Océ Printing Systems

Security Target for Océ SRA Controller version 3, bundle 8.02

Version 1.7, March 2007
Océ Printing Systems GmbH

Document History

Version	Date	Changes	Summary	Author
0.1	2005-10-31	Initial version	Initial version produced for OPS	Staffan Persson
0.2	2005-11-03	Updates	Updated evaluated platforms, administrator authentication and privileges	Staffan Persson
0.3	2005-11-15	Updates	Updated mainly the TOE description and the TOE Summary Specification	Staffan Persson
0.4	2005-11-17	Updates	Updated the TOE Summary Specification	Staffan Persson
0.5	2005-12-20	Updates	Updated after Océ internal review mainly chapter 2 and 6.	Staffan Persson
0.6	2006-02-07	Updates	Updated after review by evaluator	Staffan Persson
0.7	2006-02-14	Updates	Updated after review by evaluator and comparison with the design documentation	Staffan Persson Peter Wimmer
0.8	2006-02-20	Updates	Updated after evaluation review	Staffan Persson
0.9	2006-04-18	Updates	Updated after comments from BSI	Staffan Persson
0.91	2006-04-20	Updates	Description of VMM, VCM,…; List of third party DLLs; Abbreviations added; OS involved in logging on file system level	Peter Wimmer
0.92	2006-05-19	Updates	Review with S. Persson and N. Schwalbach	Peter Wimmer
0.93	2006-05-31	Updates	Moved FAU_SAR.1 and 2 into the TOE and updated SF.MANAGEMENT	Staffan Persson Peter Wimmer
0.94	2006-06-21	Update	Updated after evaluation review	Staffan Persson
0.95	2006-06-27	Update	Extended and separated SF.NETACCESS into three different security functions	Staffan Persson
0.96	2006-06-29	Update	Some clarifications (SNMP, DLL, etc.)	Peter Wimmer
0.97	2006-06-29	Update	Updated after evaluation review	Staffan Persson
0.98	2006-07-06	Update	Updated after evaluation review	Peter Wimmer
0.99	2006-07-20	Update	Updated after Océ review	Peter Wimmer
1.00	2006-08-09	Update	Updated after evaluator review SF.NETACCESS is in environment	Peter Wimmer
1.1	2006-10-27	Update	Removed FAU_SAR.2 due to SEAcgi; restricted V.24; added management (2.6.5) to security functions	Peter Wimmer
1.2	2006-11-08	Update	Added A.ITENV and OE.ITENV	Peter Wimmer
1.3	2006-11-	Update	Added A.COMM and OE.COMM,	Peter Wimmer

	27		A.PROTECT and OE.PROTECT	
1.4	2006-12-20	Update	Audit information not viewable via BDF; added A.CLIENT, updated authentication Updated SOF claims	Peter Wimmer Staffan Persson
1.5	2007-01-31	Update	Some minor clarifications	Peter Wimmer
1.6	2007-02-12	Update	Minor adaptions due to BSI comments	Peter Wimmer
1.7	2007-03-01	Update	Added “service panel” to A.CLIENT	Peter Wimmer

Table of Contents

1 ST Introduction

1.1 ST Identification

Title: Security Target for Océ SRA Controller Version 3, Bundle 8.02

Assurance level: EAL 3 augmented by ALC_FLR.2

Keywords: High Performance Printer, Information flow, Object Reuse

1.2 ST Overview

This document is the Security Target (ST) for the Océ Scalable Rasterized Architecture (SRA) Controller Version 3, Bundle 8.02 used in the high-performance printer Océ VarioStream 9000. The Security Target has been developed in accordance with the Common Criteria for Information Technology Security Evaluation (CC) version 2.3, for a claimed Evaluation Assurance Level 3 (EAL 3) augmented with flaw remediation of flaw reporting procedures (ALC_FLR.2).

The Océ SRA3 Controller is a software only component running on a separate board in the printer, handling all the logic of the printer and has security functionality to control information flow and to limit the access of management functions to authorized users.

1.3 ISO/IEC 15408 Conformance Claim

The Security Target is Part 2 conformant and Part 3 conformant to the CC. This means that it is conformant with the security functional requirements as specified in CC Part 2, and with the security assurance requirements for Evaluation Assurance Level 3 (EAL 3) augmented with ALC_FLR.2, as specified in Part 3 of the CC, including the CCIMB final interpretations as of September 2005.

1.4 Strength of Function Claim

The TOE contains two security functions realized by probabilistic mechanisms, being the authentication mechanism for user authentication and the access control for SNMP request. The minimum strength of function claimed for this function is SOF-basic.

1.5 ST Content and Organisation

The ST has been structured in accordance with [CC] Part 1 and [CCG]. The main sections of the ST are the TOE description, TOE security environment, security objectives, IT security requirements and rationale.

The TOE description provides general information about the TOE, serves as an aid to understand the nature of the TOE and its security functionality and provide context for the evaluation of the ST.

The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes all:

a. Assumptions regarding the TOE's intended usage and environment of use

b. Threats relevant to secure TOE operation

c. Organisational security policies with which the TOE must comply

The security objectives reflect the stated intent of the TOE. They pertain to how the TOE will counter identified threats and how it will cover identified organisational security policies and assumptions.

Each security objective is categorised as being for the TOE or for the environment.

The security requirements section provides detailed requirements, in separate subsections, for the TOE and its environment.

The IT security requirements are subdivided as follows:

a. TOE Security Functional Requirements

b. TOE Security Assurance Requirements

c. Security Functional Requirements for the IT Environment

The rationale presents evidence that the ST is a complete and cohesive set of requirements and that the TOE provides an effective set of IT security countermeasures within the security environment. The rationale is divided in two main parts. First, a security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a security requirements rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them.

1.6 Related Standards and Documents

[CC] ISO 15408 – Information Technology – Security Techniques – Evaluation Criteria for IT Security, also known as the Common Criteria or CC.

[CCG] ISO/IEC PDTR 15446 – ISO-Guide for the Production of Protection Profiles and Security Targets, Draft 2000-01-04.

[CEM] Common Methodology for Information Security Evaluation (CEM).

[IPDS] Intelligent Printer Data Stream Reference, IBM, 7.Edition, Nov 2002, S544-3417-06

[JAVA2] Java 2 Standard Edition 5.0, Build 1.5.0_05-b05, http://java.sun.com/j2se/1.5.0/docs/index.htm

[PCL] PCL5e für SRA Controller, Referenzhandbuch, Ausgabe August 1999, U24721-J-Z247-2

[PJL] PJL für SRA Controller, Ausgabe 3, Mai 2003, U24398-J-Z247-3

[RFC1759] The Printer MIB (superseded by RFC 3805)

[RFC2707] Job Monitoring MIB – V1.0, R. Bergman, T. Hastings, Ed., S. Isaacson, H. Lewis, November 1999.

[RFC3805] Printer MIB v2, R. Bergman, H. Lewis, I. McDonald, June 2004.

[UP3I] UP^{3}I, Universal Printer pre- and post-processing interface, Version 1.20, Nov. 2004

1.7 Acronyms

CB	ColorBelt Printer (VarioStream 9000)
CoDi	Configuration and Diagnostics
CSI	Channel Specific Interface
CSV	Comma Separated Values
DE	Device Electronic
DLL	Dynamic Link Library
DMA	Direct Memory Access
FC	Functional Code
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
IPDS	Intelligent Printer Data Stream
LAN	Local Area Network
LED	Light-Emitting Diode
LDEV	Logical Device
MIB	Management Information Base
OPM	Operator Panel Master
OS	Operating System
PCL	Printer Command Language
PJL	Printer Job Language
PVCS	Poly Version Control System
RFC	Request For Comments
RIP	Raster Image Processor
RMI	Remote Method Invocation
SNMP	Simple Network Management Protocol
SPM	System Parameter Manager
SRA	Scalable Raster Architecture
TRDP	Trivial Reliable Data Protocol
UP^3I	Universal Printer, Pre- and Post processing Interface.
VCM	Virtual Channel Manager
VMM	Virtual Memory Manager
XML	Extensible Markup Language

2 TOE DESCRIPTION

This section describes the Target of Evaluation (TOE) in terms of the class of product, the operational environment, and the provided security functionality. This chapter provides a general description of the product and the environment in which it is used.

2.1 Product Overview

2.1.1 Introduction

A printer is the physical device that takes media from an input source, produces marks on that media according to some page description or page control language and puts the result in some output destination, possibly with finishing applied. Printers are complex devices that consume supplies, produce waste and need mechanical service. In the management of the physical device the description, status and alert information concerning the printer and its various subparts has to be made available to the management application so that it can be reported to the users, operators for the replenishment of supplies or the repair or maintenance of the device.

In the Océ high-performance printers, this information and logic is handled by the SRA3 Controller. It consists of several Intel x86 CPU based boards cooperating in order to capture and process the incoming printer data stream received via network or channel interfaces from a host system. The controller can be configured with a varying number of boards depending on the required printing speed and the printer hardware, since the controller is used in a range of different Océ printers. The SRA3 Controller supports printer languages from IBM ([IPDS]) and HP ([PCL]).

The SRA3 Controller will be delivered and installed along with the whole printer system by an Océ service team.

For administrators to interact with the printer logic the SRA3 Controller supports two types of interfaces, the operator panels and the service panel, that are PCs connected to the SRA3 Controller via Ethernet. These user interfaces are in the evaluated configuration connected at two different network interfaces. The customer may connect to and use number of operator panels (shown as operator console in the picture below) to the SRA3 Controller.

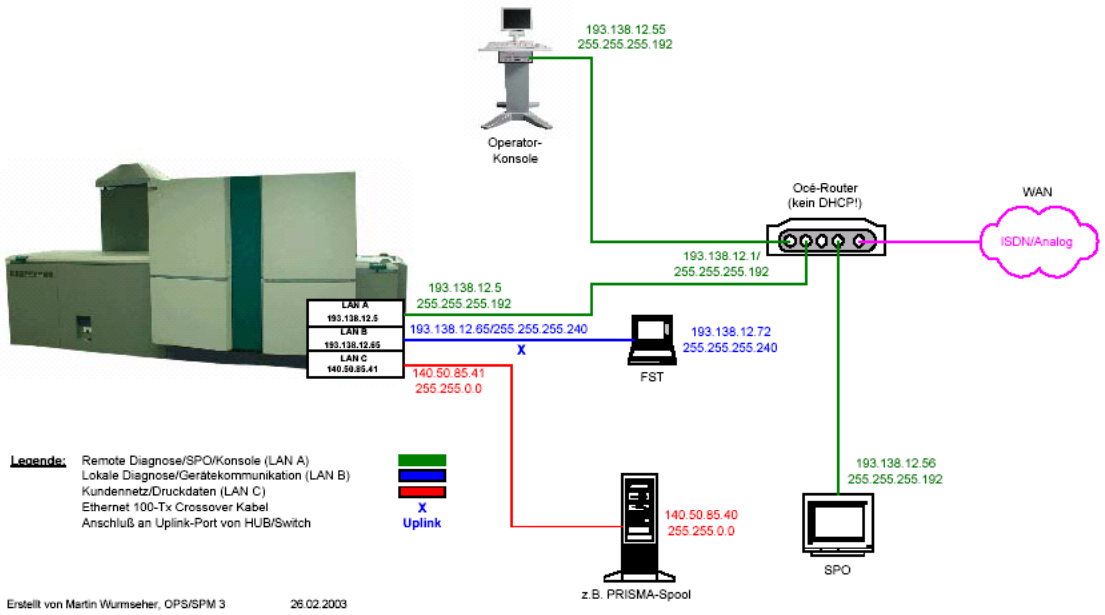

Figure 1, Printer Environment

The operator panel is intended for the customer when operating the printer, while the service panel is for the Océ service technician only. This means that the service technician has the service panel software installed on a laptop that will be connected to the printer network only when the service technician is on-site. In rare exceptions customers may want to take care of their own service and will then also be given access to the service panel software[1].

