Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0370-2006

for

Océ Digital Access Controller (DAC) R9.1.6

from

Océ Technologies B.V.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0370-2006

Océ Digital Access Controller (DAC) R9.1.6

from

Océ Technologies B.V.

Common Criteria Arrangement

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

<u>Evaluation Results:</u>

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2 augmented by ALC_FLR.1 (Basic Flaw Remediation)**

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

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

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

Bonn, October 26th, 2006

The Vice President of the Federal Office
for Information Security

IT Security Certified

Hange L.S.

SOGIS - MRA

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

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

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

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

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. 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. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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) R9.1.6 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0325-2006.

The evaluation of the product Océ Digital Access Controller (DAC) R9.1.6 was conducted by Brightsight B.V.. Brightsight B.V. is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Océ Technologies B.V.
P.O. Box 101
5900 MA Venlo
The Netherlands

The certification is concluded with

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

This work was completed by the BSI on October 26th, 2006.

The confirmed assurance package is only valid on the condition that

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

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

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

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-24.

The product Océ Digital Access Controller (DAC) R9.1.6 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Océ Technologies B.V.
P.O. Box 101
5900 MA Venlo
The Netherlands

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

Océ 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 hardwareplatform. The TOE is used with the following Océ products:

- Océ VarioPrint 1055, 1065, 1075, 2062, 2075

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 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.

In comparison to the forerunner evaluation BSI-DSZ-CC-0325-2006 in this evaluation only one configuration exists where the MFDs have an embedded DAC. Furthermore the following changes have been introduced in this re-evalution:

- new Operating System: Montavista Linux 4.0 Professional Version
- only the Ethernet and USB connectors are available (CD-ROM drive removed)
- a fingerprint sensor which is only used during the identification of the user when printing secure print jobs has been added in the environment

The IT product Océ Digital Access Controller (DAC) R9.1.6 was evaluated by Brightsight B.V.. The evaluation was completed on October 12th, 2006. The Brightsight B.V. is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Océ Technologies B.V.
P.O. Box 101
5900 MA Venlo

The Netherlands

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL2+ (Evaluation Assurance Level 2 augmented). The assurance requirements are augmented by the component ALC_FLR.1.

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1	Subset residual information protection
FIA	**Identification and authentication**
FIA_UAU.1	Timing of authentication
FIA_UAU.2	User authentication before any action
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FMT	**Security Management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security Functions**
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_TST.1	TSF testing

Table 1: SFRs for the TOE taken from CC Part 2

Note: Only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7], chapter 5.1.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
SF.FILTERING	The TOE uses a built-in firewall to block ports and ICMP commands that are not needed for the operation of the TOE. In addition all network protocols that are not supported in the security mode 'high' are disabled. By default no traffic is permitted to enter or leave the TOE except for the TCP/IP packets and the restricted ICMP command set via the ports defined in the rule table.
SF.JOB_RELEASE	The TOE verifies the identity and associated PIN code that was sent with the print job when submitted by S.REMOTE_USER with Username/PIN received from S.LOCAL_USER via the DC interface. If verification is successful, the secure print job is released for printing.
SF.SHREDDING	Once a print or scan job has been deleted, the data is overwritten. It is possible to perform multiple write cycles, with various patterns being applied. At least three write cycles will always take place. S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER can choose the moment when the shredding cycle commences. The first write cycle will occur immediately after the print job has completed. The remaining cycles may also take place immediately after the print job has been completed or at the time when the TOE enters an idle state. The shredding mechanism supports US DOD 5220-22m and Gutmann algorithms (for more information see [17] and [18]).
SF.MANAGEMENT	The TOE can be managed in relation to SF.JOB_RELEASE and SF.SHREDDING. In order to gain access, the S.REMOTE_SYSADMIN or S.SERVICE_ENGINEER must authenticate themselves to the TOE. S.SERVICE_ENGINEER does this by entering a password. S.REMOTE_SYSADMIN authenticates himself by entering a password. The TOE is delivered by Océ with pre-configured in the security mode 'high'. This provides the most restrictive set of operational settings.
SF.SELFTEST	During start-up the TOE will check the hard disk files system and the integrity of the software that forms the TOE. If defects in the hard disk files system are detected, the corrupted file system will be automatically repaired. The software includes all executables (operating system executables, Océ authored DAC executables, Third party software executables and DAC system settings). If defects are detected, the corrupted data will be replaced by correct shadow data.

