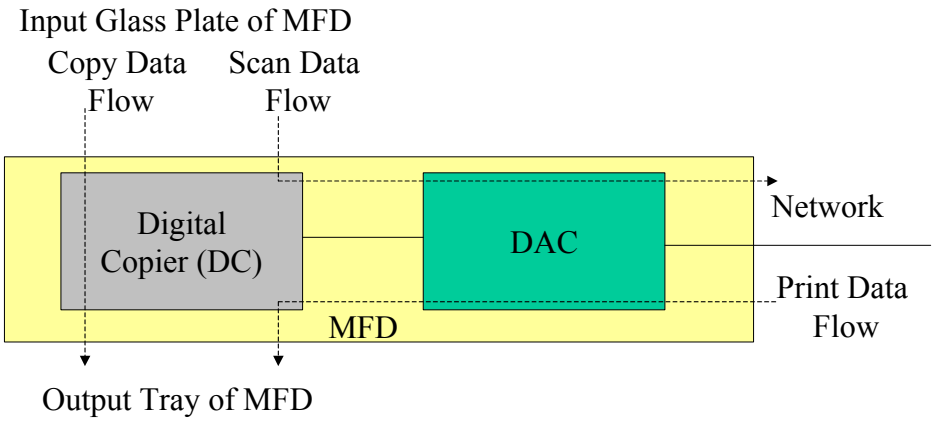


Figure 1: Relation between DC, DAC and MFD

Two physical configurations exist of the MFD: one where the DAC is external to the MFD, and one where it is internal to the MFD. These are depicted in Figure 2.

Figure 2: Views of the internal and external DAC controllers.

The internal configuration helps prevent theft of the DAC, but prevention of theft of the DAC is outside the scope of this evaluation[1]. All logical access points (CD-Rom, floppy drives, network ports, USB/serial/parallel ports etc. are fully physically accessible in the internal configuration. For the purpose of this evaluation, the two configurations are therefore identical.

[1] Note that the DAC does protect data stored in it against theft through e-shredding, but the DAC itself may be stolen.

The DAC consists of:

1. A generic off-the-shelf PC comprising at a minimum a 900Mhz Celeron processor, 128MB internal RAM, 15GB hard drive, one serial port, internal floppy and CDROM drive.
2. Generic graphics card and network card supporting either 10/100Mbs Ethernet UTP or 4/16Mbs Token Ring.
3. Drivers for the PC, graphics card and network card
4. The OS/2 operating system version 4.5.2
5. Océ DAC-specific software version 7.3.6
6. Third-party developed software: Adobe PS3-PDF Interpreter, Version 3011.106 build #35; Apache HTTP server with SSL support, Apache 1.3.29, OpenSSL 0.9.7c, mod_ssl 2.8.16.

Of these 6, the first three 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 3.

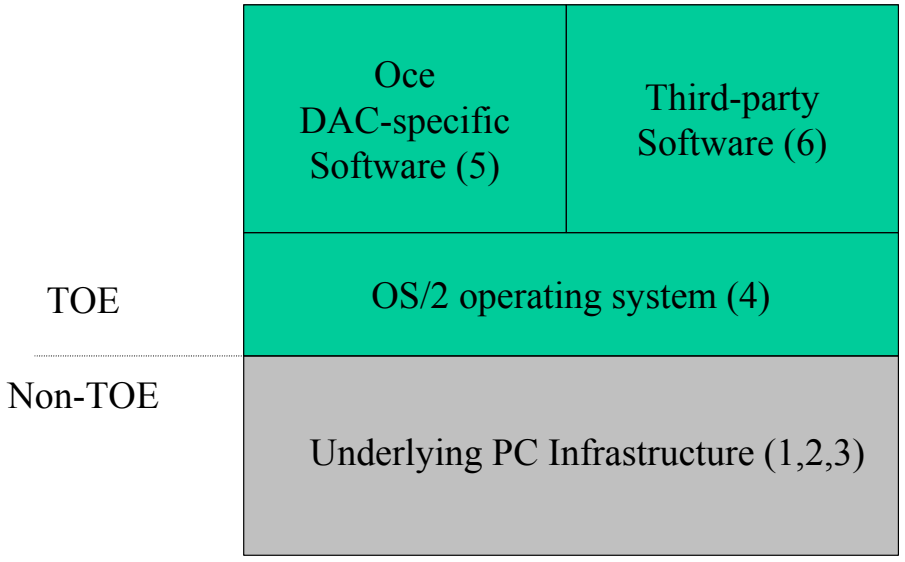


Figure 3: Division of the DAC into TOE and non-TOE.

The underlying PC hardware platform has the following characteristics:

- The CDROM is only used by the service engineer to install new software.
- The floppy is not used for any security related functions.
- The serial port is only used by the service engineer.
- All other interfaces, such as they keyboard or USB ports, have been disabled.

The physical interfaces through which the TOE communicates are:

- A serial port with a RS-232 connector 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 Digital Copier (DC) cable through which data flows between the TOE and the DC.

The user guidance for the TOE consists of :

- Océ VarioPrint 2045-65 Job manual, Code number 1060015271 - Edition 05-2004
- Océ VarioPrint 2050-70 Job manual, Code number 1060015031 - Edition 05-2004
- Océ 31x5E Job manual, Code number 1060015075 - Edition 05-2004
- Océ VarioPrint 2045-65 Configuration manual, Code number 1060015272 - Edition 05-2004
- Océ VarioPrint 2050-70 Configuration manual, Configuration Manual - Code number 1060015018 -Edition 05-2004
- Océ 31x5E Configuration manual, Code number 1060015062 - Edition 05-2004

The administrator guidance for the TOE consists of:
The DAC administration guidance for the customer system administrator takes the form of HTML pages. These are part of the Océ DAC-specific software, Version 7.3.6 release and is identified in the 'About this help' section as:

- Océ System Configuration, version 2.3, On-line help, revision 2004.

The DAC administration guidance for the Océ service engineer takes the form of a Lotus Notes application that is installed on the service engineer's laptop. The guidance contains an appendix that is identified as:

- Administrating version 7.3.6. of the Océ DAC, Version 1.0, June 2004

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

2.1.2 TOE logical scope and boundary

The TOE protects two assets: itself and the print jobs it receives.