In addition to the control panels[2], the printer status can be monitored via SNMP.

If activated, remote support channels via modem will be made available. Such channels are not part of the evaluated configuration.

The SRA3 Controller has up to four network interfaces LAN A, LAN B and optionally LAN C / D, each of these interfaces are dedicated for a specific use (see Figure 2~~Figure 2~~): LAN A is the network intended for operation and diagnostic using the operator panel; LAN B is a network intended for printer-internal communication and local service / diagnostic only, i.e. service panel only; and LAN C (Ethernet) / D (fiber optic) is the network that is used by users to send printer data to the printer. Routing of traffic between LANs A, B and C / D is disabled.

LAN A and LAN B are similar in their behaviour, with the difference that in the evaluated configuration only LAN B provides the service panel to the service operator (i.e., remote access via a service router on LAN A is restricted). LAN B is also only accessible within the premises of the printer available to local service, while LAN A and LAN C / D are considered to be external networks that are reachable outside of the perimeter protection of the physical printer.

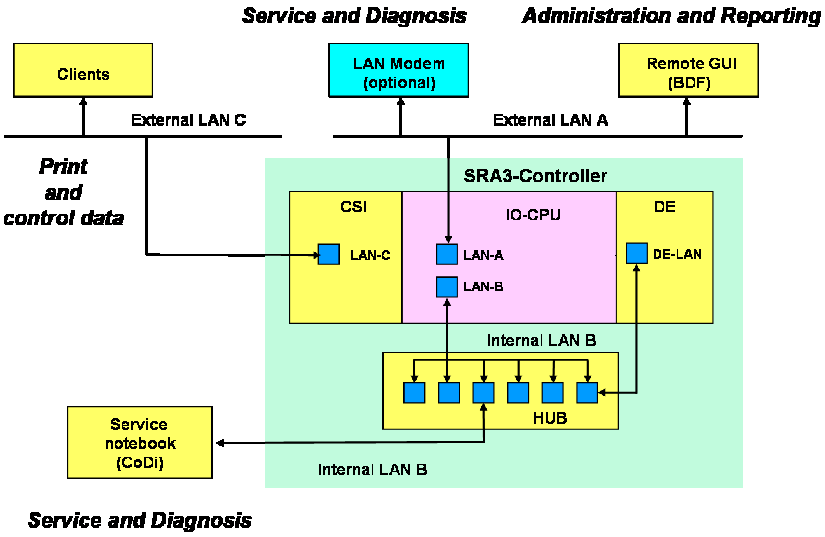

Figure 2: Networks

In addition to the Ethernet and fiber optic interfaces, print data may also be sent via SCSI, ESCON and 370 interfaces. Up to three different print client interfaces may be combined, with only one interface active at any time.

There is one additional external interface available, a FireWire interface used for connecting the printer to other devices using the UP^{3}I protocol ([UP3I]~~[UP3I]~~), which is an industry standard used for controlling print devices. The UP^{3}I interface may be used as part of the evaluated configuration, but does not have any security relevance. UP^{3}I is used for controlling various printer devices from a single operator panel (i.e., the Océ panel) by downloading and operating the respective GUI components from these devices.

The SRA3 Controller software sits on top of the OS using its own memory management for print data and resource handling. The underlying operating system used is Windows NT Embedded that has been configured and hardened not to provide any unnecessary services or features.

The administrative interfaces are called operator panel (in German *Bedienfeld*) or service panel (also referred to as *CoDi*) and use Java Remote Method Invocation (RMI) to interact with the TOE. The Java RMI based server is used to communicate with the operator panel and service panel that execute the

[1] Deprecated in the evaluated version

[2] i.e., the operator and service panels

Java code. The authentication of administrators at the operator or service panel is handled by the server process. MD5 hashes are used to encrypt the passwords when stored in the password file. RMI communication, including the authentication procedure, is protected against eavesdropping by 128 bit SSL encryption.

The service PC does not only provide an interface to the service panel, but also provides functionality for maintaining the TOE environment, such as the underlying operating system and file system. It is only possible to use the service PC over LAN B, this requires full physical access to the TOE. When using the service PC at LAN B, the physical access is controlled by the TOE environment and not by the TOE. The service operator has full control of the TOE using this interface. Even so the service operator may need to perform an identification and authentication using the service PC to perform certain operations on the TOE.

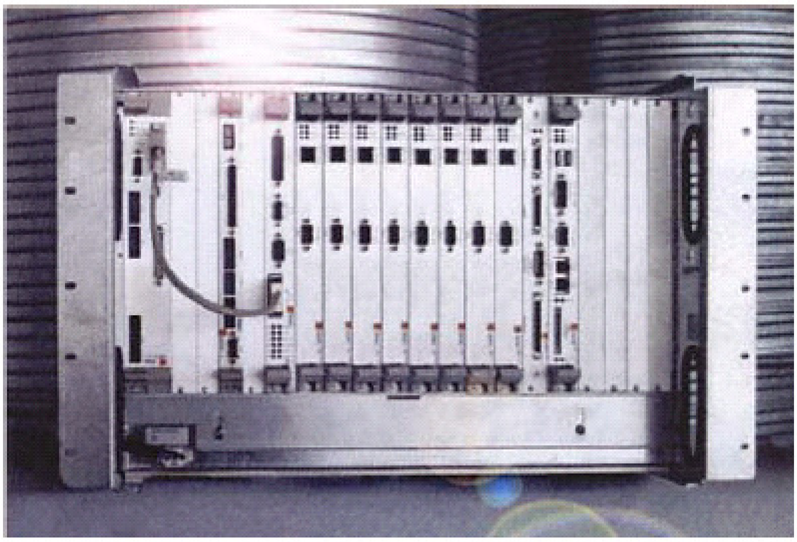

Figure 4~~3~~, Picture showing the SRA3 Controller with eight Raster Modules

Three classes of predefined set of administrator privileges (roles) are supported: *operator*, *key operator* and *service operator*. Customers of Océ usually only get access to *operator* and *key operator* roles, while the *service* role is reserved for Océ service team members. All these roles are collectively referred to as administrators. The operator, the key operator and the service operator use the same administrative interface, but the operator only has a subset of the privileges of a key operator. The service operator has a different set of privileges and may in addition use a different administrative interface than the operator and key operator. Privileges can be represented by the functionality available to the administrators in the operator panels. Each administrator role has a default set of privileges as well as a level associated with its role. An administrator can only add or remove administrators or edit privileges and the password of other administrators that are on a lower level than themselves, defining a hierarchy between administrative roles. The predefined administrative roles may be edited, but not deleted.

Internally, the system uses SNMP and a custom dispatcher to communicate with logical subsystems and additional hardware components. Externally only the Printer MIB is visible to remote hosts. SNMP requests[3] (port 161) are accepted on LAN A, LAN B and LAN C / D for the Printer MIB ([RFC3805]). SNMP traps (port 162) are sent to specified hosts. SNMP access is explicitly enabled by an administrator; SNMP access to LAN C / D is disabled by default, but may be allowed by an administrator via the operator panel

The Printer MIB provides a method for network users to utilize SNMP and existing SNMP standards to manage the networked printer. The MIB objects provide the ability to monitor and control these printers, providing fault, configuration and performance management. Important MIB parameters are the machine information (name, type and serial number), the device status (on-line, off-line, ready / not ready), the printer counters and any maintenance information. The printer MIB is the IETF proposed

[3] reading with SNMP GET and writing with SNMP SET

standard RFC1759 and later RFC3805. The information provided therein provides a standard way for SNMP applications to identify the attributes and status of a printer.

Print data is received by LAN C / D and cannot be extracted from the system during regular operation. It is not even cached on the hard drive, but only resides in RAM during processing. Print data streams can request resources to be captured on the local hard drive (for example scanned signatures, bar codes, logos or fonts). The system will not purge such resources until the print data stream explicitly requests release of the resource.

2.1.2 Installation

The printer software comes pre-installed, and the printer is set up and configured by Océ service personnel. Any software updates that are required during the life cycle of the printer are installed by Océ service technicians from disk images.

2.1.3 Supported Platforms and Environment

The controller is capable of driving various types of printer hardware, as the security functionality is not linked to the printer hardware. However, the underlying platform for the evaluation is limited to the Océ VarioStream 9000 (CB).

The controller can be used in various CPU card configurations, which will have an impact on system performance rather than on the functionality or the behaviour of the security functions. Figure 4~~Figure 3~~ shows a picture of the SRA3 Controller with eight raster modules.

2.2 Components overview

The picture below shows the external interfaces of the key SRA3 Controller as well as the functional behaviour and dependencies between the components making up the TOE.

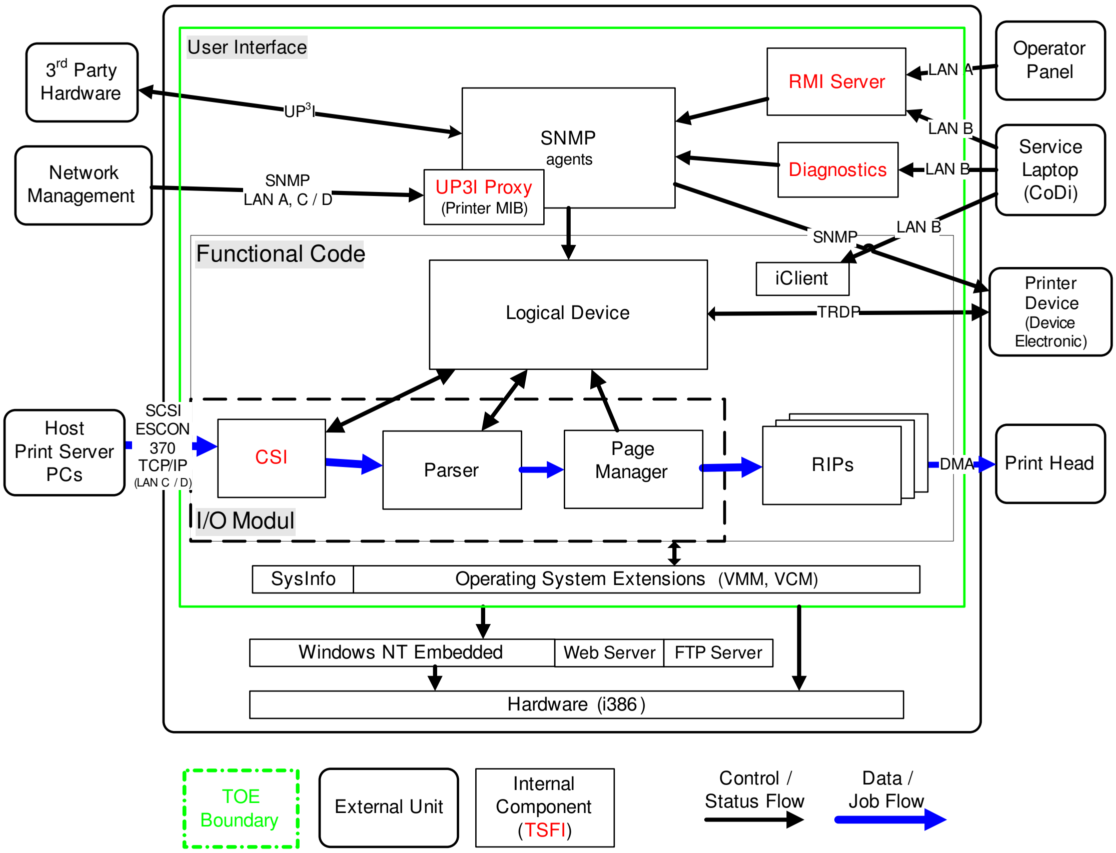

Figure 5~~4~~: Components of the SRA3 Controller

The operator panel interface (RMI) is visible on LAN A and LAN B. The network management interface is connected to both these LANs. The TOE is able to distinguish between connections coming in from the different LAN interfaces. The print clients are connected to LAN C / D or via SCSI, ESCON or 370. Third party hardware is connected to the UP3i using a FireWire interface. The printer head generates the print data on paper and the Device Electronic (DE) generates control data for controlling the mechanisms of the printer.