Table 2: TOE Security Functions

For a complete list and definition of the used subjects and objects please refer to the Security Target [7], chapter 3.1.

1.3 Strength of Function

The Strength of Function claim for all the probabilistic functions and mechanisms provided by the TOE is SOF-basic.

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

The following Threats and Organisational Security Policies are defined for the TOE:

Threat	**Description**
T.RESIDUAL_DATA	S.THIEF steals the TOE or parts thereof and retrieves stored or deleted D.SECURE_PRINT_JOB. The motivation for S.THIEF to attack the TOE is low because it requires sophisticated data recovery equipment that can recover data even after the shredding mechanism has executed to recover data that has little value to the attacker.
T.NOSY_USER	S.LOCAL_USER accesses a D.SECURE_PRINT_JOB that does not belong to him/her that is stored in the DAC. The motivation to carry out this attack is low.
T.MALWARE	A S.NETWORK_DEVICE is used by malware that may have entered the TOE's operational environment to launch an attack on the integrity of the TOE. Alternatively S.DIGITAL_COPIER is used by malware to launch an attack on the integrity of S.NETWORK_DEVICE. The motivation to carry out this attack is low.

Table 3: Threats

Organisational Security Policy	**Description**
P.JOB_DELETE	When D.SECURE_PRINT_JOB, D.PRINTJOB and D.SCANJOB objects are no longer needed by the TOE, they will be deleted by the TOE at the earliest available opportunity in a manner that meets a recognised standard.
P.TOE_ADMINISTRATION	The modification of TOE security settings shall be restricted to S.SERVICE_ENGINEER and S.REMOTE_SYSADMIN.

Table 4: Organisational Security Policies (OSPs)

For a complete list and definition of the used subjects and objects please refer to the Security Target [7], chapter 3.1.

1.5 Special configuration requirements

1.5.1 Security mode

By default, Océ delivers the DAC in the highest security mode: indicated by 'Security level: high (factory default)'. This provides the most restrictive set of operational settings.

The remote system administrator must not change the security mode. If the security mode is changed, the DAC is no longer in the certified configuration and is no longer able to assure the security of its objects and itself. 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'.

1.5.2 Authentication

1.5.2.1 Remote system administrator

The Océ system configuration application is password protected.

For the purpose of configuring the DAC prior to deployment, the DAC is delivered with a factory-default password. The remote system administrator must change the password before the DAC is deployed.

The remote system administrator must not use a short or easy-to-guess password. He must use a non-predictable sequence of at least five characters. Additionally to this minimum requirements, the remote system administrator is advised to:

- use a long password - up to 50 characters can be used.
- use a mixture of upper and lower case letters, numbers and punctuation.
- change the password every month.

Log-on to Océ system configuration is blocked for a while after an incorrect password is entered. The blocking interval is increased after successive incorrect entries.

1.5.2.2 Service engineer

The service engineer is a local administrator, and is typically employed by Océ. He has access through an USB interface to a wide range of settings on the TOE and the DC. The service engineer has elevated privileges above those of the user and the system administrator.

The TOE connection is protected with a default password. The service engineer must authenticate himself to the TOE before he is allowed to modify the TOE security settings.

At the first log on the service engineer must change the SDS password to a different value than the default value to keep the DAC Common Criteria Certified. The password must follow the following rules:

- The passwords must have alpha-numeric characters, a combination of numbers and letters.
- The password must have uppercase letters, lowercase letters, and numbers.
- The length of the password must be between 6 and 50 characters.

1.5.3 E-shredding

By default, E-shredding is enabled for all data objects.

The following E-shredding settings can be configured within security mode 'high':

- number of overwrite passes (Default:'3'),
- moment of overwriting (Default: 'Perform first pass at once, the rest in the background').

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'.

1.6 Assumptions about the operating environment

The TOE is intended to be used within a Digital Copier. The following assumptions for the environment of the TOE are made:

Name	**Definition**
A.DIGITAL_COPIER	Attachment of the TOE to a Digital Copier
A.ENVIRONMENT	Regular office environment
A.SECURITY_POLICY	Existing security policy governing the use of IT products in the customer organisation
A.SHREDDING	Shredding for print jobs and scan jobs will not be disabled
A.SLA	Any security flaws discovered in the TOE will be repaired

Table 5: Assumptions for the TOE

Note: Only the titles of the assumptions are provided. For more details please refer to the Security Target [7], chapter 3.2.