1. The TOE protects it's own integrity against threats from the LAN and the Digital Copier to which it is attached through use of a firewall and integrity checks on system files upon system reboot.
2. The TOE protects the confidentiality of secure print jobs once they have been received by the DAC by storing them until the user authenticates

himself to the DAC via a user interface on the DC. The DAC shreds the data after printing is completed.

The TOE does not form a threat to its environment for the following reasons:

- The TOE does not form a threat to the integrity of the LAN to which the DAC is attached. The TOE configuration has been tested and is configured so that the integrity of the configuration is checked and restored upon system reset.
- Additionally, all data that enters the TOE via the Digital Copier must pass through an internal firewall. There is no direct line from the Digital Copier to the network to which the DAC is attached.

In order to do so, it offers the following functionality[2]:

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 DC. The TOE can print these jobs in three 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 DC 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 DC (become a local end-user) and identify himself at the Local User Interface of the DC (LUI). Only after this, will the TOE process the job. The resulting images are sent to the attached DC 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 PINcode that has a length of 4 to 6 digits to the job.
- The PINcode is stored in the DAC.
- When identifying himself at the LUI of the DC, the local end-user also has to provide the job-specific PINcode. The DC interrogates the DAC as to the validity of the PIN. If correct, the print job data is released by the DAC and is sent to the DC. A replay attack with an intercepted PIN is countered

[2] The DC can also perform copying, but this is done without interaction with the TOE. Copy job related data does not enter the TOE boundary. This is therefore out-of-scope of this ST.

by shredding the print job data immediately after the print job is completed.

The end-users and interfaces they interact with are depicted in Figure 4.

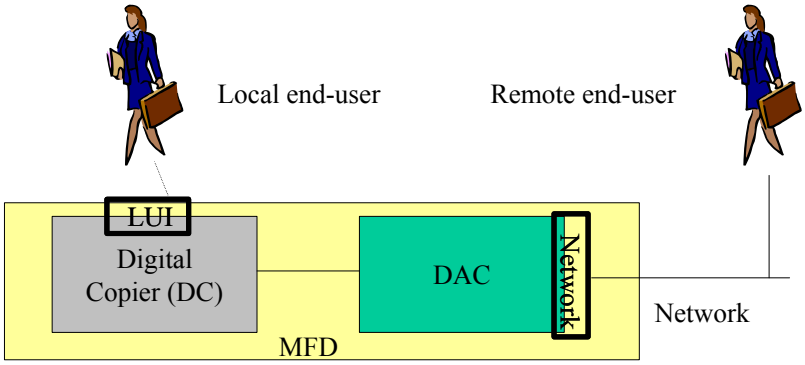


Figure 4: End-users and interfaces for printing

The TOE is configured to destroy the data relating to secure print jobs (print jobs submitted to the mailbox with an associated PIN), non-secure print jobs, scan jobs and temporary files.

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 and at what moment the shredding takes place. The first iteration takes place after the data is released. The remaining iterations can take place immediately (synchronous) or with low priority in the background (asynchronous).

The TOE administers scan jobs that are exported to the network
Local end-users can scan documents on the DC, 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 on the network.

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

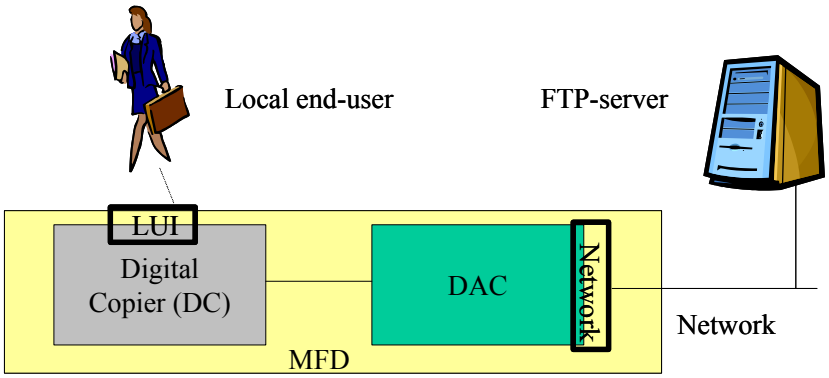


Figure 5: End-users and interfaces for scanning

The TOE is configured to destroy the data relating to secure print jobs (print jobs submitted to the mailbox with an associated PIN), non-secure print jobs, scan jobs and temporary files.

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

The user can select the number of write iterations and at what moment the shredding takes place. The first iteration takes place after the data is released. The remaining iterations can take place immediately (synchronous) or with low priority in the background (asynchronous).

The TOE can also be configured to shred all data after a specific time interval, e.g. once every 24 hours.

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:

Key Operator: These are typically administrators or secretaries from the organization owning/renting the TOE. They can interact with the DC through the LUI, and through this interaction have access to a limited amount of non-security related settings of the TOE.

Remote System administrator: These are remote administrators, typically a network administrator from the organization owning/renting the TOE. They can read a limited set of settings of the TOE through a SNMP connection, and they can change a less 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'.

Service engineer: These are local administrators, and are typically employed by Océ. They have access through RS-232 connections to a wide range of settings on the TOE and the DC. The TOE connection is PIN code protected.

The various administrators and the interfaces through which they interact with the TOE are depicted in Figure 6.

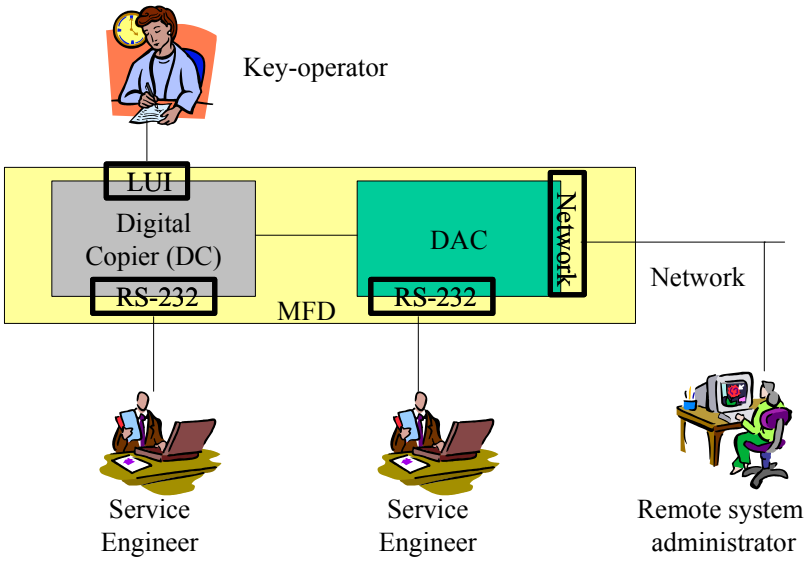


Figure 6: MFD Administrators and interfaces

The TOE has minimized all other functionality
The TOE supports TCP/IP: all other network protocols are disabled. The TOE manufacturer has closed all network ports except those that are absolutely necessary to its functioning. This includes the physical connectors on the TOE. 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 6, The Key Operator is not able to influence the security of the TOE as they have no access to security settings via the DC. The Service Engineer cannot influence the security of the TOE via the interface to the DC.

