Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0369-2007

for

Océ SRA Controller
Version 3, Bundle 8.02

from

Océ Printing Systems

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0369-2007

Printer-Controller

Océ SRA Controller Version 3, Bundle 8.02

from

Océ Printing Systems

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 3 augmented by ALC_FLR.2 (Flaw reporting procedures)**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, May 16th, 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement has been signed by the national bodies of:

Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Océ SRA Controller, Version 3, Bundle 8.02 has undergone the certification procedure at BSI.

The evaluation of the product Océ SRA Controller, Version 3, Bundle 8.02 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Océ Printing Systems
Siemensallee 2
85586 Poing

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on May 16th, 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product Océ SRA Controller, Version 3, Bundle 8.02 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Océ Printing Systems
Siemensallee 2
85586 Poing

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The TOE is the Océ Scalable Rasterized Architecture (SRA) Controller, Version 3, Bundle 8.02 used in the high-performance printer Océ VarioStream 9000.

The Océ SRA3 Controller, Bundle 8 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.

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. In the evaluated configuration these user interfaces are connected to two different network interfaces.

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.

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

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: 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.

The IT product Océ SRA Controller, Version 3, Bundle 8.02 was evaluated by atsec information security GmbH. The evaluation was completed on April 24th, 2007. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Océ Printing Systems
Siemensallee 2
85586 Poing

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3+ (Evaluation Assurance Level 3 augmented by ALC_FLR.2 (Flaw reporting procedures)). The following table shows the augmented assurance components.

Requirement	Identifier
EAL3	TOE evaluation: methodically tested and checked
+: ALC_FLR.2	Life Cycle Support – Flaw reporting procedures

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following table.

The following TOE SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security Audit**
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP	**User data protection**
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	**Identification and authentication**
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

Security Functional Requirement	Addressed issue
FMT	**Security Management**
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	**Protection of the TOE Security Functions**
FPT_RVM.1	Non-bypassability of the TSP

Table 2: SFRs for the TOE taken from CC Part 2

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FPT	**Protection of the TOE Security Functions**
FPT_STM.1	Reliable time stamps

Table 3: SFRs for the IT-Environment

Note: only the titles without the iterations of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6], chapter 5.1 and 5.3.

The TOE Security Functional Requirements in table 2 of this report are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
SF.AUDIT	Security audit function
SF.IA	Identification and authentication
SF.MANAGEMENT	Security management
SF.TICKETACCESS	Ticket access control
SF.SNMPACCESS	SNMP access control
SF.OR	Object reuse
SF.PRINTFLOW	Printer information flow
SF.ROLES	Role based administration

Table 4: Security Functions

Note: only the titles of the TOE Security Functions are provided. For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed 'basic' (SOF-basic) for specific functions as indicated in the Security Target [6], chapter 2.6.9.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The assets controlled by the TOE are information and resources, such as print data being transmitted and TSF data being maintained.

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, i.e. operator, key operator and service operator. 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 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.
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.

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.

Table 5: Threats to be countered by the TOE

Please note that no Organisational Security Policies have been defined in the ST.

1.5 Special configuration requirements

The TOE will be operated in only one configuration that will be set up by an Océ service engineer during installation. All necessary administrative actions that have to be taken to set up the TOE in the evaluated configuration are described in the Security Guide [8].

1.6 Assumptions about the operating environment

The assumptions about the operating environment are listed in the following table:

Assumption	Addressed issue
A.NOEVIL	Trustworthy TOE administrators
A.PHYSICAL	Physically secure environment
A.TIME	TOE environment provides a reliable time source
A.NETMAN	Properly installation and connection to a well-managed network
A.ITENV	Correctly working functionality in the TOE environment
A.COMM	Protected communication links to the TOE
A.PROTECT	Protected print data flow
A.CLIENT	Restricted request for the access ticket

Table 6: Assumptions about the operating environment

Note: only the titles of the assumptions are provided. For more details please refer to chapter 4 of this report or the Security Target [6], chapter 3.1.

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.

Table 7: Threats to be countered by procedural measures and/or administrative methods

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Océ SRA Controller, Version 3, Bundle 8.02

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Océ SRA Controller	Version 3 Bundle 8.02	Installed on the printer
2	DOC	Security Guide for SRA3 Controller (Bundle 8) [8]	2007-02 08.03.2007	Hard copy
3	DOC	Service Documentation English V1.8 [9]	1.8 10.2006	PDF on DVD for service engineer
4	DOC	Operating Manual Océ VarioStream 9000 [10]	2006/08 11.2006	Hard Copy
5	DOC	Océ high volume printers in a customer LAN environment [11]	1.0 07.2003	Hard Copy
6	DOC	Online help documentation [12]	01.08.03 04.04.2007	Built-in help-system “Online-Help”

Table 8: Deliverables of the TOE

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

To install and configure the TOE such that it matches the configuration described in the Security Target the service technician has to follow the guidance provided in the Security Guide [8]. The Security Guide [8] contains a chapter providing guidance how to install and configure the TOE in accordance with the Security Target.

3 Security Policy

The Océ SRA3 Controller, Bundle 8 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.

Therefor the TOE provides the following functionalities:

- Role based administration – Roles with different capabilities are used to administer and service the system.
- Password controlled access for administration – All TOE administrative access via the RMI server, using either operator or service panels, is password protected.
- Password quality control features – Password quality enforcement for administrative accounts will allow only passwords of a certain quality to be used.
- Security audit of operator actions – This will give accountability to operator actions to identify which operator has performed what operation when.
- 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.
- Object reuse protection for the data stream and resources (fonts, logos, etc.) – As the data stream normally is not cached on disk, the Virtual Memory Manager (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.
- 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.
- Network access control for management and monitoring devices – Network ACLs are used to guard administrative access via the network.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

The following assumtions regarding the usage of the TOE have to be fulfilled:

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.