1.7 Disclaimers

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Océ Digital Access Controller (DAC) R9.1.6

The TOE is a series of software that runs on a generic off-the-shelf PC (underlying platform). Together this is called the DAC (Digital Access Controller). The DAC is a PC-based MFD-controller (Multi Functional Device) that provides a wide range of printing and scanning functionality to the Digital Copier (DC) of the MFD to which the DAC is connected. The DAC provides security functionality to the DC. It does not provide copy functionality.

2.1 Physical scope of the TOE

The TOE consists of the software parts of the DAC, i.e. the operating system (Montavista Linux 4.0 Professional Version), the DAC-specific software (Océ DAC-specific software release 9.1.6) and the third-party software (Adobe PS3-PDF Interpreter, Version 3016.103 v.3.1 build #03; Apache HTTP server with SSL support, Apache 2.0.55, OpenSSL 0.9.7e (used for remote system administration) and OpenSSL 0.9.7d (used for job forwarding), mod_ssl 2.8.22). The underlying PC infrastructure is not part of the TOE (see also figure 1).

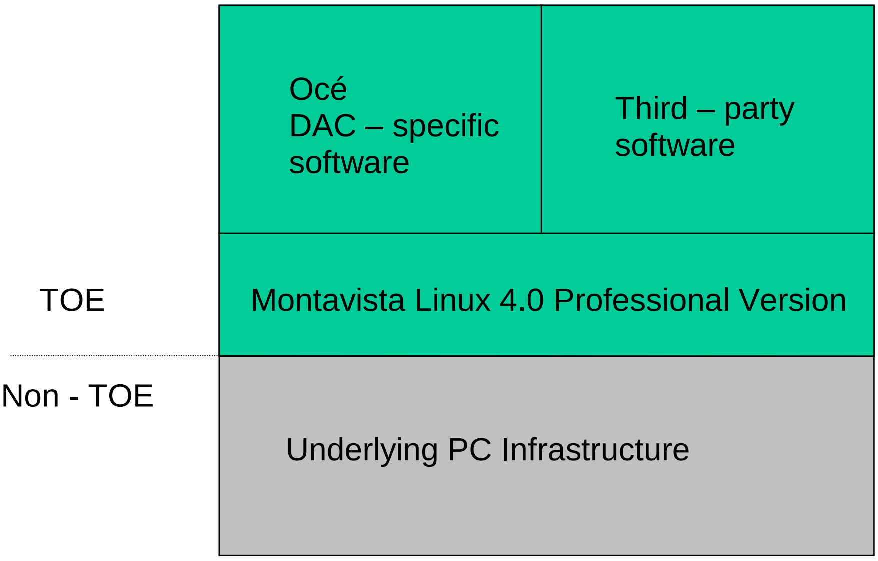
Océ
DAC – specific
software
Third – party
software
TOE
Montavista Linux 4.0 Professional Version
Non - TOE
Underlying PC Infrastructure

Figure 1: Physical scope of the TOE

2.2 TOE deliverables

The following TOE deliverables are provided for a customer who purchases the Océ Digital Access Controller (DAC) R9.1.6:

Underlying platform:

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

Océ Digital Access Controller (DAC) R9.1.6:

1. The Montavista Linux 4.0 Professional Version
2. Océ DAC-specific software R9.1.6
3. Third-party developed software: Adobe PS3-PDF Interpreter, Version 3016.103 v.3.1 build #03; Apache HTTP server with SSL support, Apache 2.0.55, OpenSSL 0.9.7e (used for remote system administration) and OpenSSL 0.9.7d (used for job forwarding), mod_ssl 2.8.22

For the delivery the DAC and the DC are packed to one package and are labelled. When they arrive at the customer the package is checked by the Océ service engineer and then installed according the installation guidance. During the DAC startup, an integrity check is performed. If integrity errors are detected, a complete re-install will be performed.

Accompanying manuals – administrator guidance:

1. Administrator guidance for the system administrator: Océ VarioPrint 1055, 1065,1075, 2062, 2075, Common Criteria Certified configuration of the DAC R9.1.6. Edition 2006-05 [9].

   This document is not delivered to the customer together with the TOE but has to be downloaded from the support section from the Océ corporate website (www.oce.com).
2. The DAC administration guidance for the customer system administrator takes the form of HTML pages. These are part of the Océ DAC-specific software, Version R9.1.6: Océ System Configuration, On-line help [16].
3. The DAC administration guidance for the Océ service engineer takes the form of a Lotus Notes application that is installed on the service engineer’s laptop. The guidance contains an appendix that is identified as “Administrating version R9.1.6 of the Océ DAC” and is a frozen version of the Océ service engineer Lotus Notes application made at the time of product release [19].