Because the Key Operator and Local End-User cannot access security related settings on the DAC, they cannot affect the TOE. For the sake of clarity, Figure 7 shows the interfaces to the TOE and the subjects that can access and manage TOE security settings.

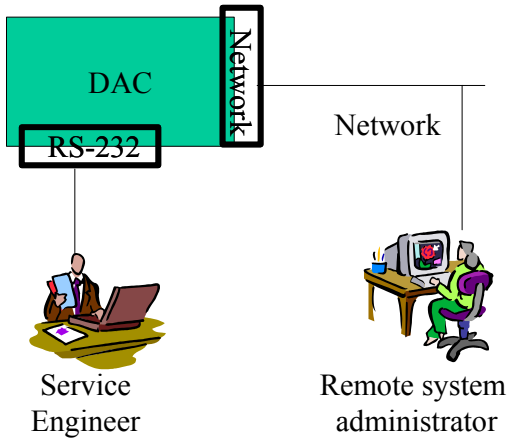


Figure 7: TOE Administrators and interfaces

3. TOE Security Environment

The TOE is intended to provide scan and print 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_COPIER	A device that physically renders a print job or scans in a job and is attached to the TOE via a cable.
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. They may be interested in the content of other users' print jobs. S.LOCAL_USER typically interacts indirectly with the TOE via S.DIGITAL_COPIER
S.REMOTE_SYSADMIN	A person who can change some TOE settings using a Océ supplied interface. They are trusted by the

	customer and are adequately trained. They are capable of making mistakes. They connect to the TOE via the network.
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 an RS232 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 and scanner jobs from the TOE. S.THIEF is not able to steal Copy jobs[3] as they never enter 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.LOCAL_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 non D.SECURE_PRINT_JOB type print job submitted by S.REMOTE_USER to the TOE.
D.SCAN_JOB	Data that is scanned in via the DC attached to the DAC. Data is sent from the TOE to a FTP server located elsewhere on the network.
D.INBOUND_TRAFFIC	TCP/IP network packets received by the TOE. D.INBOUND_TRAFFIC has the Security Attributes *Port* and *Protocol* associated with it.
D.OUTBOUND_TRAFFIC	TCP/IP network packets sent by the TOE. D.OUTBOUND_TRAFFIC has the Security Attributes *Port* and *Protocol* associated with it.

[3] See Figure 1: Relation between DC, DAC and MFD.

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 DC.
R.PRINT_JOB	The TOE processes and releases a D.PRINT_JOB to the attached DC.
R.SHRED_JOB	The TOE shreds redundant D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB data objects from the TOE's hard disk.
R.ENTER_TOE	The TOE allows D.INBOUND_TRAFFIC to enter its boundary.
R.EXIT_TOE	The TOE allows D.OUTBOUND_TRAFFIC to leave its boundary.

3.2 Assumptions

A.DIGITAL_COPIER	It is assumed that the TOE has a S.DIGITAL_COPIER device attached to it. S.DIGITAL_COPIER is an Océ VarioPrint 2045-65, 2050-70 or 31x5 Digital Copier. When D.SECURE_PRINT_JOB is sent to S.DIGITAL_COPIER, R.REMOTE_USER will specify a PIN of at least 4 and a maximum of 6 digits and, whether the job is printed or not, will delete the job on the same workday. Employees are aware of this requirement.
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.SHREDDING	The TOE assumes that the customer will not disable the shredding operation for D.PRINT_JOB and D.SCAN_JOB data objects[4].
A.SLA	It is assumed that any security flaws discovered in the TOE will be repaired by OCE (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. 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 DAC. The motivation to carry out this attack is low.

[4] The TOE shreds D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB by default when printing/scanning is completed in the delivered mode. It is possible to disable shredding for D.PRINT_JOB and D.SCAN_JOB. If this happens, the TOE claim is no longer valid.

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. Alternatively S.DIGITAL_COPIER is used by malware to launch an attack on the integrity of S.NETWORK_DEVICE. The motivation to carry out this attack is low.

3.4 Organisational Security Policies

P.JOB_DELETE	When D.SECURE_PRINT_JOB, D.PRINTJOB and D.SCANJOB 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.

[5] The TOE shreds D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB by default when printing/scanning is completed in the delivered mode. It is possible to disable shredding for D.PRINT_JOB and D.SCAN_JOB. If this happens, the TOE claim is no longer valid.

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 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.OUTBOUND_FILTER The TOE will only support TCP/IP as a network protocol. D.OUTBOUND_TRAFFIC shall only exit the TOE (R.EXIT_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 and D.SCAN_JOB data as soon as it is no longer required or during the start-up procedure if residual D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB is found on the TOE's hard disk. The first write cycle will either immediately after the job has completed or 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.

O.F.SELFTEST	The TOE will perform check of the integrity of the TSF when it is re-booted.

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 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 2045-65, 2050-70 or 31x5 Digital Copier that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE (selecting username and entering PINcode). When sending a D.SECURE_PRINT_JOB to the Digital Copier, S.REMOTE_USER shall specify a PIN that consists of a minimum of 4 and a maximum of 6 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. The DC 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 Digital Copier. The TOE will not work with any other device (including Digital Copiers from any other manufacturers).
O.E.SHREDDING	The customer requires the shredding of D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB data objects[6]

[6] The TOE shreds D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB by default when printing/scanning is completed in the delivered mode. It is possible to disable shredding for D.PRINT_JOB and D.SCAN_JOB. If this happens, the TOE claim in no longer valid.