The functional behaviour of the TOE consists of the print-flow, the supervising and configuration of the TOE. The thick (blue) arrow in Figure 5~~Figure 4~~, from the host to the print head, shows the flow of the print data. The thinner (black) arrows show the other types of communication, such as the management functions and SNMP communication with the TOE and within the TOE. The interfaces in red indicate the TSFIs. There are three main processes responsible for this: function code process (FC), operator panel process and diagnostics process. The FC process is concerned with the print-flow; the operator panel process is for the operation of the printer by the administrator; and the diagnostics process is for the maintenance of the TOE and the printer.

The internal communication is done using the SMNP protocol. This means for example that the RMI server communicates with the internal SNMP agents using the SNMP protocol.

2.2.1 Functional Code

Print data is provided to the controller by a print data interface, the Channel Specific Interface (CSI). This usually implements an Ethernet interface (LAN C / D, TCP ports 5001 and 9100), but also other physical interfaces are possible. Interfaces with a strict dedicated usage (SCSI, ESCON, 370) are built as a point-to-point connection between a print server and the CSI. Only one of these client interfaces may be active at any given time, to avoid confusing print data. The transfer uses the print language supported by the controller encapsulated in communication protocol of the interface. The controller removes the communication protocol and passes the printer data to the language parser, which analyses the data and act upon its content. The parser determines which print data contains printer commands and which contains data to be printed.

Printing properties are set up via printer commands in the data stream or using the operator panel GUI. The printer commands can change the status of the setup of the printer and affect the printer behaviour, using the Logical Device (LDEV). For performance reasons, the LDEV transfers commands to the printer via a proprietary protocol (TRDP).

Print data is translated into an intermediate (meta) printer language, which in turn will be translated by the RIP (Raster Image Processor) into pixels.

The processed print data will be managed by the page manager and temporarily stored along with its resources in a page buffer. Each page is considered a closed unit that will be processed at each stage. The page manager is the central processing and management of the print data. It knows the operational status of the printer and knows the status of each page at any certain time. The controller can handle the parallel processing of up to nine RIPs and must therefore maintain the correct order of all the pages that are processed in parallel. The RIP or the RIPs are processing the next page as they are completed with previous pages, provided sufficient memory is available. The time to process a page is depending on the performance and resources available to the RIP.

The rastered pages are temporarily stored in a raster memory, until the page manager instructs the RIP to transfer the pages to the print head. Data from the page manager to the RIP and from the RIP to the print head is transferred via DMA.

For the PostScript-container implementation of IPDS, DLLs from third party vendors are used.

2.2.2 Operating system

Windows NT embedded is used as the underlying operating system. It has been configured to improve performance and security. The memory swapping mechanism of the operating system has been disabled. Unused network services of the operating system are unavailable. Only required TCP and UDP ports are activated on a per interface basis. The operating system is part of the TOE environment (see Figure 5~~Figure 4~~).

Date and time information is provided to the operating system by the underlying hardware.

2.2.2.1 Operating system extensions

For the implementation of the controller functionality on a multi-processing-system, the operating system was enhanced by a virtual memory management (VMM) unit as well as a virtual channel management (VCM) unit. These virtual units provide for parallel computing as well as independence from the physical processing unit; they are part of the TOE.

- VMM: Virtual Memory Management provides access to both local and distributed memory
- VCM: Virtual Channel Management provides a communication mechanism between components of the Functional Code

Status information and parameters used within the Functional Code are stored using the SysInfo mechanism, which acts as a local information repository.

2.2.2.2 Services

Web server and file transfer services are provided by the operating system:

- HTTP: delivers the operator panel to clients and provides access to the audit interface
- FTP: provides access to the hard disk of the SRA3 Controller for system maintenance by Océ service.
  Diagnostics (see 2.2.4) provides an additional FTP service on port 5078. It is explicitly started via CoDi after authentication using a proprietary mechanism.

2.2.2.3 IP Filter

The operating system also provides IP port filtering, which restricts inbound network access to a few protocols and ports on specific interfaces only, outbound network traffic is unrestricted. LAN A is restricted to communication necessary for remote access via the operator and service panels, while LAN B is restricted to printer internal communication and access via the service panel. Client access is restricted to LAN C / D only. Proper IP filters are set up at installation time and are never changed during normal operation of the TOE.

2.2.3 Operator Panel task

The *operator panel task* consists of an RMI server ([JAVA2]), internal SNMP agents, an SNMP dispatcher (SPM) and an SNMP master agent, which are all part of the TOE.

The *operator panel GUI* is external to the TOE and is communicating with the TOE based on SNMP messages over RMI. This GUI is a Java Webstart application, which is downloaded by the operator panel client PC from a HTTP server (Tomcat) on the SRA3 Controller. One operator panel is usually located within the printer premises; additional operator panels may be arbitrarily located in the local network.

An RMI server is deployed for the communication with external resources, i.e. the operator or service panel clients. All communication from external clients via the RMI server is handled by another internal SNMP agent. The RMI server authorises communication before forwarding requests to the internal agents. When an operator or service panel registers with the RMI server, a unique token is provided by the RMI server, used to separately authorise all subsequent requests.

Internal agents and servers exist for the adjustment of paper, error messaging, start-up and powering down the device and the saving of settings, the diagnostics agent for the service panel (a.k.a. CoDi maintenance software) and the UP^{3}I agent for pre- and post-processing devices. These agents use proprietary MIBs[4] to change settings of the controller and the print device and to save the current parameters.

The *SPM* (*System Parameter Manager*) is responsible for the operation of the operating panel process. It provides the exchange of current changes of parameters (MIB values) between agents, thus providing current information to all agents.

[4] these internal MIBs are not accessible from the outside

An *SNMP master agent* (the UP^{3}I proxy) makes a limited set of SNMP functionality available externally via the Printer MIB. The Printer MIB provides a standardised query interface to the printer.

2.2.4 Diagnostics task

Diagnostics of the SRA3 Controller consists of an internal part for displaying maintenance features as well as execution of maintenance tasks, and an external front end, running on an authenticated PC of a service technician (in the TOE environment). Access to the diagnostics system is provided either via the local network or a serial V.24 interface[5].

2.3 Scope of the Target of Evaluation

The Target of Evaluation with the security relevant interfaces (TSFI) is shown in Figure 5~~Figure 4~~ above. The Target of Evaluation is limited to the software that has been developed by Océ and is running on the SRA3 Controller card. The PostScript-container implementation of IPDS via DLLs from third-party vendors is not part of the TOE.

2.4 Evaluated configuration

The evaluated configuration includes the following features:

1. Activation of the password rule.
2. Removing developer or test users that are part of the default installation, leaving only the following types of user roles *operator*, *key operator* and *service operator*.
3. Network access control that allows read access for external SNMP and limited write access[6]
4. Network access control for operator panels
5. Administration by the service operator over modem connected to LAN A is not allowed
6. Tracing intended for debugging must not be activated.

The TOE will be brought into the evaluated configuration as part of the installation process. This is described in the Security Guide for the SRA3 Controller.

2.5 TOE Environment and Physical Protection

The TOE is expected to be operated under some physical control. There are three levels of physical protection needed by the TOE environment, related to different parts of the network and network interfaces of the TOE.

1. It is expected that LAN C / D is within a well-managed network environment. This means that this network is accessible only to non-hostile users that are allowed to submit print jobs. No other printer network, printer or the TOE must be accessible in this environment.
2. It is expected that LAN A is within a well-managed network environment. This means that the networks are under the control of the organisation operating the printer. In this environment it is possible to connect operator panels. The operator panels used by the operators, key operators and service operators to manage, i.e. to change any TOE data, must be within this area.
3. Full physical access to the TOE and the connection to LAN B must only be available to service operators, to prevent tampering with or the replacement of the TOE. The TOE shall be situated in a secure area (e.g., data center), which is only accessible by authorized personnel.

[5] access via the V.24 interface is prohibited in the evaluated configuration

[6] The write access is not to any security relevant information, but limited to sysContact, sysName, sysLocation and to localization.

Note that the TOE environment of (1) does not have any user authentication. Anyone within this environment is able to submit print jobs. Any restrictions to submit print jobs must be implemented within the TOE environment. The TOE environment of (2) grants authorized operator panels read access and for certain IP addresses also configuration update rights.

2.6 Security Functions

The SRA3 Controller supports the following security relevant features that can be evaluated. These are the key security functions identified during the readiness assessment.

1. Role based administration – Roles with different capabilities are used to administer and service the system.
2. Password controlled access for administration – All TOE administrative access via the RMI server, using either operator or service panels, is password protected.
3. Password quality control features – Password quality enforcement for administrative accounts will allow only passwords of a certain quality to be used.
4. Security audit of operator actions – This will give accountability to operator actions to identify which operator has performed what operation when.
5. Management of the security functions – user management, password change, access ticket and SNMP access configuration via the control panels and viewing of security audit information via the service panel.
6. Object reuse protection for the data stream and resources (fonts, logos, etc.) – As the data stream normally is not cached on disk, the VMM can be used to show that data from previous jobs can not show up in new jobs. Resources that are cached on disk are only accessible by the SRA3 Controller.
7. Printer data protection of the data stream – The data stream is never stored on disk and never transmitted to any other network interface than to the intended printing interfaces.
8. Network access control for management and monitoring devices – Network ACLs are used to guard administrative access via the network.

Each of these security functions is described in further detail in separate sections below.

2.6.1 Role Based Administration

Administrators are users using the administrative interface of the TOE, i.e. the service or operator panel. They are the only users known to the TOE. End users that are submitting print jobs or obtaining SNMP information from the TOE are not considered users in this sense, since they are not individually identified or authenticated and therefore are not known to the TOE. In order to print, end users need access to the network the TOE is connected to and (in case of SNMP) which is allowed to perform external SNMP access to information.

Administrators can individually be assigned privileges. To simplify administration, there are predefined sets of privileges available determining who is allowed to administrate or service the system. The predefined sets of privileges are templates that are given the roles, each of them with its own privileges to perform certain security functions for the administration of the TOE. There is a predefined set of roles with its own privileges for the administrator roles of *operator, key operator* and *service operator*. An administrator will then be given the predefined set of privileges associated with any of these roles. However, the privileges of each user are managed individually. Each user has certain tasks to perform which can be described as[7]:

- User – A person or application that submits print jobs to the printer; typically viewed as the "end user" within the overall printing environment. Note: This role is not known to the TOE, but described here for completeness.

[7] These roles are based on RFC 3805, but renamed to fit to the terminology of the Océ Printing System.

The following users (i.e., administrators) are known to the TOE.