Accompanying manuals – user guidance:

1. Job manuals

- Océ VarioPrint 1055-75:
  Job manual Code number 1060028223, Edition 2005-02 [10]
- Océ VarioPrint 2062:
  Job manual Code number 1060028188, Edition 2005-02 [11]
- Océ VarioPrint 2075:
  Job manual Code number 1060028155, Edition 2005-02 [12]

2. Configuration manuals

- Océ VarioPrint 1055-75:
  Configuration manual Code number 1060028232, Edition 2005-02 [13]
- Océ VarioPrint 2062:
  Configuration manual Code number 1060028188, Edition 2005-02 [14]
- Océ Varioprint 2075:
  Configuration manual Code number 1060028167, Edition 2005-02 [15]

These manuals are delivered in paper form with the DAC and can also be downloaded from the support section of the Océ corporate website (www.oce.com).

3 Security Policy

The TOE, the software part of a Digital Access Controller (DAC) is part of a multifunctional device (MFD) for copying, printing and scanning. MFDs consist of two main parts: a controller and a Digital Copier (DC). The DAC is connected between a network and the DC.

The security policy of the TOE is to provide:

- protection against unauthorised access to data which is stored temporarily in the DAC
- protection against malware in the TOE's operational environment which might launch an attack on the integrity of the TOE.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

4.1.1 Remote system administrator

It is assumed that the DAC is used in the security mode 'high (factory default)'. The security mode will not be changed.

The remote system administrator will read the available system administrator documentation ([9] and [16]) and must be aware of the security policy of the organisation. The remote system administrator has to work in a security aware manner with the DAC.

4.1.2 Local and remote users

When secure print jobs are sent to the DAC, the user will specify a PIN of at least four digits and a maximum of six digits and, whether the job is printed or not, will delete the job on the same working day. Employees are aware of this requirement.

The user will read the available user documentation and must be aware of the security policy of the organisation. The user has to work in a security aware manner with the DAC.

4.1.3 E-shredding

It is assumed that the E-shredding operation for print jobs and scan job data objects will not be disabled.

4.1.4 Authentication

4.1.4.1 Remote system administrator

The Océ System Configuration application is password protected.

For the purpose of configuring the DAC prior to deployment, the DAC is delivered with a factory-default password. The remote system administrator will change the password before the DAC is deployed.

The remote system administrator will not use a short or easy-to-guess password. It is assumed that a non-predictable sequence of at least five characters will be used. Additionally to these minimum requirements, the remote system administrator is advised to:

- use a long password - up to 50 characters can be used.
- use a mixture of upper and lower case letters, numbers and punctuation.
- change the password every month.

Log-on to Océ system configuration is blocked for a while after an incorrect password is entered. The blocking interval is increased after successive incorrect entries.

4.1.4.2 Service engineer

The service engineer is a local administrator, and is typically employed by Océ. He has access through an USB interface to a wide range of settings on the TOE and the DC. The service engineer has elevated privileges above those of the user and the system administrator.

The TOE connection is protected with a default password. The service engineer must authenticate himself to the TOE before he is allowed to modify the TOE security settings. At the first log on the service engineer must change the SDS password to a different value than the default value to keep the DAC Common Criteria Centified. The password must comply with the following rules:

- The passwords must have alpha-numeric characters, a combination of numbers and letters.
- The password must have uppercase letters, lowercase letters, and numbers.
- The length of the password must be between 6 and 50 characters.

4.2 Environmental assumptions

4.2.1 Security policy

It is assumed that the customer organisation will have a security policy governing the use of IT products by employees in the organisation.

The security policy describes and requires a low to medium level of assurance (Common Criteria Evaluation Assurance Level 2) for the DAC.

It is assumed that the network, which the DAC is attached to, is protected by security measures that are intended to prevent malicious programs, viruses and network traffic, not related to the working of the operational environment, entering the network to which it is attached. Although the virus database files and various patches are kept up to date, the policy recognises that new threats emerge over time and that occasionally they may enter the environment from outside and provides measures to help limit the damage. The policy will define how IT products are protected against threats originating from outside the organisation.