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**
- **D.OUTBOUND_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) = DAC, ICMP, DNS, DHCP, LPR, HTTP, HTTPS, FTP, SNMP and Protocol = TCP/IP**
- **The TOE shall perform R.EXIT_TOE on D.OUTBOUND_TRAFFIC only if Port(D.OUTBOUND_TRAFFIC) = DAC, ICMP, DNS, DHCP, LPR, HTTP, HTTPS, FTP, SNMP and Protocol = TCP/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** 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** 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[7] 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**

- **on deletion of R.RELEASE_JOB, R.PRINT_JOB, and R.SCAN_JOB by S.LOCAL_USER, S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER**
- **on start-up or reboot of the TOE**.[8]

[7] 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.

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)

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

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)

---

8 The DAC 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.

9 This is a 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

10 The DAC 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_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** [11] security attributes **Port and Protocol** to **nobody.**[12]

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**[13] 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)

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**
- **Set the shredding moment**
- **Shred print jobs: yes/no (D.PRINT_JOB)**[14]
- **Shred scan jobs: yes/no (D.SCAN_JOB)**[15]

Dependencies: No dependencies.

---

[11] 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’.

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

[13] The word ‘the’ before ‘nobody’ was removed for grammatical reasons.

[14] Disabling these functions will invalidate the Security Target claim. The functions are available but there is an Organisational Security Policy that defines that they should be enabled by default.

[15] See footnote 14

FMT_SMR.1 Security roles

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

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **the TSF**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **the TSF data**.

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

Dependencies: FPT_AMT.1 (not included)[16]

[16] The dependency FPT_AMT.1 Abstract machine is not included, because the underlying IT platform does not contribute to the TOE requirements (See part 1, paragraph 147). The underlying PC platform is a standard PC platform that works. Testing of the platform does not provide assurance that will support the claims at the level of EAL2, as functional testing of the DAC in its operational environment is performed (it does what is should do).

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[17].

[17] 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 and ICMP commands that are not needed for the operation of the TOE. In addition all network protocols that are not supported in the security mode 'high' are disabled.

By default no traffic is permitted to enter or leave to TOE except for the TCP/IP packets and the restricted ICMP command set 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 send with the print job when submitted by S.REMOTE_USER with Username/PIN received from S.LOCAL_USER via the DC interface. If verification is successful, the secure print job is released for printing.

SF.SHREDDING
Once a print 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. S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER can choose the moment when the shredding cycle commences. The first write cycle can occur immediately after the print job has completed or to improve job throughput performance, once the TOE enters an idle state. The remaining cycles may also take place immediately after the print job has been completed or also at the time when the TOE enters an idle state. The shredding mechanism supports US DOD 5220-22m and Gutmann algorithms[18].

SF.MANAGEMENT
The TOE can be managed in relation to SF.JOB_RELEASE and 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 pre-configured in the security mode 'high'. This provides the most restrictive set of operational settings.

SF.SELFTEST
During start-up the TOE will check the hard disk files system and the integrity of the software the forms the TOE. If defects in the hard disk files system are

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

detected, the corrupted file system will be automatically repaired. The software includes all executables (operating system executables, Océ authored DAC executables, Third party software executables and DAC system settings). If defects are detected, the corrupted data will be replaced by correct shadow data.

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. There is also a probabilistic function and mechanisms that protects D.SECURE_PRINT_JOB and is used for the authentication of S.LOCAL_USER.

Subject	Function	Mechanism
S.REMOTE_SYSADMIN	SF.MANAGEMENT, SF.SHREDDING	An alpha-numeric password (ASCII characters 32-127) ranging in length between 5 and 50 digits. The first failed attempt results in a 10 second retry delay, the second attempt in a 30 second delay and for all following failed attempt a 90 second delay.
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 from 4 to 6 digits.

6.1.2 Strength of function claim

The SFRs FIA_UID.1, FIA_UAU.1, FIA_UID.2 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_UAU.1, FIA_UID.2 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 fulfilment of the respective requirement.

Configuration Management (ACM) assurance measures
The documents containing the description of the configuration management system and how it is used are:

- Océ-Technologies B.V., Internal Report 99431.141 Version and Release numbering, version 1, 2000-02-07.
- Océ-Technologies B.V., DAC Security Target Overview (Product document), Version 3 R&D Reviewed, 2004-05-06.

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, Océ31x5 Production and Installation of DAC controller (Product document), Version 2 R&D Approved, 2003-07-21.

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

- Océ-Technologies B.V., DAC Security Target Overview (Product document), Version 3 R&D Reviewed, 2004-05-06.
- Océ-Technologies B.V., Functional Specification of the DAC, Version 3 R&D Approved, 2002-10-8
- Océ-Technologies B.V., Internal Firewall in DAC (Product document), Version 0.4 r&D Draft, 2004-02-20
- Océ-Technologies B.V., DAC; Functional Specification Printjob Handling (Product document), version 1.7 R&D Released, 1999-11-06
- Océ-Technologies B.V., Functional specification Security on the Web based SAS (Product document), Version 3 R&D Preliminary, 2004-01-27
- Océ-Technologies B.V., Functional specification scanjobhandling DAC (Product document), Version 1.3 R&D Approved, 2001-04-10
- Océ-Technologies B.V., Data shredding in the DAC, Version 1.0 R&D Reviewed[2], 2004-02-13
- Océ-Technologies B.V., Functional specification DAC webserver (Product document), Version 3.0 R&D Approved, 2004-02-02
- Océ-Technologies B.V., Security Software Rules (Océ standard), Version 01 Released, 2003-11-20

The High Level Design is in: Océ-Technologies B.V., DAC Security Target Overview (Product document), Version 3 R&D Reviewed, 2004-05-06.

The correspondence tables between TSF, Functional Specifications and High Level Design are in: Océ-Technologies B.V., DAC Security Target Overview (Product document), Version 3 R&D Reviewed, 2004-05-06.

Guidance (AGD) assurance measures
The document containing the guidance for administrators can be found in: Océ-Technologies B.V., Océ System Configuration version 2.3 on-line help, Revision 2004, May 2004. The guidance for the customer administrators is in: Océ-Technologies B.V., Océ System Configuration version 2.3 on-line help, Revision 2004, May 2004.

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., DAC Security Target Overview (Product document), Version 3 R&D Reviewed, 2004-05-06.