4.2 Environmental assumptions

The following assumtions about the TOE environment have to be fulfilled:

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.

4.3 Clarification of scope

The Target of Evaluation is limited to the software that has been developed by Océ and is running on the SRA3 Controller card.

Windows NT embedded is used as the underlying operating system. It has been configured to improve performance and security. The operating system is part of the TOE environment.

Date and time information is provided to the operating system by the underlying hardware. Web server and file transfer services are provided by the operating system.

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. Proper IP filters are set up at installation time and are never changed during normal operation of the TOE.

5 Architectural Information

The TOE consists of three subsystems:

Operator Panel Task:
The Operator Panel task provides an API for (graphical) user interfaces, such as the operator panel and the service panel. The central component is the System Parameter Manager, which dispatches all incoming and outgoing requests.

Diagnostics Task:
The diagnostic task consists of the Service Eventlog Agent and the Remote Diagnostic Process and implements various tools for system audit and review and for system maintenance.

Functional Code / Print Flow:
The printing workflow consists of the following steps:

- Receive print data from external sources
- Interpretation and analysis of data
- Raster pages to be printed in temporary storage as bitmap
- Transfer of bitmap to the character generator of the printer

6 Documentation

The documentation [8] – [12] is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

7 IT Product Testing

7.1 Developer Testing

Developer testing took place in November 2006 on the developer's site in Poing.

The developer follows a twofold approach for testing the TOE:

1. Direct tests of the TSF
2. Indirect tests of the TSF

1.) is performed by conducting an adequate number of manual tests on a printing system comprising the SRA3 controller running the TOE in the evaluated configuration

2.) is performed by

1. reviewing the design of the respective TOE functionality
2. deducing the correct behaviour by observing print results when running the tests on a printer (or printing system) simulation involving the SRA3 controller running the TOE in the evaluated configuration

For direct testing (1), which took place a the developer's site in Poing, a VS9000 printing system comprising SRA3 controller running the TOE was available on the test floor. A simulation system comprising the SRA3 controller running the TOE is available at the developer's offices. The used test systems were configured according to the evaluated configuration as required by the ST [6], the Security Guide [8] and the test plan.

The developer provided a depth- and coverage analysis, that showed that the TSF, all TSFI, and all High Level Design subsystems have been tested appropriately.

The developer provided results for both test approaches that show that all developer tests yielded positive (OK) results.

7.2 Evaluator Independent Testing

The test effort of the evaluator comprised the re-run of selected vendor test cases and test cases derived or created by the evaluator.

Testing has been performed on the developer's site in Poing in November 2006.

The developer provided a VS9000 printing system including the SRA3 controller with the TOE installed (Bundle 08.02). The used test system was configured according to the evaluated configuration as required by the ST [6], the Security Guide [8] and the test plan.

The evaluator selected a test subset that recruited itself from the vendor tests. The following TSF were subject to this testing: SF.AUDIT, SF.IA, SF.MANAGEMENT, SF.TICKETACCESS, SF.SNMPACCESS and SF.ROLES. All tests being part of the subset have been tested successfully.

The evaluator performed the design review for the SF.PRINTFLOW TSF by means of an interview with a developer. The evaluator found the explanation gained during that interview consistent with the document and the claims in the TSF, thus the test was successful.

In addition, the evaluator performed variations of vendor test cases using different machines, parameters or evaluator defined tests using test software different than the vendor used (SNMP browsers).

The evaluator testing, including selected developer tests and evaluator tests yielded the expected test results, hence the overall result is: OK.

7.3 Evaluator Penetration Testing

The evaluator performed independent penetration testing that was focused on recent development in terms of flaws for networked services as well as TOE configuration and implementation errors.

The TOE behaved according to the specification and no indications of flaws have been found.

8 Evaluated Configuration

The SRA 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.

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.

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

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 to non-security relevant information
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 [8] for the SRA3 Controller.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL 3+.

The verdicts for the CC, Part 3 assurance components (according to EAL 3 augmented by ALC_FLR.2 and the class ASE for the Security Target evaluation) are summarised in the following table:

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	CC Class ADO	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS

Assurance classes and components		Verdict
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 9: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL3 augmented by ALC_FLR.2.

The following TOE Security Functions fulfil the claimed Strength of Function:
SF.IA – Identification and authentication
SF.SNMPACCESS – SNMP access control

The results of the evaluation are only applicable to the Océ SRA Controller, Version 3, Bundle 8.02 (for identification of the TOE components please refer to chapter 2 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [8] – [12] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ACL	Access Control List
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
IT	Information Technology
LAN	Local Area Network
PP	Protection Profile
SRA	Scalable Rasterized Architecture
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
VMM	Virtual Memory Manager

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0369-2007, Version 1.7, 01.03.2007 , Security Target for Océ SRA Controller, Version 3, Bundle 8.02, Océ Printing Systems GmbH

[7] Evaluation Technical Report, Version 5, 23.04.2007, Evaluation Technical Report Océ SRA Controller Version 3, Bundle 8.02 (confidential document)

[8] Security Guide for SRA3 Controller (Bundle 8), Version 2007-02, 08.03.2007, Océ Printing Systems GmbH

[9] Service Documentation English V1.8, Version 1.8, 10.2006, Océ Printing Systems GmbH

[10] Operating Manual Océ VarioStream 9000, Version 2006/08, 11.2006, Océ Printing Systems GmbH

[11] Océ high volume printers in a customer LAN environment, Version 1.0, 07.2003, Océ Printing Systems GmbH

[12] Online help documentation, Version 01.08.03, 2007-04-04, Océ Printing Systems GmbH

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”