Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0615-2009

for

Océ PRISMAsync 11.9.75.55
as used in the Océ VarioPrint 41x0 Release 1.3

from

Océ Technologies BV

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0615-2009

Printer Controller

Océ PRISMAsync 11.9.75.55
as used in the Océ VarioPrint 41x0 Release 1.3

from	Océ Technologies BV
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

Common Criteria

The IT product identified in this certificate has been evaluated at an 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, 13 November 2009
For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [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]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[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

2.1 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 the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from 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.

2.2 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 January 2009 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and 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 PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0510-2008. Specific results from the evaluation process BSI-DSZ-CC-0510-2008 were re-used.

The evaluation of the product Océ PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3 was conducted by Brightsight BV. The evaluation was completed on 23 October 2009. The Brightsight BV is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Océ Technologies BV

The product was developed by: Océ Technologies BV

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 PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://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 developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Océ Technologies BV
P.O. 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

The Target of Evaluation (TOE) is the Océ PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3.

The Océ PRISMAsync is a PC-based Multi Function Device (MFD) controller. The Océ PRISMAsync provides a wide range of printing, scanning and copying functionality to the MFD peripherals to which it is connected. The Océ PRISMAsync provides Security Functionality to the MFD.

The Target of Evaluation is a collection of software components (Océ developed software, 3rd party printer language interpreters, Operating System) that use the underlying hardware platform. The TOE is a subset of the complete Océ PRISMAsync (for further details concerning the TOE boundary see chapter 2 of this report and chapter 2.1.1 of the Security Target [6]).

The TOE assumes that its operational environment is a repro-room contained within a regular office environment. Physical access to the operational environment is restricted to TOE operators and Océ service engineers as defined in the Security Target [6], chapter 3.

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 EAL2 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.

There are no SFRs defined which are relevant for the IT-Environment of the TOE.

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

TOE Security Function	Addressed issue
SF.FILTERING	The TOE uses a built-in firewall to block ports that are not needed for the operation of the TOE. In addition no network protocols that are not supported by the evaluated configuration are enabled.
SF.SHREDDING	Once a print, copy or scan job has been deleted, the data is overwritten. It is possible to perform multiple write cycles, with various patterns being applied. At least three write cycles will always take place. The first write cycle starts after the job has been deleted and to improve job throughput performance, all other remaining cycles are done once the TOE enters an idle state. The shredding mechanism supports US DOD 5220-22m and Gutmann algorithms.

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

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 to 3.4.

This certification covers the following configurations of the TOE: The Océ PRISMAsync can operate in two different security modes: 'High' and 'Normal'. The TOE configuration only covers the Océ PRISMAsync operating in the security mode 'High' as delivered by Océ to the customer. This mode provides a restricted set of functionality that is configured to meet the Security Target claim. Changing the operational mode irretrievably invalidates the claims made in the Security Target.

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 PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release/Edition	Form of Delivery
1	SW	Océ PRISMAsync-specific software	11.9.75.55	Pre-installed on the hard disk of the Océ PRISMAsync
2	SW	The Microsoft Windows embedded Operating System	XP with service pack 2 plus the patches listed in the Security Target [6], Appendix F	Pre-installed on the hard disk of the Océ PRISMAsync
3	SW	Adobe PS3-PDF Interpreter	3018	Pre-installed on the hard disk of the Océ PRISMAsync
4	SW	Zoran PCL6 interpreter	IPS6.0.2	Pre-installed on the hard disk of the Océ PRISMAsync
5	SW	Apache Tomcat Web server (with SSL support)	5.5.26	Pre-installed on the hard disk of the Océ PRISMAsync
6	DOC	Océ VarioPrint 4110/4120 Common Criteria certified configuration of the Océ PRISMAsync [9]	2009-09	Electronic document
7	DOC	Océ VarioPrint 4110/4120 Manual type Operating information [10]	2008-11	Electronic document
8	DOC	Océ VarioPrint 4110/4120 Administrator settings and tasks [11]	2009-05	Electronic document
9	DOC	Océ VarioPrint 4110/4120 Security service documentation [12]	2009-10	Electronic document

Table 2: Deliverables of the TOE

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

The 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.

The name of the TOE in the configuration report (Smart Imager) is not the same as the one in the ST (PRISMAsync). However, this is considered to be acceptable since the following remark is made on p. 4 of the guidance document “Océ VarioPrint 4110/4120 Common Criteria certified configuration of the Océ PRISMAsync” [9]: “In the past PRISMAsync was named Smart Imager. It may happen that you still encounter this name, especially in the configuration report or in the about of the Setting Editor. In this case, note that the name Smart Imager refers to the same system as PRISMAsync.”

