

Certification Report

BSI-DSZ-CC-0517-2009

for

**Océ Digital Access Controller (DAC) R10.1.5
for use in the Océ VarioPrint 1055, 1055 BC,
1055 DP, 1065, 1075, 2062, 2075, 2075 DP
printer/copier/scanner products**

from

Océ Technologies B.V.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



Deutsches

erteilt vom



IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0517-2009

Océ Digital Access Controller (DAC) R10.1.5

for use in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products

from Océ Technologies B.V.
PP Conformance: None
Functionality: product specific Security Target Common Criteria
Part 2 conformant
Assurance: Common Criteria Part 3 conformant
EAL 2 augmented by
ALC_FLR.1



Common Criteria
Recognition
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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 20 February 2009

For the Federal Office for Information Security



SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG¹ 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.....7
 - 1 Specifications of the Certification Procedure.....7
 - 2 Recognition Agreements.....7
 - 2.1 European Recognition of ITSEC/CC - Certificates.....7
 - 2.2 International Recognition of CC - Certificates.....8
 - 3 Performance of Evaluation and Certification.....8
 - 4 Validity of the certification result.....8
 - 5 Publication.....9
- B Certification Results.....11
 - 1 Executive Summary.....12
 - 2 Identification of the TOE.....13
 - 3 Security Policy.....14
 - 4 Assumptions and Clarification of Scope.....14
 - 5 Architectural Information.....15
 - 6 Documentation.....16
 - 7 IT Product Testing.....16
 - 7.1 Test configuration.....16
 - 7.2 Developer Testing.....16
 - 7.3 Evaluator Testing.....16
 - 7.4 Penetration Testing.....17
 - 8 Evaluated Configuration.....17
 - 9 Results of the Evaluation.....18
 - 9.1 CC specific results.....18
 - 9.2 Results of cryptographic assessment.....18
 - 10 Obligations and notes for the usage of the TOE.....19
 - 11 Security Target.....19
 - 12 Definitions.....19
 - 12.1 Acronyms.....19
 - 12.2 Glossary.....20
 - 13 Bibliography.....21
- C Excerpts from the Criteria.....23
- D Annexes.....31

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)⁵ [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998. This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for all Evaluation Assurance Levels (EAL 1 – EAL 7).

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France, the United Kingdom and the Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

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 07 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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition 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 (CCRA). 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>

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 Digital Access Controller (DAC) R10.1.5 for use in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0370-2006.

The evaluation of the product Océ Digital Access Controller (DAC) R10.1.5 for use in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products was conducted by Brightsight. The evaluation was completed on 03 February 2009. The Brightsight is an evaluation facility (ITSEF)⁶ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Océ Technologies B.V.

The product was developed by: Océ Technologies B.V.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

⁶ Information Technology Security Evaluation Facility

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Océ Digital Access Controller (DAC) R10.1.5 has been included in the BSI list of the certified products, which is published regularly (see also Internet: <http://www.bsi.bund.de>) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer⁷ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ Océ Technologies B.V.
St. Urbanusweg 43
PO. Box 101
5900 MA Venlo
The Netherlands

This page is intentionally left blank.

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.

1 Executive Summary

Océ Technologies B.V. produces a wide range of Multifunctional Devices (MFDs) for copying, printing and scanning. MFDs consist of two main parts: a Digital Access Controller (DAC) and a Digital Copier (DC). The DAC consists of two parts, the underlying hardware platform which is not part of the TOE and the software which forms the TOE. The Target of Evaluation (TOE) is the software running on the hardware platform.

The TOE is the Digital Access Controller (DAC) R10.1.5 for use in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/scanner/copier products (see table 2 for detailed information).

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

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
SF.FILTERING	Built-in firewall
SF.JOB_RELEASE	Secure printing
SF.SHREDDING	Overwriting of deleted print job data
SF.MANAGEMENT	Management of TOE Security Functionality
SF.SELFTEST	Checks for failures and integrity during start-up

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The claimed TOE's Strength of Functions 'basic' (SOF-basic) for specific functions as indicated in the Security Target [6], chapter 6.1.2 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.2 – 3.4.

This certification covers the following configurations of the TOE:

- The TOE covers the DAC operating in the security mode 'high (factory default)' as delivered by Océ to the customer.
- The overwrite mechanism has to be enabled for all scan and print jobs.