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

- Océ-Technologies B.V., Test specification HTTPS certificate, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification FTP, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification firewall, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Lijst_security_PR1.xls, no date
- Océ-Technologies B.V., DAC Common Criteria security test plan Internal Report, Version 1.1 R&D For Review A, 2004-05-13
- Océ-Technologies B.V., DAC Common Criteria security test results Internal Report, Version 1.1 R&D For Review A, 2004-05-13
- Océ-Technologies B.V., Test specification strong password websas, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification E-shredding, Version 1.1 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification SNMP readonly, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification security tab (Product document), Version 1.0 R&D Approved, 2004-04-15.

A test analysis showing that the depth of the tests is sufficient to show that the TSF operates in accordance with its High Level Design can be found in: Océ-Technologies B.V., Dac Common Criteria Security Tests Plan, Internal Report 2004RD6486, Version 1.1 Released, 2004-05-18.

The test documentation (test scripts, test scenarios and test reports) can be found in

- Océ-Technologies B.V., Test specification HTTPS certificate, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification FTP, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification firewall, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Lijst_security_PR1.xls, no date
- Océ-Technologies B.V., DAC Common Criteria security test plan Internal Report, Version 1.1 R&D For Review A, 2004-05-13
- Océ-Technologies B.V., DAC Common Criteria security test results Internal Report, Version 1.1 R&D For Review A, 2004-05-13
- Océ-Technologies B.V., Test specification strong password websas, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification E-shredding, Version 1.1 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification SNMP readonly, Version 1.0 R&D Approved, 2004-04-16
- Océ-Technologies B.V., Test specification security tab (Product document), Version 1.0 R&D Approved, 2004-04-15.

Vulnerability Assessment (AVA) assurance measures
An overview of the guidance and environment issues can be found in: Océ-Technologies B.V., DAC Common Criteria security test results Internal Report, Version 1.1 R&D For Review A, 2004-05-13.

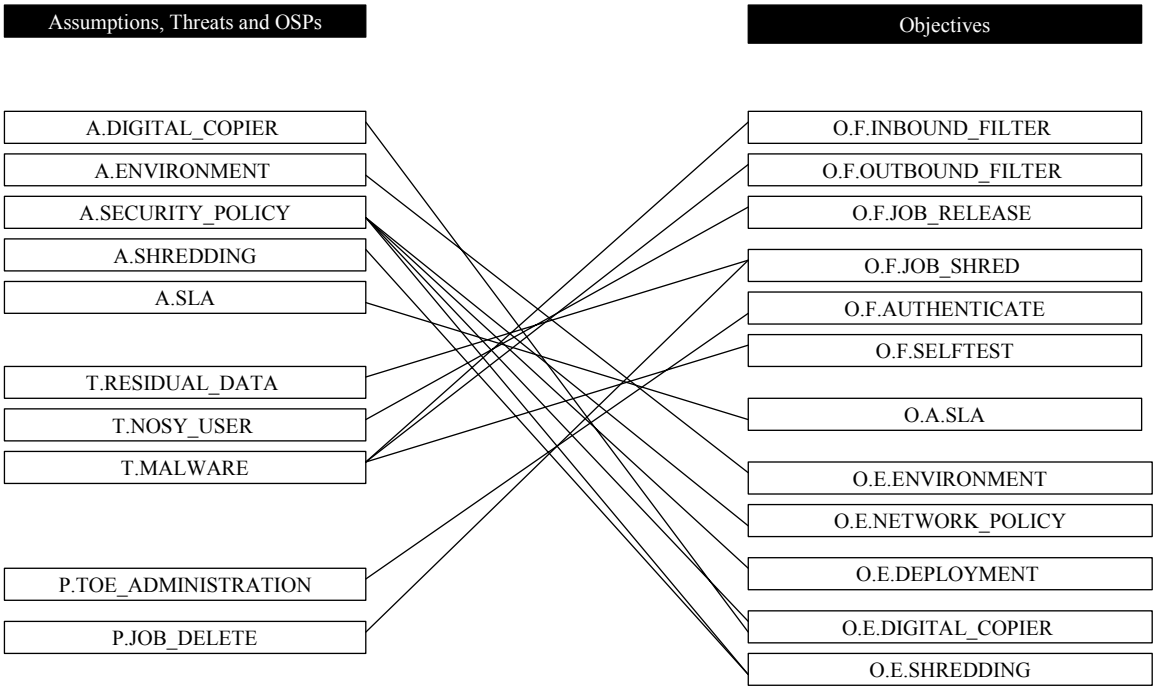
An analysis of vulnerabilities can be found in: Océ-Technologies B.V., DAC Common Criteria security test results Internal Report, Version 1.1 R&D For Review A, 2004-05-13.

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 figure.

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 2045-65, 2050-70 or 31x5 Digital Copier that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE (selecting Username and entering PINcode). When sending a D.SECURE_PRINT_JOB to the Digital Copier, S.REMOTE_USER is aware that they must specify a PIN that consists of a minimum of 4 and a maximum of 6 digits and shall delete the job on the same workday that it is sent to the TOE, whether or not it is printed. The DC 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 Digital Copier.

The TOE will not work with any other device (including Digital Copiers from any other manufacturers).

Although the assumption states that a Digital Copier from Océ will be used, the Digital Copier is an un-trusted device. The chances of an attack on the LAN being mounted via the Digital Copier interface are reduced by the TOE filtering the outbound traffic so that only ports that are absolutely necessary for the operation of the TOE are open. Requiring D.SECURE_PRINT_JOB 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. Additionally the access to the job is limited by specifying a minimum PIN length.

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 2045-65, 2050-70 or 31x5 Digital Copier that provides a Local User Interface and Glass Plate through which S.LOCAL_USER can interact easily with the TOE (selecting Username and entering PINcode). When sending a D.SECURE_PRINT_JOB to the Digital Copier, S.REMOTE_USER is aware that they must specify a PIN that consists of a minimum of 4 and a maximum of 6 digits and shall delete the job on the same

workday that it is sent to the TOE, whether or not it is printed. The DC 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 Digital Copier. The TOE will not work with any other device (including Digital Copiers from any other manufacturers).

O.E.SHREDDING – The customer requires the shredding of D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB data objects. The TOE shreds D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB by default when printing/scanning is completed in the delivered mode. It is possible to disable shredding for D.PRINT_JOB and D.SCAN_JOB. If this happens, the TOE claim in no longer valid.

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 and D.SCAN_JOB data objects. The TOE shreds D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB by default when printing/scanning is completed in the delivered mode. It is possible to disable shredding for D.PRINT_JOB and D.SCAN_JOB. If this happens, the TOE claim in no longer valid.