- Operator – A person responsible for maintaining a printer on a day-to-day basis, including such tasks as filling empty media trays, emptying full output trays, replacing toner cartridges, clearing simple paper jams, etc. The operator will specify the printer characteristic and perform printer maintenance tasks using the operator panel. The only security-relevant actions of an operator are changing his own password, editing allowed IP addresses for external SNMP access and enabling external SNMP access both via LAN A and LAN C / D.
- Key operator – A person responsible for configuration and troubleshooting of components involved in the overall printing environment, including printers, print queues and network connectivity issues. This person is typically responsible for ensuring the overall operational integrity of the print system components, and is typically viewed as the central point of coordination among all other role models. A key operator may perform user management (add, edit, delete) for operator accounts.
- Service operator – A person responsible for repairing a malfunctioning printer, performing routine preventive maintenance, and other tasks that typically require advanced training on the printer internals. An example of a service operator would be a manufacturer's field service representative, or other person formally trained by the manufacturer or similar representative. The service operator may also use the service PC to access the TOE environment. Any such access to LAN B is not under the control by the TOE, but must be handled by the TOE environment by restricting the physical access to the LAN B and V.24 interface.

These tasks require certain privileges to be available to the administrator. While privileges are a non-hierarchical set of rights that any administrator can have, administrators are organized in a hierarchy defined by their level: *operator* is on the lowest level, while *service* is on top.

In addition, any administrator with a certain privilege may grant that privilege to another administrator. However, restrictions are imposed by the before mentioned *level* with regard to *user management*: only other administrators, which are on a lower level, may be edited.

A *key operator* (as the head of operators) has an elevated set of privileges in comparison to an *operator*. Certain operations cannot be performed by the key operator, but have to be performed by the *service* operator. Thus, the classification of administrators relates to their expertise, not their trustworthiness. Furthermore, certain operations are part of the services contract and thereby performed by the service operator role of the Océ service team.

To avoid any concurrency problems of updating by different operators, the concept of access ticket has been introduced. The operator panel holding the access ticket is the only operator panel allowed to make any configuration updates to the TOE and the printer.

2.6.2 Password Controlled Access for Administration

Using the operator panel (on LAN A) and service panel (CoDi, on LAN B), all access to administrative accounts is password protected. This is to prevent unauthorized users that are not administrators to gain any administrator rights. The authentication of administrators at the operator or service panels is handled by the server process. MD5 hashes are used to encrypt the passwords when stored in the password file.

The password policy is configurable and will apply to all administrators. The quality of the passwords is addressed in the next section.

2.6.3 Password Quality

For the authentication to be effective, a password policy is implemented, enforcing administrators to select passwords with a certain quality. This applies both to the passwords they select for themselves or for other administrators. The password policy would prevent the selection of obviously weak (i.e. easy to guess) passwords and limit successful password guessing attacks.

2.6.4 Security Audit

The audit of actions traces user (i.e. administrative) access to the TOE. The audit trail is useful to establish accountability, identify misuse of authorized users (i.e. administrators) or password guessing attempts of unauthorized users. The security audit trail[8] is stored via the operating system (in files), may be accessed via the service panel and may be exported using a web interface.

A number of different types of events are recorded by the audit function, but only the auditing of security relevant events and information is of interest for security. This means actions related to security functions, such as authentication success or failure.

Deletion of audit information is only available to the service operator.

2.6.5 Security Management

The administration of users, user rights, passwords and roles, SNMP and ticket access controls as well as access to security audit information is implemented by the security management functions of the SRA3 Controller. Access to these management functions is implemented via the control panels and itself depends on administrative rights and roles.

2.6.6 Object Reuse

Object reuse is the protection for the data stream against reuse by other users / print jobs. As the data stream normally is not cached on disk, the VMM can be used to show that data from previous jobs cannot show up in new jobs.

Resources are loaded by print data commands and are only accessible and may only be erased by the SRA3 Controller.

This is a user data protection mechanism that may either rely on a resource being erased once it has been released, or that a resource being erased once it is re-allocated. Both of them are acceptable as long as resources cannot be accessed using any other method than the allocation mechanisms actually performing the erasure.

2.6.7 Printer Data Protection

Data protection deal with the protection of the print data. The data stream is never stored on disk and never transmitted to any other network interface than to the intended printing interfaces. This is actually a security function controlling the flow of information, i.e. user data to be printed. The printer data protection is static and cannot be configured. The print data can only be printed.

2.6.8 Network, SNMP and Ticket Access Control

A network protocol and port filter allows only certain protocols (TCP or UDP) and port numbers on each of the different LAN A, LAN B and LAN C / D for inbound connections.

External SNMP access is restricted to a selected set of IP-addresses and a community string is required. This provides basic protection of the externally available MIB parameters containing printer status information, which is not of high security relevance.

Update access control is available to restrict the management on the operator network to specific IP-addresses. This means that although the administrator is authenticated, no update is possible unless the IP-address of the operator or service panel is an accepted one and is in possession of the access ticket.

2.6.9 Mechanisms that Need a Strength of Function Rating

There are two security functions that rely on probabilistic or permutational mechanisms. This is the authentication function (password mechanism) and the access control for SNMP requests (IP address in combination with a community string). The overall strength of function claim of these functions are SOF-basic.

In order to add security to the implementation of the Printer MIB standard RFC 3805, Océ has added IP-address filtering to restrict access to certain addresses only.

[8] General audit information, which is not security relevant, is readable via the operator panel (via *VarioStream →Displays →Errors and Warnings*) to all administrators.

Even at SOF-basic, administrators may not select just any type of password, such as trivial passwords or password being too short. This is enforced by a password policy that is enforced by the TOE in combination with rules saying that the password has to be changed on a regular basis. In the same way, the administrators may not select just any type of community strings, such as trivial community strings or community strings being too short.

3 TOE Security Environment

The assumptions made and the threats addressed are summarised in the following section.

3.1 Assumptions

The following conditions are assumed to exist in the TOE operational environment. These assumptions include essential environmental constraints on the secure use of the TOE.

Assumption	Description
A.NOEVIL	The TOE administrators (operator, key operator and service operator) are trustworthy to perform the actions they are trusted to do in accordance with security policies, and not to interfere with the abstract machine and the clients (e.g. do not install software), making sure that the TOE, its clients and the TOE environment are competently installed and administered.
A.PHYSICAL	The TOE is operated in a physically secure environment to which only authorized administrators (operator, key operator and service operator) have access. This includes physical access to the default operator panel, the print server and the LAN B network, which only the service operator may access.
A.TIME	It is assumed that the TOE environment provides a reliable time source to support the generation of audit records.
A.NETMAN	It is assumed that the TOE is properly installed and connected to a well-managed network, which physically separates and limits the access to the user network (LAN C / D), the operator network (LAN A) and the service network (LAN B).
A.ITENV	Functions in the TOE environment related to memory management, program execution, access control and privilege management provided by the underlying OS as well as functions related to printer language interpretation that are part of the TOE environment are working correctly and have no undocumented security critical side effects on the security functions of the TOE.
A.COMM	Communication links between the Operator Panel task of the TOE and operator and service panels in the TOE environment are protected against unauthorized modification and disclosure of communication data.
A.PROTECT	It is assumed that communication between print / network management clients and the SRA3 controller is protected against disclosure, either by a secure network environment or by encrypted connections to a print / network management server.
A.CLIENT	Only the standard operator panel and the service panel may request the access ticket. Further operator panels may be added, but are not allowed to obtain an access ticket.

3.2 Threats

The threats are categorized as those addressed by the TOE and those addressed by the environment.

The assets controlled by the TOE are information and resources, such as print data being transmitted and TSF data being maintained. It is assumed that an attacker is either an unauthorized user of the TOE, or an authorized administrator of the TOE who has been granted limited access rights to the TOE. Any administrator may only perform operating and maintenance for which he is authorized, i.e. has received appropriate training and experience.

It is assumed that the attacker has limited resources and comes from a well-managed user community in a non-hostile working environment. The TOE is not intended to be used in an environment in which protection against determined or sophisticated attacks is required.

Users are printer users, sending print jobs to the printer and owning the print data being sent to the printer. These users are not authenticated by the TOE or otherwise known to the TOE. The authorized users known to the TOE are the administrators only.

3.2.1 Threats Addressed by the TOE

The threats below are addressed by the TOE.

Threat	Description
T.ACCOUNT	Security relevant actions occur without awareness by administrators. Lack of accountability of security relevant events of user or system processes may lead to failure in identifying possible security violations.
T.ADMIN	An attacker could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error or other actions.
T.BYPASS	An attacker may bypass TOE security functions to gain access to resources or information protected by the TOE.
T.DATA	An attacker may gain unauthorised access to print data of other users or any other information protected by the TOE via user error, system error or a technical attack.

3.2.2 Threats Addressed by the TOE Environment

The threats below must be countered by procedural measures and/or administrative methods.

Threat	Description
TE.PASS	An attacker may bypass the TOE to access resources or resources protected by the TOE by attacking the underlying operating system in order to gain access to TOE resources and information.
TE.USAGE	The TOE may be configured, used and administered in an insecure manner, allowing an illegitimate user gaining access to resources or information protected by the TOE.

3.3 Organisational Security Policies

There are no organisational security policies for this TOE or the TOE environment.

4 SECURITY OBJECTIVES

The security objectives provide a concise statement of the intended response to the security problem. It will describe which security needs will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

4.1 Security Objectives for the TOE

The following security objectives for the TOE will be satisfied by technical (IT) countermeasures implemented by the TOE.

Objective	Description
O.ACCOUNT	The TOE must ensure that TOE administrators can subsequently be held accountable for their security relevant actions.
O.AUTH	The TOE must ensure that administrators are identified and authenticated before being granted access to the TOE mediated resources.
O.AUTHORIZE	The TOE must provide the ability to specify and manage access rights to administrative functions and objects managed by the TOE and shall enforce them.
O.BYPASS	The TOE security policy enforcement functions must be invoked and succeeded before access to TOE objects and services are allowed.
O.DATA	The TOE must ensure that access to print data from a user is protected by the TOE preventing access from any other user.

4.2 Security Objectives for the IT environment

The following are the non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they do not require the implementation of functions in the TOE. These security objectives are assumed to be in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in the TOE security environment.

Objective	Description
OE.NOEVIL	The TOE administrators are trustworthy to perform the actions in accordance with security policies and not to interfere with the abstract machine, making sure that the TOE, its clients and the TOE environment are competently installed and administered.
OE.PHYSICAL	The TOE is operated in a physically secure environment to which only authorized administrators (operator, key operator and service operator) have access. This includes physical access to the default operator panel, the print server and the LAN B network, which only the service operator may access.
OE.TIME	The TOE environment must ensure a reliable time function to support the generation of audit records.
OE.NETMAN	The TOE environment must ensure that the TOE is properly installed and connected to a well-managed network, which separates and limits the access to the user network (LAN C / D) the operator network (LAN A) and the service network (LAN B).
OE.FILTER	The TOE environment shall provide an IP filtering capability configured to restrict access to authorized service ports of the TOE.
OE.ITENV	Functions in the TOE environment related to memory management, program execution, access control and privilege management provided by the underlying OS as well as functions related to printer language interpretation that are part of the TOE environment are working correctly and have no undocumented security critical side effects on the security functions of the TOE.

Objective	Description
OE.COMM	The communication links between the Operator Panel task of the TOE and operator and service panels in the TOE environment are protected from unauthorized modification and disclosure of communication data.
OE.PROTECT	The communication between print clients / network management servers and the SRA3 controller is protected against disclosure.
OE.CLIENT	Only the standard operator panel and the service panel may request the access ticket. Further operator panels may be added, but are not allowed to obtain an access ticket.

5 IT SECURITY REQUIREMENTS

This chapter contains the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that must be satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and Evaluation Assurance Level (EAL) 3 assurance components from Part 3 of the CC, augmented with ALC_FLR.2 for flaw remediation. In addition the Security Functional Requirements (SFRs) for the TOE IT-environment are described.

5.1 TOE Security Functional Requirements

This section identifies and specifies the SFR components that the TOE is intended to meet for the purposes of this CC evaluation. All of these SFR components are chosen from Part 2 of the CC to directly or indirectly (i.e., via a functional component dependency) satisfy the security objectives for the TOE, summarized in Table 1.