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 Digital Access Controller (DAC) R10.1.5 for use in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Océ DAC-specific software	R10.1.5	Installed on HW-platform
2	SW	Montvista Linux operating system	Version 4.0.1 (with updates until August 9, 2007 and New-Zealand time-zone fix. These updates are specified in appendix F of the ST [6])	Installed on HW-platform
3	SW	Adobe PS3-PDF Interpreter	Version 3016.103 v.3.1 build #03	Installed on HW-platform
4	SW	Apache HTTP server with SSL support	Apache 2.0.59	Installed on HW-platform
5	SW	OpenSSL	Version 0.9.7I	Installed on HW-platform
6	SW	SAMBA	Version 3.0.25b	Installed on HW-platform
7	SW	PHP	Version 4.4.7	Installed on HW-platform
8	DOC	User Guidance: Océ VarioPrint 1055-75 Job manual [9] Océ VarioPrint 2062 Job manual [10] Océ VarioPrint 2075 Job manual [11] Océ VarioPrint 1055-75 Configuration manual [12] Océ VarioPrint 2062 Configuration manual [13] Océ VarioPrint 2075 Configuration manual [14]	All Code Number 1060061982, Edition 2007, 2.1,	On CD (Code Number 1060061982, Edition 2007, 2.1) together with the MFD or download from the support section from the Océ corporate website (www.oce.com)
9	DOC	Administrator Guidance: Océ System Configuration, On-line help	R10.1.5	HTML pages that are part of the Océ DAC-specific software

Table 2: Deliverables of the TOE

The hardware platform for the TOE consists of:

- An embedded uATX motherboard based PC comprising at a minimum a Via Eden C3 800 MHz processor, 256MB internal RAM, 20GB hard drive
- Generic graphics card and network card supporting 10/100/1000Mbs Ethernet UTP
- Drivers for the PC, graphics card and network card
- USB hardware support

The DAC is customized and installed according to the customer order form and packaged with the MFD into one package. The package is labelled and transported to the customer.

The MFD together with the DAC is installed and configured according to the evaluated configuration at the customer site by Océ Service Technicians.

The customer operator can instruct the TOE to print out a configuration report. This configuration report clearly lists the separate software components and their versions. The customer can compare the configuration report to the Security Target or this Certification Report in order to determine that he received the TOE.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

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

The TOE protects it's own integrity against threats from the LAN, service engineer laptop, USB memory sticks and the Digital Copier to which it is attached through use of a firewall and integrity checks on system files upon system reboot.

The TOE protects the confidentiality of secure print jobs once they have been received by the DAC by storing them until the user authenticates himself to the DAC via a user interface on the DC. The DAC shreds the data after printing is completed.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: Physical protection of the TOE by the environment, secure management of the network to which the TOE is attached and the local physical interfaces of the TOE as well as the allowed MFDs to which the DAC is connected. Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The following diagram indicates the subsystems of the TOE (blue boxes) that implement the security functionality and the external interfaces (black boxes).