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 and D.SCAN_JOB data as soon as it is no longer required or during the start-up procedure if residual D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB is found on the TOE's hard disk. The first write cycle will either immediately after the job has completed or 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 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.

O.F.OUTBOUND_FILTER - The TOE will only support TCP/IP as a network protocol. D.OUTBOUND_TRAFFIC shall only exit the TOE (R.EXIT_TOE) if its Port is specified as being open in the Appendix D.

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.

Although policy states that a Digital Copier from Oce will be used, the Digital Copier is an un-trusted device. The chances of an attack on the LAN being mounted via the Digital Copier interface are reduced by the TOE filtering the outbound traffic so that only ports that are absolutely necessary for the operation of the TOE are open.

O.F.SELFTEST – The TOE will perform check of the integrity of the TSF when it is re-booted.

During start-up, the TOE checks to see if any of the TSF relevant files on the hard disk have been modified. This can happen due to a malware attack but occurs more often as a result of a power outage. Maintaining the integrity of the TOE gives assurance in support of the claim that the TOE will not form a threat against it operational environment.

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

O.F.JOB_SHRED - The TOE shall delete all D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB data as soon as it is no longer required or during the start-up procedure if residual D.SECURE_PRINT_JOB, D.PRINT_JOB and D.SCAN_JOB is found on the TOE's hard disk. The first write cycle will either immediately after the job has completed or 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 not 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:

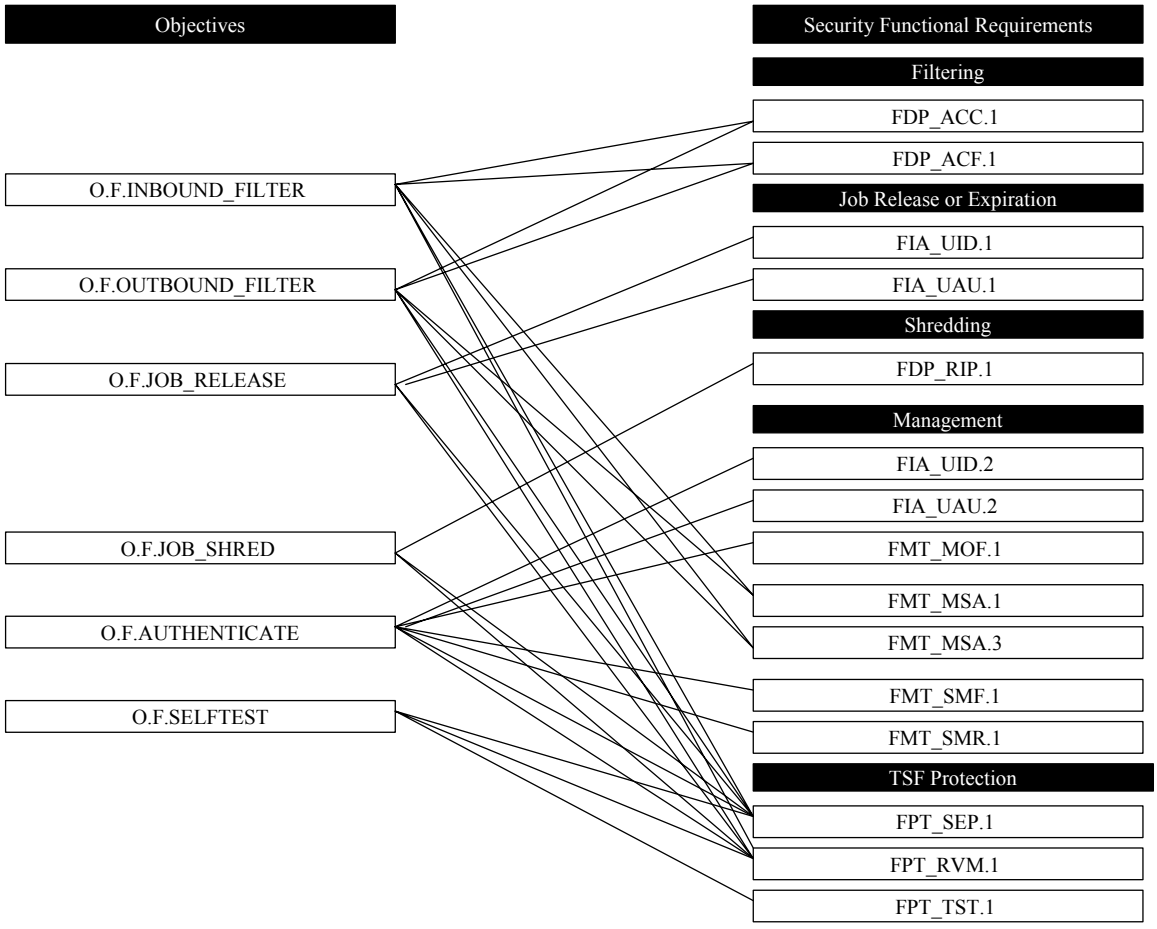
O.F.AUTHENTICATE - The TOE ensures that S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER must identify and authenticate themselves to the TOE before allowing them to modify the TOE security settings.

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.



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.

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.

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 Digital Copier and the network to which the TOE is attached being created.

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.

O.F.OUTBOUND_FILTER
FDP_ACC.1 Subset access control
Outbound traffic is filtered so that only traffic relating to the operation of the TOE is allowed to leave 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.

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 exit points through which an attack could be launched.

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 other non-TSF mechanisms from which a possible attack could be made.

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 Digital Copier and the network to which the TOE is attached being created.

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.

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 DAC/DC 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 DAC/DC interface. This SFR supports the security objective by requiring the S.LOCAL_USER to authenticate himself as part of the job release process.

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.

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.

O.F.JOB_SHRED
FDP_RIP.1 Subset residual; information protection
This SFR supports the objective by ensuring that once a print or scan job has completed, or if during the startup procedure, 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_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.

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.

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_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.

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.