The following table gives an overview of the functional components from the Common Criteria Part 2 that are relevant for this TOE.

Component	Component Name
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_RVM.1	Non-bypassability of the TSP

The following paragraphs give an overview of the functional requirements listed in the table above with respect to the TOE. They serve as an introduction to the detailed definition of the functional requirements, which are presented in the next section.

Class FAU contains the security requirements associated with audit generation and audit review. These requirements are needed to maintain accountability of the authorized administrators and to be able to identify certain types of attacks, such as password guessing. It is represented by the FAU_GEN.1 for the generation of events, FAU_SAR.1 for the review.

Class FDP contains the security requirements associated with the user data control. User data consists of printer data that are sent to the TOE and other data that are produced by the printer about its state and presented over SNMP. The requirements for protection of the printer data is covered by an information flow policy in FDP_IFC.1 and FDP_IFF.1. It is also covered by the requirement for residual information protection FDP_RIP.1. The network access control to the TOE, to SNMP data and to get the access ticket is covered by the access control policy in FDP_ACC.1 and FDP_ACF.1 (b and c respectively).

Note: FDP_ACC.1a and FDP_ACF.1a are part of the environment.

Class FIA contains requirements for the identification and authentication of users accessing the TOE and its data. The administrators are the only users that are known to the TOE as shown in FDP_ATD.1. These administrators must be identified and authenticated FIA_UAU.1 and FIA_UID.1. In order to limit password guessing attacks there is the requirement for authentication failures FIA_AFL.1 and a password policy as in FIA_SOS.1.

Class FMT contains requirements for secure management of the TSF and TSF data. The requirements for the security roles are defined by FMT_SMR.1 and the requirements for the management functions available to these roles are defined in FMT_SMF.1. FMT-SMF.1 identifies the user management, the password policy management and the network access control management. The management of the security functions and TSF data are covered by FMT_MOF.1. The static attribute initialisation and management of security attributes is covered by FMT_MSA.3 and FMT_MSA.1 respectively. This includes the management of user data and network access control data.

Class FPT contains requirements for the integrity and management of the mechanisms that provide the TSF and to the integrity of TSF data. The TSF data covered by this class of requirement is the non-bypassability of the TSP.

Operations that are completed on the SFR components are indicated throughout this section by the use of ***bold italic*** text. The iteration operation has been performed for FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3. The SFR components are identified by adding small-caps letters, e.g. FMT_MSA.1a and FMT_MSA.1b. Application notes that have been added after the requirements are identified as underlined text.

5.1.1 Class FAU Security audit

5.1.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***not specified*** level of audit; and

c)

- ***Adding, deleting or editing users***
- ***Change user (user identification and authentication)***
- ***Requesting the access ticket***
- ***Modifying ticket access rights (allowed IP-addresses)***
- ***Enabling or disabling external SNMP access***
- ***Modifying external SNMP access rights (allowed IP-addresses)***
- ***Setting the time.***

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***none***.

Note: The event log used for all types of security and non-security relevant events is used.

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***service operators*** with the capability to read ***all audit information*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2 Class FDP User data protection

5.1.2.1 FDP_ACC.1b Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***Ticket Access Control SFP*** on ***the external IT entities that can communicate over the network interfaces of the TOE using RMI***.

Note: This policy restricts on which IP addresses operators are allowed to perform administration, i.e. from which IP addresses the update ticket can be requested. This applies to the administrative network interface LAN A. Requesting the access ticket via LAN B is not subject to any restrictions.

5.1.2.2 FDP_ACC.1c Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***SNMP Access Control SFP*** on ***the external IT entities that can communicate over the network interfaces of the TOE using SNMP***.

Note: The policy restricts external SNMP access to certain addresses. This applies to all network interfaces.

5.1.2.3 FDP_ACF.1b Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Ticket Access Control SFP*** to objects based on the following ***list of subjects and objects***:

- ***Subject: incoming RMI request; Attribute: IP address***
- ***Object: network interface; Attribute: allowed IP addresses***

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

- ***Access using RMI to perform update operations is only permitted from IP-addresses that are allowed to obtain the update ticket***

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***Read access to the RMI interface is always possible***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***no further rule***.

Note: even from allowed IP-addresses, the access ticket may only be obtained if no other administrator of the same or a higher level currently is holding the ticket. The access ticket may be requested by both operator and service panels.

5.1.2.4 FDP_ACF.1c Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***SNMP Access Control SFP*** to objects based on the following ***list of subjects and objects***:

- ***Subject: incoming external SNMP request; Attribute: IP address, community***
- ***Object: network interface; Attribute: IP address for accepting SNMP***
- ***Object: community; Attribute: access right (Read/write or Read only)***

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

- ***Access using SNMP is only permitted from IP-addresses being allowed***
- ***The access rights are the ones associated with the matching community name***

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 ***rule that no access will be given to non-matching community names***.

Note: external SNMP access is given based on the IP addresses, the access rights on the community strings. Each community string has its own access rights (e.g., SNMP GET and SET operations). It is possible to give access to all IP addresses or to deny any external SNMP access. The IP addresses are given as hostnames or as an IP number sequence. For this SFR there is a SOF claim, being SOF-basic

5.1.2.5 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***Print Data information flow control SFP*** on ***all data coming in on the print data interface***.

Note: There may be certain information that is derived from the print data, such as print job name or number of pages printed and statistics that will not be subject to the Print Data information flow SFP. This is a well-defined type and very limited amounts of information. This is therefore considered covered channels, which is outside of the scope of an EAL3 evaluation.

5.1.2.6 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the ***Print Data information flow control SFP*** based on the following types of subject and information security attributes: ***data being printer data, which is all data coming in on the print data interface***.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***print data coming into the TOE will only flow to the printer head and not be visible on any other TOE external interface***.

FDP_IFF.1.3 The TSF shall enforce the ***no additional information flow control SFP rules***.

FDP_IFF.1.4 The TSF shall provide the following ***no additional SFP capabilities***.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***none***.

Note: There are commands in the printer languages that allow certain information in the printer to be sent back to the user. This information is limited to printer status information and does not contain user data to be printed by the printer.

5.1.2.7 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***allocation of the resource to*** the following objects: ***print data***.

Note: This is associated with resources holding print data only. This does not apply to print data resources that are explicitly cached on the local hard drive, e.g. logos or fonts. These resources can be printed by any user that is able to print in the same print language. The system will not purge these resources. The resources have to be explicitly removed by the key operator.

5.1.3 Class FIA Identification and authentication

5.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***one*** unsuccessful authentication attempts occur related to ***authentication of administrators***.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***delay the authentication of that user name with one second***.

5.1.3.2 FIA_ATD.1 User attribute definition

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

- ***User name***
- ***Role***

- ***Password***
- ***Privileges***

Note: The roles are uniquely identified by the level. The user name may not necessarily be the name of the user, but rather the name of the role such as operator or key operator. In case of multiple operators or key operators, they must be given individual names such that accountability can be maintained.

5.1.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***the minimum password policy constraints, defined by the following attributes:***

- ***Must be at least 8 characters long,***
- ***Must include at least 1 numerical or symbol character***
- ***Must not contain more than 2 equal characters in a row***
- ***Passwords are case-sensitive***
- ***Last three passwords must not be reused***
- ***Validity: 90 days***

Note: This policy must be activated by the service operator, but not configured in any other way. When activated, it applies to all administrator roles. For this SFR there is a SOF claim, being SOF-basic.

5.1.3.4 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- ***connection to the RMI and loading the control panels***
- ***obtaining an access ticket***
- ***turning off the printer***
- ***viewing the network settings***
- ***viewing the online help***

on behalf of the user to be performed before the user is authenticated.

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

Note: This applies to the network interfaces to which the administrator can connect to operate the TOE using the control panels. Excluded is any SNMP access since SNMP operations are not subject to any authentication of TOE users. External SNMP access is given, provided the request is coming from an allowed IP address and the community string is matching.

5.1.3.5 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- ***connection to the RMI and loading the control panels***
- ***obtaining an access ticket***
- ***turning off the printer***
- ***viewing the network settings***
- ***viewing the online help***

on behalf of the user to be performed before the user is identified.

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

Note: See the application note under FIA_UAU.1 above.

5.1.4 Class FMT Security management

5.1.4.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***modify the behaviour of*** the functions ***listed below*** to ***an authorised administrator:***

- ***user management (other users)***
- ***change the own user profile (password and language)***
- ***configuration of operator access (for the operator panel)***
- ***configuration of external SNMP access***

Note: These functions are available to any administrator with sufficient privileges. The interface used for performing the operations is listed after each function. Any user that has the privilege to change the user information can do so, but will be limited to give away the privileges they have themselves.

An administrator can only add or remove users with a role on a user level that is lower than the level of the administrator. This means that although key administrators can give any other administrator all the privileges that key operator possesses, he cannot add new key operators, only operators.

5.1.4.2 FMT_MSA.1a Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***Ticket Access Control SFP*** to restrict the ability to ***modify*** the security attributes ***IP addresses allowed to obtain the update ticket*** to ***service operators***.

Note: Ticket access control is restricting the ability of operators to make any changes to security attributes. In addition certain roles are restricted to change the security attributes. Using the template roles, only the service operator may modify the addresses allowing network access (operator update access). However, any administrator can be given such rights.

5.1.4.3 FMT_MSA.1b Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***Ticket Access Control SFP*** to restrict the ability to ***modify*** the security attributes ***IP addresses allowed to perform SNMP operation*** to ***administrators***.

Note: Ticket access control is restricting the ability of operators to make any changes to security attributes. In addition certain roles are restricted to change the security attributes. Using the template roles, administrators (operator, key operator and service operator) may modify the addresses allowing external SNMP access.

5.1.4.4 FMT_MSA.3a Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the ***service operators*** to specify alternative initial values to override the default values when an object or information is created.

Note: With restrictive values is meant that no access is given to any IP address to gain the ticket, allowing only local update access from the console used for installation.

5.1.4.5 FMT_MSA.3b Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the ***administrators*** to specify alternative initial values to override the default values when an object or information is created.

Note: With restrictive values means that no external SNMP access is given for any IP addresses.

5.1.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- ***User management (of administrators) including password management***
- ***Password policy management (activation or deactivation)***
- ***Network access control management***

5.1.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***operator, key operator and service operator***.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Class FPT Protection of the TSF

5.1.5.1 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.

5.2 TOE Security Assurance Requirements

The target assurance components for this TOE are those for EAL3 augmented with ALC_FLR.2, as specified in Part 3 of the CC. The following table provides an overview of the assurance components that form the assurance level for the TOE:

Assurance class	Assurance components
Configuration management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 1, Security Assurance Components

5.3 Security Functional Requirements for the IT Environment

5.3.1 Class FDP User data protection

5.3.1.1 FDP_ACC.1a Subset access control

FDP_ACC.1.1 The **IT environment** shall enforce the ***Network Access Control SFP*** on ***the external IT entities that can communicate over the network interfaces of the TOE using TCP/IP***.

Note: The policy restricts network access to certain protocols and ports. This applies to all network interfaces available, i.e. LAN A, LAN B and LAN C / D.

5.3.1.2 FDP_ACF.1a Security attribute based access control

FDP_ACF.1.1 The **IT environment** shall enforce the ***Network Access Control SFP*** to objects based on the following ***list of subjects and objects***:

- ***Subject: TCP/IP request; Attribute: Protocol (TCP or UDP), Port number***
- ***Object: network interface (LAN A, LAN B or LAN C / D); Attribute: none***

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

- ***Inbound network access is only permitted on the interfaces as follows (protocol and port):***
  - ***LAN A: TCP/21, TCP/80, UDP/161, TCP/5077, TCP/5078, TCP/31337, TCP/31338, TCP/31339***
  - ***LAN B: TCP/21, TCP/80, TCP/135, TCP/139, TCP/5077, TCP/5078, TCP/5079, TCP/31337, TCP/31338, TCP/31339, all UDP ports***
  - ***LAN C / D: UDP/161, TCP/5001, TCP/9100***
- ***Outbound connections are not restricted***

FDP_ACF.1.3 The **IT environment** shall explicitly authorise access of subjects to objects based on the following additional rules: ***none***.