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 Océ PRISMAsync provides a wide range of printing, scanning and copying functionality to the MFD peripherals to which it is connected. The Océ PRISMAsync provides Security Functionality to the MFD.

The TOE protects two assets: itself and the copy, print and scan job data that it receives. Firstly, the TOE protects it’s own integrity against threats from the LAN to which it is attached through use of a firewall. Secondly, the TOE protects the confidentiality of print, copy and scan job data after they are no longer needed. The Océ PRISMAsync does this by e-shredding the data after they are deleted.

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, management of the network to which the TOE is attached and the local physical interfaces of the TOE. Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

The following diagram indicates the subsystems of the TOE that implement the Security Functionality.

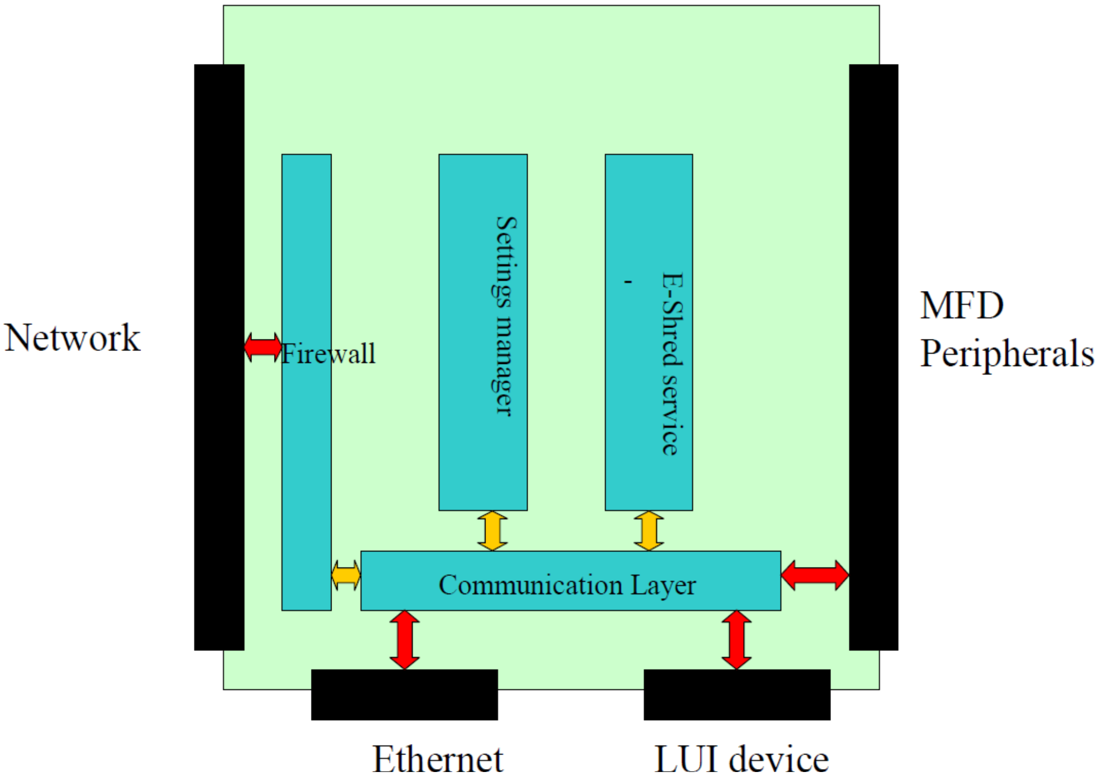

Figure 1: Overview of the TOE subsystems

The four blue boxes indicate the subsystems of the TOE. That are:
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 MFD Peripheral Interface.
Firewall: The firewall subsystem is part of the Windows XP embedded operating system provided by Microsoft. It provides state-full inspection of the inbound network packets that pass through the network card. The firewall settings are not user configurable.
Settings manager: The Settings manager subsystem manages a number of settings that are related to its operation. This subsystem manages security related settings of the Océ PRISMAsync. There are no security-related settings that can be changed by the ordinary users in the configured mode of operation.
E-shred service: The E-shred subsystem provides the shredding of the job data objects (Print Job, Scan job and Copy job).