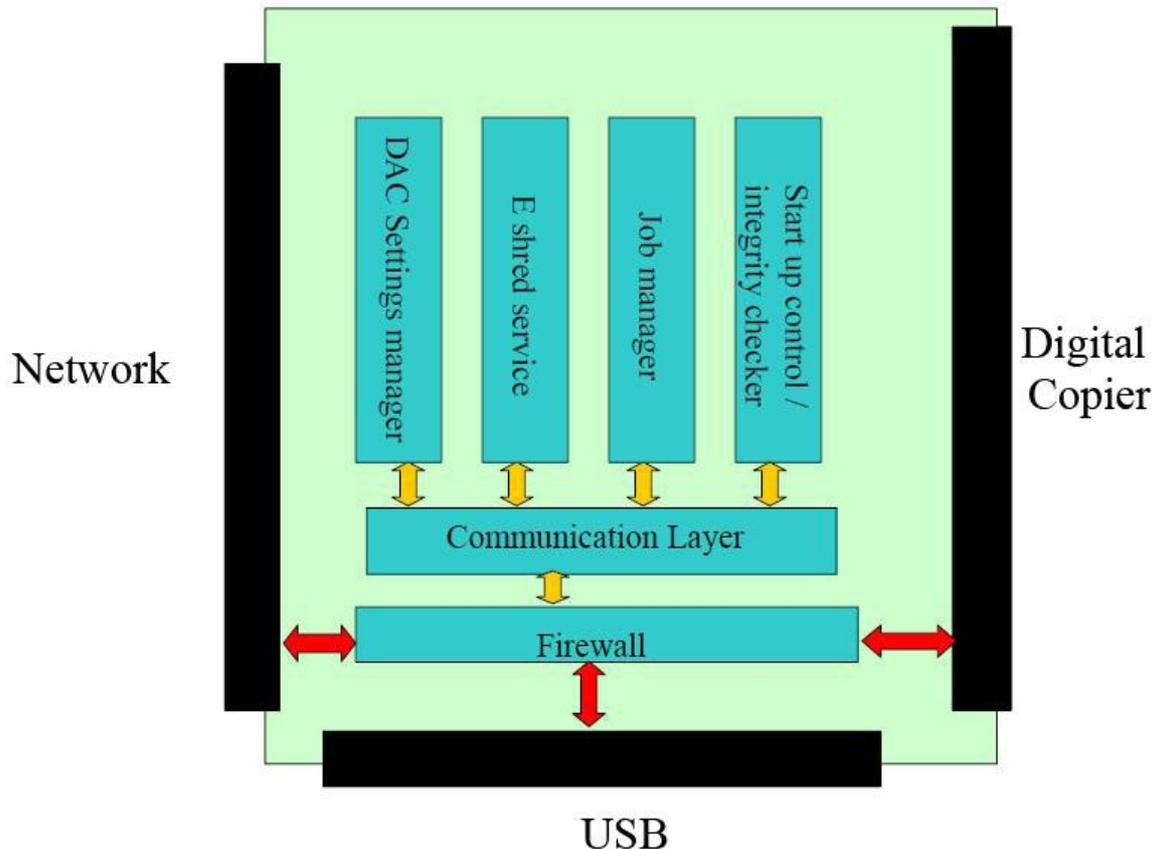


Figure 1: Overview of the TOE subsystems and external interfaces

The subsystems are as follows:

Communication Layer: This subsystem provides the communication functionality between the TOE subsystems and the internal interfaces between the subsystems. In addition, this subsystem provides the communication functionality to the Digital Copier interface.

Firewall: This subsystem provides stateful inspection of the network packets that pass through the network card (both inbound and outbound). It ensures that there is no direct path between the Digital Copier and the network to which the DAC is attached.

Job Manager: This subsystem manages the print and scan jobs that are handled by the DAC. There are four types of job:

- Standard Print Job (D.PRINT_JOB in ST)
- User associated Print Job (D.PRINT_JOB in ST)
- User associated print job with unique PIN(D.SECURE_PRINT_JOB in ST)
- Scan job (D.SCAN_JOB in ST)

DAC Settings manager: This subsystem manages security related settings of the DAC.

Start-up control/Integrity checker: This subsystem performs an integrity check as part of the start-up process when power is applied to the DAC. The DAC file system is checked for inconsistencies.

E-shred service: This subsystem provides the shredding of the job data objects that are handled by the Job Manager subsystem (Standard Print Job, User associated Print Job, User associated print job with unique PIN and Scan job).

The external interfaces are the network interface, the USB-interface and the interface to the Digital Copier.

6 Documentation

The evaluated documentation as outlined in table 2 is provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Test configuration

Tests were performed with the DAC connected to the Océ VarioPrint 1055 and 2075.

The security mode was 'High' (factory default) with E-shredding switched on.

The following software components are used:

- MontaVista Linux Version 4.0.1, with updates until August 9, 2007 and New-Zealand time-zone fix. These updates are specified in appendix F of the ST [6]
- Océ Digital Access Controller -specific software release 10.1.5
- Adobe 3016.103, v3.1 build #3
- Apache: 2.0.59 with OpenSSL 0.9.7l
- Samba 3.0.25b
- PHP 4.4.7

7.2 Developer Testing

The developer has performed all necessary functional tests for the Security Functions. The depth of testing corresponded with the depth of the level of the Functional Specification. All Security Functions have been tested at least once.

In addition, the developer has performed extensive vulnerability tests that exceeds the attack potential required by EAL2.

7.3 Evaluator Testing

The evaluators repeated all of the developer tests and additionally performed independent evaluator tests. All Security Functions have been tested at least once.

The depth of testing corresponded with the depth of the level of the Functional Specification.

The objectives for the tests are derived from the security functions and are:

- Check that filtering performs conform to the Functional Specification. With all network functionality enabled in security level 'high (factory default)', the firewall should be properly configured. Check that on the external Ethernet connector the firewall only allows certain defined ports.