FDP_ACF.1.4 The **IT environment** shall explicitly deny access of subjects to objects based on the ***rule that no access will be given to network access attempts not matching these rules***.

Note: Network access is given based on this static rule. No administrator can make changes to this rule.

5.3.2 Class FPT Protection of the TSF

5.3.2.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The **IT environment** shall be able to provide reliable time stamps for use by the TSF.

Note: Reliable time stamps are provided by the Microsoft embedded NT operating system. This is considered part of the TOE environment. However, the management of the time is part of the TOE and is performed by the service role using the service panel.

6 TOE SUMMARY SPECIFICATION

This chapter provides a description of the TOE security functions and assurance measures, which meet the TOE security requirements specified in chapter 5.

6.1 TOE Security Functions

6.1.1 SF.AUDIT – Security audit function

The audit generation function generates entries of security relevant events to the event log file in the SRA3 Controller. The functions generating the events are located in different parts of the TOE. The event log is used for registering events that are relevant for service of the TOE, including the security relevant events. The security function SF.AUDIT only describes the security relevant events.

Following is a description of the security relevant events (as identified in FAU_GEN.1.1) and how they are identified in the event log:

- **Start-up and shutdown of the audit function**
- **Adding, deleting or editing users**
- **Change user (user identification and authentication)**
- **Requesting the ticket**
- **Modifying ticket access rights (allowed IP-addresses)**
- **Enabling or disabling external SNMP access**
- **Modifying external SNMP access rights (allowed IP-addresses)**
- **Setting the time**

The audit function is for each event recording the type of event, the date and time, subject identity (in case of operator actions) and outcome of the event. The type of event, date and time are registered in its own field for each event. The subject identity and outcome of the event is recorded as part of the data associated with the event.

Note: operator actions are identified as “BdfChange” and are in the event log data listing “Client” and “User” specifying the client interface name (panel name) and the operator name.

6.1.2 SF.IA – Identification and authentication

Identification and authentication is provided to the administrator over the operator or service panel using the menu “[00]General →User”. Authentication of administrators prevents unauthorized enabling of remote administration as well as access to internal traces.

The operator / service panel is available to the administrator before authentication has been performed. The TOE always starts from a state that is “Logged off”. The administrator must then login to the TOE. It is also possible for a new operator to perform a login that will automatically logoff the previous operator, for example when the operator panel is handed over from one administrator to another. For this reason the user identification and authentication is called “User Change” since it changes the status of the operator panel from acting on behalf of one (or none) user to another. The user identity (which may be identical to a user name) is selected from the panel, and the password for that user will then be typed into the appropriate field.

If the password doesn’t match the user identity selected, logon is refused and a window with a warning message will be shown followed by a delay of at least one second. This will be repeated until the authentication succeeds.

Passwords are subject to the password policy described in FIA_SOS.1, which states that passwords must have a certain size and must be composed of certain different characters.

6.1.3 SF.MANAGEMENT – Security management

The administrative interfaces, .i.e. the operator panel and the service panel, use Java Remote Method Invocation (RMI) to interact with the TOE. These Java methods are then sent to the TOE for execution. The privileges of the administrator determine which submenus are available in the operator or service panel.

There are two interfaces available. The operator panel is available to the operator, key operator and service, while the service panel is intended for the service only. Most of the management functions they present are not security related, but related to the operation and management of the printer system. Only the security management aspects are described here.

Operator Panel and Service Panel management functions:

- User management is available under "[00]General →User management" which allows the authorized administrator to add, delete and edit users.
- Change the own user profile is possible using "[00]General →User" which allows the user to change the (own) user profile, such as changing the password and the language of the interface.
  The password change can be performed once the user is logged in using the menu tree of the operator panel or service panel. This requires the user to type the old password and to type in the new password twice. If the new password doesn't fulfil the password policy, the password change will not take place and a warning will be shown.
- Hosts allowed to obtain an access ticket are configured using the operator panel "[00]General →Security →Network management".
- Configuration of external SNMP access is done using "VarioStream →Configuration →Emulations →SNMP configuration". This allows an administrator to activate or deactivate external SNMP, to specify the communities for which read/write or read only access is allowed and to specify the host names from which requests are accepted. Any hosts or just a list of accepted hosts may be given.
- Access to the Printer MIB via LAN C / D is enabled separately via "VarioStream →Configuration →Channels →Channel A" ("Permit Printer MIB access").
- Viewing / export of (security) audit (log) information via the service panel (VS9000 →Error documents →Event Log) as XML or CSV files.

Read access to audit information is available to all administrators[9]. Erasing audit data is only possible for the service operator via the TOE environment.

6.1.4 SF.TICKETACCESS – Ticket access control

The SF.TICKETACCESS will restrict update (write) access to printer settings to administrators currently holding the access ticket. Requests for the access ticket are restricted to certain IP addresses. Read access is always possible for an authenticated administrator. Both operator and service panels may request the access ticket.

6.1.5 SF.SNMPACCESS – SNMP access control

The SF.SNMPACCESS will restrict external SNMP access (via the Printer MIB), which is available for standard network management within a company network. Access will be restricted to specified IP addresses and to the rights associated with the respective SNMP community, as specified in FDP_ACF.1c. Provided the community is matching, an administrator may allow access to all IP addresses, or limit it to a list of addresses. External SNMP access via the (client) LAN C / D is disabled by default. SNMP access on either LAN A, B or on LAN C / D may separately and explicitly be activated by an administrator.

[9] Via the web interface, which has no access restrictions

6.1.6 SF.OR – Object reuse

The security function SF.OR will ensure that any resources holding print data will be cleared from content when allocated. This is to ensure that no print data will be accessible in the TOE after being printed. This is done to all resources holding print data and which are re-allocated.

This is associated with resources holding print data only, and does not apply to print data resources that are explicitly cached on the local hard drive, e.g. logos or fonts. These resources can be printed by any user that is able to print in the same print language. The system will not purge these resources by itself. The resources have to be explicitly removed by an operator. Any operator is allowed to remove resources.

6.1.7 SF.PRINTFLOW – Printer information flow

This is to ensure that print data received by the SRA3 Controller will only be transferred to the print head. This feature is not configurable, which also prevents an authorized administrator to redirect any print data to any other external interface. Since the LAN C / D interface is a dedicated network for submitting print data, any data that is submitted on LAN C / D is considered print data.

The security function SF.PRINTFLOW works in conjunction with SF.OR that prevents print data from being disclosed by re-allocation of resources holding print data.

6.1.8 SF.ROLES – Role based administration

Administrators of the TOE have different rights and privileges (i.e. which entries of a user are visible and/or changeable), defined by their role (*operator*, *key operator* and *service*).

The privileges are assigned to each administrator. The access rights are divided into menu tree (visible / not visible) and elements (read only / read write) and enforced via the operator / service panel.. Thus, the privileges of administrators are associated with logical management and system operating functions of the GUI.

Each administrator is associated with an authorization level, defining his authority to modify other administrative accounts. An administrator may only create (i.e., select a user template), edit or delete other users with a lower authorization level.

Default configurations exist for the predefined roles of operator, key operator and service operator. The service operator may access all existing menu items and change the options and parameters they provide. The *service* menus are not available to the *operator* and *key operator*, and an *operator* may not access the *user management* menu. While no user is logged in, it is possible to change the language settings and view the network configuration of the SRA3 Controller. The access ticket may always be requested, regardless whether a user is logged in or not.

6.2 TOE Assurance Measures

This chapter describes the measures the developer has taken to achieve the desired EAL3 augmented assurance level. These assurance requirements provide, primarily via review of supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

a) Confirmation of effective configuration management

b) Confirmation of product delivery and installation procedures

c) Confirmation of the life-cycle security in the development environment

d) Confirmation that the guidance documentation is adequate

e) Verification of a sample of the vendor functional testing

f) Verification of the developer's analysis for vulnerabilities and resistance against obvious penetration attacks

g) Independent functional testing

To define the assurance measures claimed to satisfy the security assurance requirements specified in chapter 5.2, a mapping is provided between the security assurance requirements (SARs) and the assurance measures, which are intended to satisfy the assurance requirements. As shown in Table 3, the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

SAR	Assurance Measure
ACM_CAP.3	Two CM tools are used for the relevant documentation. PVCS (Poly Version Control System) is used for the controller source code and operating system extensions and Continuus for the Java source code of the operator panel. These tools provide the necessary authorisation control mechanism that is used in the TOE development.
ACM_SCP.1	All source code and test cases are checked into the CM systems, test result logs are also maintained under CM. Third party software that is used in the product is also checked into the CM. The design documentation being part of the assurance measures are under PVCS.
ADO_DEL.1	The TOE is delivered and installed by Océ service technicians following delivery procedures and using checklists. This documentation is release specific.
ADO_IGS.1	The installation, generation, and start-up procedures are covered by the delivery procedures described in ADO_DEL.1.
ADV_FSP.1	There is a functional specification available, identifying and describing all externally visible interfaces. This is a top-level document referring to a number of standards and other design documentation.
ADV_HLD.2	There is a high-level design available, identifying and describing all subsystems and the internal and externally visible interfaces. This consists of a top-level document referring to other high-level design documentation.
ADV_RCR.1	This is covered by Informal correspondence demonstration providing a correspondence between the Security Target and the security functions and interfaces in the functional specification as well as in the high-level design.
AGD_ADM.1	There is an operator guide available to the operators and the key operators, describing the specific printers. In addition there are guidance and required training and testing available for the Océ service operator. For the secure installation and operation there is a security guide.
AGD_USR.1	There is a user guide available describing how an end user can use the printer. There are however no security relevant issues in this guide since the user is not known to the TOE and doesn't interact with any TSF.
ALC_DVS.1	The development security is covered by company wide security procedures and specific measures for logical protection in the development environment.
ALC_FLR.2	Flaw remediation measures are implemented having a well-defined point of contact to which service and customers can report potential security flaws. Defects and their status are tracked within the problem tracking tool. A dedicated website notifies customers of updates to the TOE that implement corrections due to identified flaws.
ATE_COV.2	Detailed test plans are produced to test the functions of the TOE. Those test plans include an analysis of the test coverage, an analysis of the functional interfaces tested and an analysis of the testing against the high-level design
ATE_DPT.1	See ATE_COV.2 above.
ATE_FUN.1	Testing is performed in a test framework, replicating the range of printer platforms as defined by the ST. Test results are documented such that the test can be repeated.
ATE_IND.2	The TOE and an equivalent set of resources are provided to the evaluation facility in a manner suitable for testing.
AVA_MSU.1	This is addressed by the guidance documentation described under AGD_ADM.1.
AVA_SOF.1	The TOE has two mechanisms with strength-of-function claims. The authentication mechanism for user authentication and the access control for SNMP requests. For these mechanisms a strength-of-function analysis has been done, which has been

SAR	Assurance Measure
	documented in a separate report.
AVA_VLA.1	There is a separate document called vulnerability analysis that contains the developer vulnerability analysis, describing Océ's approach to identify vulnerabilities as well as the results of the findings.

7 PP CLAIMS

This Security Target does not claim conformance with any Protection Profile.