O.F.SELFTTEST
FPT_TST.1 TSF Testing

When the TOE is started up, it will perform a suite of self tests and determine that it is working correctly. If it determines that there is a problem it will try to repair itself. If this fails it will place itself in an 'out-of order' mode

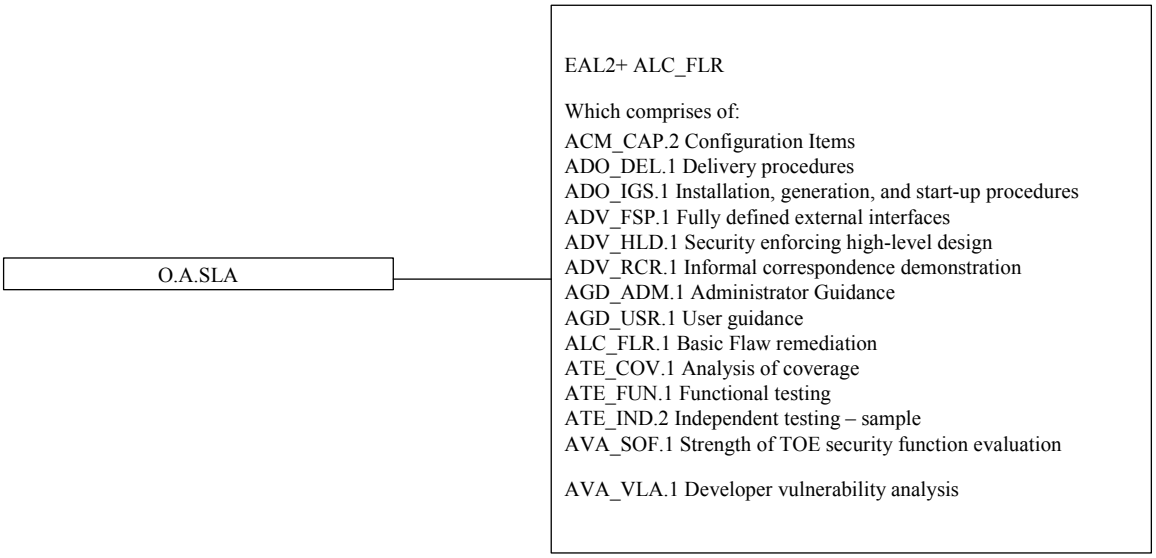
FPT_SEP.1 TSF domain separation
Self-testing of the TOE occurs in an area of the TOE that is separate to non-TSF related operation.

FPT_RVM.1 Non-bypassability of the TSP
The self-test mechanism cannot be by passed.

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



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 against 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: FDP_ACF.1, FDP_ACC.1, FMT_MSA.1, FMT_MSA.3, FIA_UID.1, FMT_SMF.1, FMT_SMR.1, FPT_AMT.1.

The dependency FPT_AMT.1 Abstract machine is not included, because the underlying IT platform does not contribute to the TOE requirements (See part 1, paragraph 147). The underlying PC platform is a standard PC platform that works. Testing of the platform does not provide assurance that will support the claims at the level of EAL2, as functional testing of the DAC in its operational environment is performed (it does what is should do).

All other dependencies are met.

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.

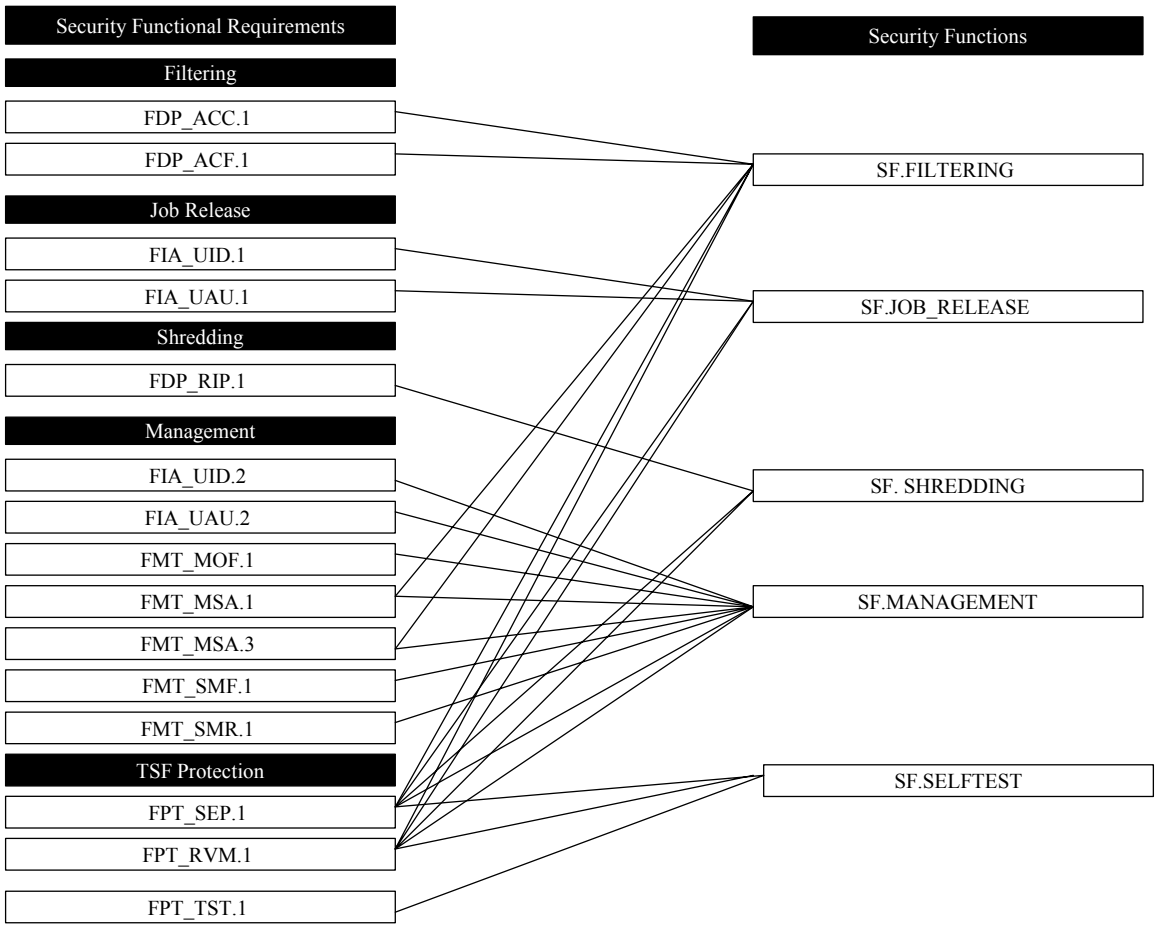
8.2.6 The requirements are mutually supportive

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_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_PRINTJOB, D.PRINTJOB and D.SCANJOB is deleted once they are no longer needed, or, if during the startup procedure residual print or scan job data is found on the hard disk. 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 DAC 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 print job 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.JOB_RELEASE This protects the integrity of the print job mechanism against un-authorised subjects and threat attacks.
3. 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.
4. 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.
5. The TOE start-up check 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. SELFTEST. This protects the integrity of the start-up check 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 DAC 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.
5. The TOE start-up check 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. SELFTEST. This ensures that no security management mechanisms can be used by un-authorised subjects.