The external physical interfaces are identified by black blocks. These are the interfaces to the network, the Ethernet, the LUI device and the MFD peripherals. The external logical interfaces are shown by a red arrow. They show the communication path between each subsystem and their associated physical interface to the outside world. The internal interfaces are indicated by orange arrows. They show the internal TSF communication between the subsystems. They show that the internal communication path between each subsystem is through the Communication Layer subsystem.

6 Documentation

The evaluated documentation as outlined in table 2 is being 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 are performed with the Océ PRISMAsync 11.9.75.55 connected to the Océ VarioPrint 4100.

The security mode is ‘High’ (factory default). The following software components are used:

- The Microsoft Windows XP embedded operating system with service pack 2 plus the patches listed in the ST [6], Appendix F.
- Océ PRISMAsync-specific software release 11.9.75.55.
- Adobe PS3-PDF Interpreter, Version 3018
- Zoran PCL6 interpreter, Version IPS6.0.2
- Apache Tomcat web server with SSL support, Version 5.5.26.

7.2 Developer Testing

The depth of testing corresponded with the depth of the level of the Functional Specification. The developer has performed all necessary functional tests for the Security Functions. All Security Functions have been tested at least once. In addition, the developer has performed extensive vulnerability test that exceeds the attack potential required by EAL2. All test results were as expected.

7.3 Evaluator Testing

The evaluator tests are built upon the security functions as defined in ST. The evaluators ran all of the developer tests, as well as independent evaluator tests. In total the following security functions have been tested: SF.FILTERING, SF.SHREDDING and SF.MANAGEMENT.

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

- Check that filtering conforms to the Functional Specification. With all network functionality enabled in security level 'High', the firewall should be properly configured. Check that on the external Ethernet connector the firewall only allows certain defined ports.
- Check that shredding conforms to the Functional Specification.
- Check that the TOE administrator authentication and the Océ service engineer authentication conforms to the Functional Specification.

The depth of testing corresponded with the depth of the level of the Functional Specification. All test results were as expected.

7.4 Penetration Testing

The evaluators took the Functional Specification as starting point for the identification of which interfaces and which Security Functions need to be 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 scanners for obvious vulnerabilities on the network interface.

All test results were as expected. The Security Functionality worked as expected. The vulnerability tests showed that the TOE is resistant against all tested public known vulnerabilities based on recent internet scans. The vulnerability scans did not reveal vulnerabilities that could be exploited on the level of EAL2.

8 Evaluated Configuration

This certification covers the following configuration of the TOE: The Océ PRISMAsync can operate in two different security modes: ‘High’ and ‘Normal’. The TOE configuration only covers the Océ PRISMAsync operating in the security mode ‘High’ as delivered by Océ to the customer. This mode provides a restricted set of functionality that is configured to meet the Security Target claim. Changing the operational mode irretrievably invalidates the claims made in the Security Target.

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 EAL2 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-0510-2008, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change of the external interfaces and the updates of the TOE software components.

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.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. In addition, the following aspects need to be fulfilled when using the TOE:

- The customer should read the Security Target [6] for the assumptions and organisational security policies to create the intended environment of the TOE.
- In order to maintain the CC certified configuration of the TOE, it must never be set in any other security mode than the mode ‘High’.
- The security instruction given by guidance documentation (especially [9] and [12]) have to be followed.

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
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LUI	Local User Interface
MFD	Multi Functional Decive
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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-0615-2009, Version 4.6.2, 08 October 2009, "ST of the Océ PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3 ", Océ Technologies BV

[7] Evaluation Technical Report, Version 4.0, 22 October 2009, "Evaluation Technical Report Océ PRISMAsync 11.9.75.55 as used in the Océ VarioPrint 41x0 Release 1.3", Brightsight BV (confidential document)

[8] Configuration list for the TOE, Version 1.9.2, 08 October 2009, "Configuration Management List for the Océ PRISMAsync Controller R11.9.75.55 as used in the Océ VarioPrint 4110/4120 printer/copier/scanner release 1.3 products", Océ Technologies BV (confidential document)

[9] Océ VarioPrint 4110/4120 Common Criteria certified configuration of the Océ PRISMAsync, Edition 2009-09, Océ Technologies BV

[10] Océ VarioPrint 4110/4120 Manual type Operating information, Edition 2008-11, Océ Technologies BV

[11] Océ VarioPrint 4110/4120 Administrator settings and tasks, Edition 2009-05, Océ Technologies BV

[12] Océ VarioPrint 4110/4120 Security service documentation, Edition 2009-10, Océ Technologies BV

[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

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 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.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.