8 RATIONALE

The rationale chapter demonstrates how the security objectives of the TOE are met and how objectives, threats and security functions relate to each other. The rationale section will identify which security functions contribute to which objectives and identify which threats are countered by the individual security functions.

8.1 Security Objectives Rationale

8.1.1 Security Objectives Coverage

The following table provides a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat and that each threat is countered by at least one objective, assumption or policy.

Table 2 Objectives related to Threats and Assumptions

	T.ACCOUNT	T.ADMIN	T.BYPASS	T.DATA	TE.PASS	TE.USAGE	A.NETMAN	A.NOEVIL	A.PHYSICAL	A.TIME	A.ITENV	A.COMM	A.PROTECT	A.CLIENT
O.ACCOUNT	X													
O.AUTH		X												
O.AUTHORIZE		X												
O.BYPASS			X											
O.DATA				X										
OE.NETMAN	X	X				X	X							
OE.NOEVIL						X		X						
OE.PHYSICAL		X	X		X				X					
OE.TIME	X									X				
OE.FILTER		X	X		X									
OE.ITENV			X								X			
OE.COMM			X									X		
OE.PROTECT				X									X	
OE.CLIENT	X	X	X											X

8.1.2 Security Objectives Sufficiency

Below is a rational for the security objectives sufficiency in meeting the threats and assumptions of the TOE and the TOE environment, since there are no organisational security policies.

Table 3, Threats, Assumptions and Policies are Related to Security Objectives

Environment	Is addressed by
T.ACCOUNT	O.ACCOUNT requires that TOE administrators are accountable for their security relevant actions. OE.NETMAN ensures that no other access will be given to the service network of LAN B than to the service operator. OE.CLIENT ensures that only authorized users request write access to administrative functions, since

Environment	Is addressed by
	only the standard operator panel or the service panel (which are protected by A.PHYSICAL) are permitted to obtain an access ticket. OE.TIME ensures that every audit record has a correct time stamp.
T.ADMIN	O.AUTH requires that the TOE administrators are identified and authenticated before being granted access to the TOE mediated resources. O.AUTHORIZE requires that TOE must provide the ability to specify and manage as well as enforce access rights to administrative functions and objects managed by the TOE, thereby ensuring that operator has very limited rights, while other administrators may be given more access rights. OE.NETMAN requires that the network is well managed, by giving only limited access to the LAN A and no access to LAN B other than to the service operator. OE.FILTER also limits access to specific network services of the TOE on the different LANs. OE.PHYSICAL requires the physical protection of LAN B, the default operator panel and the print server, thus avoiding a set of possible attacks. OE.CLIENT ensures that only authorised users request access to administrative functions.
T.BYPASS	O.BYPASS requires that the TOE security policy enforcement functions must always be invoked and succeed before access to TOE objects and services is allowed. It prevents the user from circumventing the TOE security functions. OE.FILTER enforces that certain network services are available only on specific LANs, thus ensuring that no unauthorized user can access these services from the wrong LAN. OE.PHYSICAL requires that physical access to the TOE is possible only for authorized administrators. OE.ITENV requires that the TOE environment provides secure and orderly functions for privilege management. OE.COMM requires that communication links between the Operator Panel task of the TOE and operator and service panels in the TOE environment are protected against unauthorized modification and disclosure of communication data. OE.CLIENT ensures that only authorised users request access to administrative functions.
T.DATA	O.DATA requires that access to print data from a user is protected by the TOE preventing access from any other user. OE.PROTECT requires that communication between print clients / network management servers and the SRA3 controller is protected against disclosure.
TE.PASS	OE.PHYSICAL requires that physical access to the TOE, the default operator panel and the print server is possible only for authorized administrators. OE.FILTER ensures that no unwanted network services of the operating system can be exposed on the LAN.
TE.USAGE	OE.NETMAN requires that networks are well managed and separate from each other, allowing only access to LAN A to authorized administrators and access to LAN B only is allowed for service operators. OE.NOEVIL requires that all administrators (operators, key operators and service operators) are trustworthy and trained in accordance with their tasks.
A.NETMAN	OE.NETMAN requires that the TOE environment will ensure that the TOE is connected to a well-managed network, which limits the access to administrative LAN, only allowing administrators to LAN B and limiting LAN A to a well managed environment.
A.NOEVIL	OE.NOEVIL requires that TOE administrators are trustworthy to perform the actions in accordance with security policies and not to interfere with the abstract machine, making sure that the TOE, its clients and the TOE environment are competently installed and administered.
A.PHYSICAL	OE.PHYSICAL requires that the TOE, the default operator panel, the print server and LAN B are operated in a physically secure environment to which only authorized administrators have access.
A.TIME	OE.TIME requires that the TOE environment provide a reliable time function.
A.ITENV	OE.ITENV requires that the TOE environment provides secure and orderly

Environment	Is addressed by
	functions for memory management, program execution, access control, privilege management as well as for printer language interpretation.
A.COMM	OE.COMM requires that communication links between the Operator Panel task of the TOE and operator and service panels in the TOE environment are protected against unauthorized modification and disclosure of communication data.
A.PROTECT	OE.PROTECT requires that communication between print clients / network management servers and the SRA3 controller is protected against disclosure.
A.CLIENT	OE.CLIENT requires that only the standard operator panel and the service panel may request the access ticket.

8.2 Security Requirements Rationale

8.2.1 Security Requirements Coverage

The table below shows a mapping of Security Functional Requirements for the TOE and the TOE environment to Security Objectives for the TOE and the TOE environment. Following the mapping, a rational discussion is given on how each Security Objective is addressed by the corresponding Security Functional Requirements.

The *italic* text used in the table represents those functional components that are met by the TOE environment.

Table 4, TOE Security Objectives Mapped to the Security Functional Requirements

	O.ACCOUNT	O.AUTH	O.AUTHORIZE	O.BYPASS	O.DATA	OE.TIME	OE.FILTER
FAU_GEN.1	X						
FAU_SAR.1	X						
FDP_ACC.1a				*X*			*X*
FDP_ACC.1b			X				
FDP_ACC.1c			X				
FDP_ACF.1a				*X*			*X*
FDP_ACF.1b			X				
FDP_ACF.1c			X				
FDP_IFC.1					X		
FDP_IFF.1					X		
FDP_RIP.1					X		
FIA_AFL.1		X					
FIA_ATD.1		X					
FIA_SOS.1		X					
FIA_UAU.1		X					
FIA_UID.1		X					
FMT_MOF.1			X				
FMT_MSA.1a			X				
FMT_MSA.1b			X				
FMT_MSA.3a			X				
FMT_MSA.3b			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPT_RVM.1				X			
FPT_STM.1	X					X	

Table 5, TOE Security Objectives and the Rationale for Mapping to the SFRs

Objective	**Is fulfilled by the SFRs**
O.ACCOUNT	FAU_GEN.1 ensures that audit events are generated for security relevant events; FAU_SAR.1 ensures that these events are available to authorized administrators; *FPT_STM.1*ensures that a reliable time stamp for these events is given.
O.AUTH	FIA_AFL.1 ensures that attackers against the TOE does not have unlimited number of authentication attempts; FIA_ATD.1 ensures that for all users, the necessary user data are provided to enforce the authentication function;

Objective	Is fulfilled by the SFRs
	FIA_SOS.1 ensures that passwords are selected with a certain quality, preventing easy to guess passwords from being selected; FIA_UID.1 and FIA_UAU.1 ensures that administrators are identified and authenticated before access is given to the TOE.
O.AUTHORIZE	FDP_ACC.1b and FDP_ACF.1b ensure that network access is restricted to administrators to perform administrative update operations based on the IP address; FDP_ACC.1c and FDP_ACF.1c ensure that external SNMP access is only given for certain IP addresses and for matching community strings. FMT_MOF.1 ensures that the modification of the security behaviour of certain security functions is restricted to authorized administrators; FMT_MSA.1a ensures that the management of the network access rights is restricted to certain authorized administrators; FMT_MSA.1b ensures that the management of the external SNMP access rights is restricted to certain authorized administrators; FMT_MSA.3a and FMT_MSA.3b ensures that initial restrictive values are provided for the ticket access control and SNMP access control functions; FMT_SMF.1 ensures that security management functions are provided to the administrators; FMT_SMR.1 ensures that user can be associated with the roles necessary for the security management of the TOE.
O.BYPASS	FPT_RVM.1 ensures that security policy enforcement functions are invoked and succeed before each function is allowed to proceed so the access control is always enforced. In addition *FDP_ACC.1a* and *FDP_ACF.1a* enforces that only allowed protocols and ports are allowed access, for which security functions such as identification and authentication are activated. These security requirements work together to prevent bypassing and circumvention of TOE security policy.
O.DATA	FDP_IFC.1 and FDP_IFF.1 ensures that print data, i.e. all data coming from the print data interface, will not be visible on any other interface than being printed; FDP_RIP.1 ensure that any previous information content of resource for print data is made unavailable when resources are allocated to print data.
OE.TIME	FPT_STM.1 ensures that a reliable time stamp is provided by the TOE environment.
OE.FILTER	FDP_ACC.1a and FDP_ACF.1a together ensure access control to network services offered by the TOE or its underlying operating system, filtering out any network traffic that does not meet the filter settings. This access control is provided by the TOE environment (Windows NT) on the level of IP protocols and ports. Different filters for different LANs ensure that only the allowed services for every LAN can be accessed.

8.2.2 Functional Security Requirements Sufficiency

As stated in the tables above, every objective is addressed by at least one security functional requirement and every FSR is necessitated to cover at least one objective. By showing that the stated security objectives are met, we are able to demonstrate the suitability and sufficiency of the chosen SFRs.

The requirements are mutual supportive, i.e. there exist no conflicts between different requirements, and they are consistent in defining a proper set of demands on the functionality the TOE is supposed to offer.

8.2.3 Rationale of Evaluation Assurance Level

This security target claims EAL3 augmented with ALC_FLR.2. This seems to be appropriate since the TOE is supposed to thwart attackers of limited resources. The EAL3 assurance requirements bring enough assurance elements for the TOE, operating within its environment as described in this document.

Furthermore, the EAL 3 assurance level augmented with ALC_FLR.2 is technically feasible and achievable based on the requirements on life-cycle support, development documents, secure delivery procedure, and configuration management. It is appropriate to satisfy users' expectations.

8.2.4 Rationale of SOF-basic

The TOE mechanisms will resist technical attacks by unauthorized users. The TOE mechanisms will also resist user errors, system errors, or non-malicious actions by authorized users. The environment also assumes that those individuals who have authorized physical access to the TOE are trusted not to behave maliciously.

Consequently, a level of strength of function basic (SOF-basic) which indicates that a function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a basic attack potential is consistent with the security objectives of the TOE. This claim applies to identification and authentication as specified in FIA_SOS.1, using the described settings, and satisfied by SF.IA, as well as to the access control function FDP_ACF.1c satisfied by SF.SNMPACCESS.

8.2.5 Security Requirements Dependency Analysis

Following the Common Criteria and choosing security requirements to be met by a TOE, certain dependencies on other security requirements may arise. The following section shows whether these dependencies are resolved and, in case they are not, gives reasons for that.

8.2.5.1 Security Functional Requirements Dependency Analysis

Note: SFRs on the TOE Environment are shown in *italics*. If there are alternative requirements to resolve a dependency the valid ones are put in **bold** letters. The rational for unresolved dependencies are described as part of the table.