FPT_TST.1
This Security Functional Requirement ensures that the TOE to performs a self-test during start up. This SFR is supported by SF.SELFTEST. The self-test helps protect the TOE against T.MALWARE so that it does not become a possible threat agent against S.NETWORK_DEVICE.

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

This claim is adequate to defend against the identified threats to the TOE that are identified in the TOE Security Environment. The threats (attacks) that the TOE protects itself against with regard to the SOF claim are:

T.RESIDUAL_DATA
In TOE physical scope and boundary, it is stated that the TOE does not claim to implement any measure that protect against physical theft of itself. Were this to happen, it is task of the TOE to ensure that no residual data can be accessed by the thief. This is done by:

- Shredding the data at the moment the job data is not longer needed by the TOE or when the TOE enters has completed operations and enters an idle state.
- Shredding any data during the start up of the TOE that was not shredded according to the standard manner of operation because, for instance, the TOE experienced a power failure.

The motivation to carry out this attack 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 acting as threat agent)
The local user is attempting to mount an attack by exploiting an obvious vulnerability. In order to do this, no expertise or resources are needed. As the time to execute the attack is longer than a working day and requires the attacker to attempt a large number of possible PINs that are associated with D.SECURE_PRINT_JOB, the motivation to carry out this attack is low.

T.MALWARE

T.MALWARE is handled by O.F.SELFTTEST,O.F.INBOUND_FILTER and O.F.OUTBOUND_FILTER. The motivation to attack the TOE with malware is low as the TOE provides filtering and integrity protection mechanisms that would require a high degree of expertise and tools in order to bypass them. This is in part due to the selection of the TOE components. The effort that would be required to create malware that could successfully attack the TOE is not in relation to the possible rewards.

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
DAC	Digital Access Controller
DC	Digital Copier
ITSEF	IT Security Evaluation Facility
LUI	Local User Interface (of a DC)
MFD	Multifunctional device for copying, printing and scanning, connected to a network (Combination of a DC and a DAC)
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 DAC for controlling the inbound and outbound flow of data is given below:

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

Traffic that flows between the DAC and the LAN via the network card

ICMP(administration)

Protocol	*Source Port / ICMP Type*	*Destination Port / ICMP Code*	*Direction*
ICMP	3	>=0	Inbound
ICMP	0	0	Outbound
ICMP	4	>=0	Both
ICMP	8	0	Inbound
ICMP	11	>0	Inbound
ICMP	11	1	Outbound
ICMP	12	>=0	Both

DNS, DHCP (administration)

Protocol	*Source Port*	*Destination Port*	*Direction*
UDP	53	>1023	Inbound
UDP+TCP	>1023	53	Outbound
TCP/ACK	53	>1023	Inbound
UDP	67	68	Both

LPR (accepting print jobs)

Protocol	*Source Port*	*Destination Port*	*Direction*
TCP	>1024	515	Inbound
TCP/ACK	515	>1024	Outbound

Web HTTPS server with HTTP redirect (administration)

Protocol	*Source Port*	*Destination Port*	*Direction*
TCP	>1023	443	Inbound
TCP/ACK	443	>1023	Outbound
TCP	>1023	80	Inbound
TCP/ACK	80	>1023	Outbound

FTP client (forwarding scan jobs to remote FTP server)

Protocol	*Source Port*	*Destination Port*	*Direction*
TCP	20	>1023	Inbound

TCP/ACK	>1023	20	Outbound
TCP	21	>1023	Inbound
TCP/ACK	>1023	21	Outbound

SNMP (read only administration)

Protocol	*Source Port*	*Destination Port*	*Direction*
UDP		161	Inbound
UDP	161		Outbound
UDP+TCP	162		Inbound
UDP+TCP		162	Outbound

Traffic that flows between the DAC and the DC via the linking cable

ICMP(administration)

Protocol	*Source Port / ICMP Type*	*Destination Port / ICMP Code*	*Direction*
ICMP		0	Inbound
ICMP		0	Outbound

DAC-DC

Protocol	*Source Port*	*Destination Port*	*Direction*
TCP	5010	>1023	Inbound
TCP/ACK	>1023	5010	Outbound

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
S8 Security / security level / required level	Changing this setting invalidates the claim
S12 Security / data shredding / shred moment	Sets the actual moment of shredding
S13 Security / data shredding / shred non secure jobs	Sets the type of print jobs to shred
S14 Security / data shredding / shred scan jobs	Sets whether scanned jobs are shredded
S97 Configuration / Network / TCPIP / HTTPD	Configures the Webserver that uses the TCPIP
S98 Configuration / Network / TCPIP / HTTPD / Port nr	Configures the port number that is used by the webserver
S144 Configuration / Applications / Web based SAS / Enable	Enables web based SAS
S146 Configuration / Applications / Web based SAS / ResetSASPassword	Resets the SAS password to its default value
S163 Configuration / licenses / Erase license	Erases the current license file
S206 Enable LPD / Disable LPD	Toggles the LPD daemon

REMOTE_SYSADMIN

Administration Function	Description
S8 Security / security level / required level	Changing this setting invalidates the claim
S12 Security / data shredding / shred moment	Sets the actual moment of shredding
S13 Security / data shredding / shred non secure jobs	Sets the type of print jobs to shred
S14 Security / data shredding / shred scan jobs	Sets whether scanned jobs are shredded
S98 Configuration / Network / TCPIP / HTTPD / Port nr	Configures the Webserver that uses the TCPIP
S99 Configuration / Network / TCPIP / HTTPD / self signed certificate / common name	Configures the port number that is used by the webserver
S147 / Applications / Web based SAS / SetSASPassword	Sets the S.REMOTE_SYSADMIN password
S206 Enable LPD / Disable LPD	Toggles the LPD daemon

Distribution list

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