- Check that the job release function performs conform to the Functional Specification.
- Check that the self-test mechanism performs conform to the Functional Specification.
- Check that the shredding mechanism performs conform to the Functional Specification.
- Check that authentication mechanisms perform conform to the Functional Specification.

All test results were as expected.

7.4 Penetration Testing

Following the developer and evaluator independent vulnerability analysis, the evaluators identified the necessary penetration tests. The evaluators took the functional specification as starting point for the identification of which interfaces and which functions need to be penetration tested. Based on the more detailed knowledge of the high-level design some tests are included additionally.

The evaluators applied a number of publicly available network and vulnerability scanners for the search for obvious vulnerabilities.

All test results were as expected. The security functionality works as expected. The vulnerability tests showed that the TOE is resistant against all tested public known vulnerabilities that were identified on recent internet searching. The network and vulnerability scanners did not revealed vulnerabilities that could be exploited on the level of EAL2.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The DAC can operate in three different security modes: 'high', 'normal' and 'low'. The TOE covers the DAC operating in the security mode 'high (factory default)' as delivered by Océ to the customer. This mode is the initial version of the security mode 'high' and provides a restricted set of functionality that is configured to meet the Security Target claim. Once changed, it is not possible to get the DAC back into the certified configuration ('high (factory default)') by changing the security mode back to 'high'. Changing the operational mode invalidates the claim made in the Security Target.

The remote system administrator must not change the 'Jobs to overwrite' settings. If E-shredding is disabled for 'scan jobs' or 'print jobs without security code', the DAC is no longer in the certified configuration and is no longer able to assure the security of 'scan jobs' and 'print jobs without security code'.

9 Results of the Evaluation

9.1 CC specific results

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.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 2 package as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0370-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following aspects:

- Evaluate that the claimed security functionality is still correctly present in the updated versions of the software parts.
- Evaluate that the firewall settings comply to the new set of allowed protocols and that the built in firewall still protects the TOE as expected.
- Evaluate that the added possibility to hash the PINs for the protected print jobs does not weaken the Security Function for the secure release of print jobs. The hashing of the PINs is not a Security Function for the TOE.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: product specific Security Target
Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
EAL 2 augmented by
ALC_FLR.1
- The following TOE Security Functions fulfil the claimed Strength of Function : basic
SF.JOB_RELEASE and SF.MANAGEMENT

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

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

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
DAC	Digital Access Controller
DC	Digital Copier
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MFD	Multifunctional Device
PC	Personal Computer
PP	Protection Profile
RAM	Random-Access Memory
SAR	Security Assurance Requirements
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair

12.2 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.

13 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.⁸
- [5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website
- [6] Security Target BSI-DSZ-0517-2009, Version 3.3, "Security Target The Océ Digital Access Controller (DAC) R10.1.5, as used in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products", Océ Technologies B.V.
- [7] Evaluation Technical Report, Version 7.0, 19th January 2009, "Evaluation Technical Report Digital Access Controller (DAC) R10.1.5", Brightsight (confidential document)
- [8] Configuration list for the TOE, Version 3.3, 19th January 2009, "Configuration Management List for the Océ Digital Access Controller (DAC) R10.1.5, as used in the as used in the Océ VarioPrint 1055, 1055 BC, 1055 DP, 1065, 1075, 2062, 2075, 2075 DP printer/copier/scanner products", Océ Technologies B.V. (confidential document)
- [9] Océ VarioPrint 1055-75 Job manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [10] Océ VarioPrint 2062 Job manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [11] Océ VarioPrint 2075 Job manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [12] Océ VarioPrint 1055-75 Configuration manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [13] Océ VarioPrint 2062 Configuration manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [14] Océ VarioPrint 2075 Configuration manual, Code Number 1060061982, Edition 2007, 2.1, Océ Technologies B.V.
- [15] Océ System Configuration, On-line help for Océ DAC R10.1.5, version 4.3, Océ Technologies B.V.
- [16] DAC administration guidance for Océ service engineer "Administrating R10.1.5 of the Océ DAC" (Lotus Notes Application), Océ Technologies B.V.

⁸ specifically

- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

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:

- **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.
- **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:

- **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.
- **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:

- **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.
- **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:

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

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 Evaluation Assurance Level Components							by
		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.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.