Table 6, Security Functional Requirements Dependencies for the TOE and TOE Environment

Component	Dependencies/comment	Resolved
FAU_GEN.1	*FPT_STM.1*	Resolved by the TOE environment.
FAU_SAR.1	FAU_GEN.1	Yes
FDP_ACC.1a	*FDP_ACF.1a*	Yes
FDP_ACC.1b	FDP_ACF.1b	Yes
FDP_ACC.1c	FDP_ACF.1c	Yes
FDP_ACF.1a	*FDP_ACC.1a*, FMT_MSA.3	*FDP_ACC.1a*, but not FMT_MSA.3 since the access control rules are hard coded and cannot be configured by any administrator.
FDP_ACF.1b	FDP_ACC.1b, FMT_MSA.3a	Yes
FDP_ACF.1c	FDP_ACC.1c, FMT_MSA.3b	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, but not FMT_MSA.3 since no attributes needed to be initialized for the print data information flow.
FDP_RIP.1	No dependencies	–
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	No dependencies	–
FIA_SOS.1	No dependencies	–
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	No dependencies	–

Component	Dependencies/comment	Resolved
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	Yes
FMT_MSA.1a	[**FDP_ACC.1b** or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	Yes. The access control policy for network access to obtaining the access ticket (FDP_ACC.1b) is configurable.
FMT_MSA.1b	[**FDP_ACC.1c** or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	Yes. The access control policy for external SNMP (FDP_ACC.1c) is configurable.
FMT_MSA.3a	FMT_MSA.1a, FMT_SMR.1	Yes
FMT_MSA.3b	FMT_MSA.1b, FMT_SMR.1	Yes
FMT_SMF.1	No dependencies	–
FMT_SMR.1	FIA_UID.1	Yes
FPT_RVM.1	No dependencies	–
FPT_STM.1	No dependencies	–

8.2.5.2 Demonstration of Mutual Support between the Security Requirements

The requirements FAU_GEN.1, FAU_SAR.1 define the requirements for the audit system by specifying the audit events, in relation to the other security functional requirements. The association of each audit event with user identities is consistent with the use of the identification and authentication function (FIA_UID.1 and FIA_UAU.1), so that FAU_GEN.1 has a basis for associating the events to user identities causing that event. In order to record the time and date of the events, FAU_GEN.1 requires a reliable time-stamp, which is provided by FPT_STM.1 (provided by the IT environment). The requirements FAU_SAR.1 provides service operators with the capability to read all the audit information generated by the audit function.

The requirements for access control is limited by the static access control policy defined in FDP_ACC.1a, restricting only certain protocols and port to be accessed on the network interfaces. This requirement is addressed by the TOE environment. The requirements for access control are further defined by the access control policy in FDP_ACC.1 (b and c) providing subset access control to network access from the administrative network, based on the access for SNMP and right to make updates using the operator panel. FDP_ACC.1b is for access to ticket (update lock), and FDP_ACC.1c is for SNMP access rights. The subjects and object, as well as the security attributes are defined in FDP_ACF.1a (addressed by the TOE environment), FDP_ACF.1b and FDP_ACF.1c. The subset information flow control (FDP_IFC.1) provides protection to the print data sent by the end users. FDP_IFF.1 will make sure that no printer data will occur on any other interface than on the printer head. The printer data is identified as such since the end users have their own interface for submitting print data to the TOE. The requirement for residual information protection FDP_RIP.1 will ensure that the printer data will not remain in the TOE after it has been printed.

The requirements for identification and authentication are addressed by FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1 and FIA_UID.1. The timing of identification and authentication is specified by FIA_UID.1 and FIA_UAU.1. Authentication failures are handled by FIA_AFL.1 by detecting and delaying further login after a certain number of failed consecutive login attempts. The attributes, including passwords, associated with individual users are specified in FIA_ATD.1. Restrictions on the passwords used for user authentication is specified by FIA_SOS.1, preventing administrators to select weak or easy to guess passwords.

The management functions are specified by FMT_SMF.1, specifying management functions for password management, user management, access control management and audit management. The roles identified by the TOE are specified in FMT_SMR.1.

The management of the authentication function is described in FMT_MOF.1 and the management of passwords, password policy, access control information and audit options is covered by FMT_MOF.1. These management functions are also restricted to specific identified, authenticated and authorized administrators. For the discretionary access control, management of the security attributes is made by

FMT_MSA.1 (a and b) and restricted attributes are specified by FMT_MSA.3 (a and b) for the network access (ticket) and for the external SNMP access respectively.

FPT_RVM.1 defines that the TSP enforcement functions are invoked and succeeded before any other function is allowed to proceed, preventing bypassability of the TSP.

The ability of the TOE security functions to fulfil the security functional requirements is demonstrated by the internal consistency of the security functional requirements, shown in section 8.3.1, and by the demonstration that each of these security requirements are being satisfied with one or more TOE security functions in combination as explained below in section 8.3.

8.2.5.3 Security Assurance Dependencies Analysis

The assurance level selected within this TOE is EAL3 augmented with ALC_FLR.2. Since ALC_FLR.2 does not have any dependencies and each EAL does not have any unresolved dependencies all dependencies are considered satisfied.

8.3 TOE Summary Specification Rationale

The TOE security functions work together to satisfy the security functional requirements. Below is a justification for each SFR, how the related security functions meets the requirements and as well for the sum of security assurance requirements.

8.3.1 Security Functions Rationale

This section is intended to provide a demonstration that the TOE security functions satisfy all TOE SFRs included in the ST. This is accomplished by mapping the TOE security functions onto the TOE SFRs by *Table 7*~~*Table 7*~~, which shows that:

- Each TOE SFR is mapped onto at least one TOE security function, and
- Each TOE security function is mapped onto at least one TOE SFR.

Note that FPT_STM.1, FDP_ACC.1a and FDP_ACF.1a are TOE environment security functional requirements and are satisfied by the TOE environment.

Table 7 SFR related to Security Functions

	SF.AUDIT	SF.IA	SF.MANAGEMENT	SF.TICKETACCESS	SF.SNMPACCESS	SF.OR	SF.PRINTFLOW	SF.ROLES
FAU_GEN.1	X							
FAU_SAR.1			X					
FDP_ACC.1b				X				
FDP_ACC.1c					X			
FDP_ACF.1b				X				
FDP_ACF.1c					X			
FDP_IFC.1							X	
FDP_IFF.1							X	
FDP_RIP.1						X		
FIA_AFL.1		X						
FIA_ATD.1								X

	SF.AUDIT	SF.IA	SF.MANAGEMENT	SF.TICKETACCESS	SF.SNMPACCESS	SF.OR	SF.PRINTFLOW	SF.ROLES
FIA_SOS.1		X						
FIA_UAU.1		X						
FIA_UID.1		X						
FMT_MOF.1			X					X
FMT_MSA.1a			X					
FMT_MSA.1b			X					
FMT_MSA.3a			X					
FMT_MSA.3b			X					
FMT_SMF.1			X					
FMT_SMR.1								X
FPT_RVM.1		X		X	X			

The following table shows that the IT security functions (SF), as specified in the TOE Summary Specification, meet all the security functional requirements (SFR) for the TOE and work together to satisfy the TOE security functional requirements.

SFR	Security Functions (TOE Summary Specification)
FAU_GEN.1	The requirement for generation of audit events is satisfied by the security function SF.AUDIT, which will generate audit records for the specified events to an audit file. The audit record containing the timestamp is produced by SF.AUDIT, relying in the time stamps provided by the TOE environment (FPT_STM.1).
FAU_SAR.1	The requirement to provide read capability to all audit information to the service operator is satisfied by the security function SF.MANAGEMENT.
FDP_ACC.1b	The requirement for access control is satisfied by the function SF.TICKETACCESS. All requests for the *access ticket* are subject to access control of SF.TICKETACCESS for ticket access.
FDP_ACC.1c	The requirement for access control is satisfied by the function SF.SNMPACCESS. All SNMP operations are subject to access control of SF.SNMPACCESS for external SMNP access.
FDP_ACF.1b	The requirement is satisfied by the function SF.TICKETACCESS for ticket access, which enforces the ticket access control SFP based on the IP address by comparing with the permitted list of IP addresses.
FDP_ACF.1c	The requirement is satisfied by the function SF.SNMPACCESS for external SMNP access, which enforces the SNMP access control SFP based on the IP address (by comparing with the permitted list of IP addresses) and a community string (which grants access based on the access rights associated with different community strings).
FDP_IFC.1	The requirement is satisfied by SF.PRINTFLOW, which enforces that print data only will be transferred from the print user to the print head.
FDP_IFF.1	The requirement is satisfied by SF.PRINTFLOW, which enforces the print data information flow SFP based on the incoming interface of the print data.
FDP_RIP.1	The requirement is satisfied by SF.OR, which ensures that print data is erased and

SFR	Security Functions (TOE Summary Specification)
	not kept in any storage available for any user after a print job has been completed.
FIA_AFL.1	The requirement is satisfied by the function SF.IA, which enforces that authentication failures are followed by a delay.
FIA_ATD.1	The requirement for user attributes is being fulfilled by SF.ROLES. However, the user attribute information is used by the function SF.IA.
FIA_SOS.1	The requirement for the verification of secrets is fulfilled by the user name / password mechanisms being part of SF.IA. The password policy constraints for a secure configuration are given. The administrator has the ability to specify different values, which will apply for all administrators of the TOE.
FIA_UAU.1	The requirement for administrator authentication is being fulfilled by identification and authentication function SF.IA.
FIA_UID.1	The requirement for administrator identification is being fulfilled by identification and authentication function SF.IA.
FMT_MOF.1	The requirement is being fulfilled by SF.MANAGEMENT and SF.ROLES, allowing administrators to perform management of the security functions behaviour according to their respective level. This includes modifying the behaviour of the identification and authentication function, by specifying the password policy.
FMT_MSA.1a	The requirement is being fulfilled by SF.MANAGEMENT, allowing the service operator to change which network addresses can be given update (ticket) access rights, in accordance with the Ticket Access Control SFP.
FMT_MSA.1b	The requirement is being fulfilled by SF.MANAGEMENT, allowing an administrator to change which network addresses can be given external SNMP access rights, in accordance with the SNMP Access Control SFP.
FMT_MSA.3a	The requirement for restrictive values is fulfilled by SF.MANAGEMENT, not giving access to the ticket from any network addresses that haven't been explicitly activated by the service operator.
FMT_MSA.3b	The requirement for restrictive values is fulfilled by SF.MANAGEMENT, not giving external SNMP access from any network addresses that haven't been explicitly activated by an administrator.
FMT_SMF.1	The requirement for the TSF to provide management functions is being satisfied by the security function SF.MANAGEMENT.
FMT_SMR.1	The requirement for roles maintained by the TOE, the operator, key operator and service is satisfied by the security function SF.ROLES, which provides a privilege model and role templates for each of the roles.
FPT_RVM.1	The requirement for non-bypassability of the TSP is a security property of the TOE that is satisfied by the combination of the architecture and security functions, ensuring that the access control functions are being invoked before access is granted.

The table above shows how the security functions work together to satisfy the security functional requirements.

8.3.2 Assurance Measures Rationale

In section 6.2 the TOE summary specification includes a justification that the TOE security assurance requirements are met by the assurance measures.

8.3.3 Minimum Strength of Function Rationale

The TOE mechanisms will resist technical attacks by operators or unauthorized users. The TOE mechanisms will also resist user errors, system errors, or non-malicious actions by authorized users. Resistance to sophisticated types of attacks, when such resistance is required, is provided by the TOE operational environment. The environment also assumes that those individuals who have authorized physical access to the TOE are trusted to not behave maliciously.

Consequently, a level of strength of function basic (SOF-basic), which indicates that a function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a low attack potential is consistent with the security objectives of the TOE. This claim applies to identification and authentication as specified in FIA_SOS.1, using the described settings, and satisfied by SF.IA; and to access control for SNMP access as specified in FDP_ACF.1c, using both IP addresses and community string, and satisfied by SF.SNMPACCESS.

8.4 PP Claims Rationale

No claims to any Protection Profile are made.