The employees of the organisation are aware of, are trained in and operate according to the terms and conditions of the policy. The policy also covers physical security and the need for employees to work in a security aware manner including the usage of the DAC.

4.2.2 Environment

It is assumed that the operational environment of the DAC is a regular office environment. Physical access to the operational environment is restricted. The environment contains non-threatening office personnel (local users, remote users, remote system administrator, Océ service engineer). A “thief” (cleaning staff, burglar, visitor, in rare cases a user who will have no moral issues in stealing the TOE or parts of it and attempts to retrieve earlier printer and scanner jobs from the TOE) is only rarely present in this environment and not on a recurring base.

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).

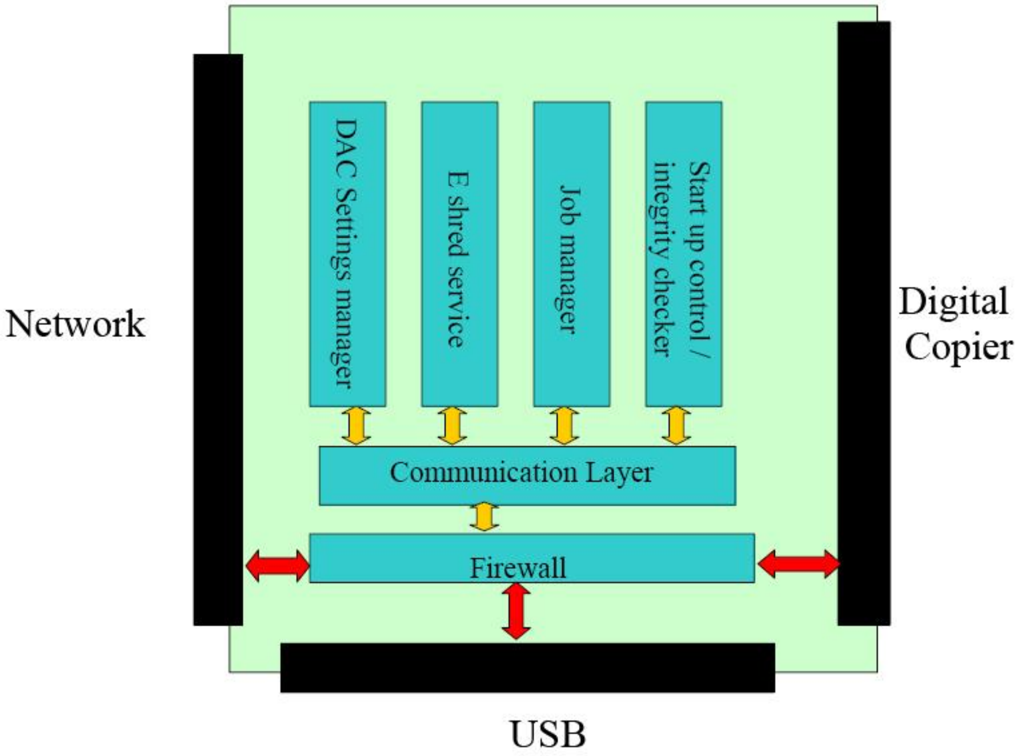

Figure 2: Overview of the TOE subsystems and external interfaces

The subsystems are the following:

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 state-full 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:

1. Standard Print Job (D.PRINT_JOB in ST)
2. User associated Print Job (D.PRINT_JOB in ST)
3. User associated print job with unique PIN(D.SECURE_PRINT_JOB in ST)
4. 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 inconstancies.

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 documentation [9] – [16] is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

The documentation is intended for administrators and users:

- For the system administrator the system administrator guidance [9] and the DAC administration guidance [16] are provided.
- For the user of the MFD, the job manuals [10] – [12] and the configuration manuals [13] – [15] are provided.

For more information see chapter 2.2 of this report.

7 IT Product Testing

7.1 Independent Testing

7.1.1 Testing approach

The tests are built upon the security functions as defined in the Security Target [7]. All security functions have associated tests. The security functions are SF.FILTERING, SF.JOB_RELEASE, SF.MANAGEMENT, SF.SHREDDING and SF.SELFTEST.

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

1. Check of filtering if it performs conform to the functional specification. With all network functionality enabled in security level high, the firewall should be properly configured. Check of the external Ethernet connector if the firewall only allows certain defined ports.
2. Check of security printing if it performs conform to the functional specification.
3. Check of shredding if it performs conform to the functional specification.

4. Check of Web SAS authentication and SDS authentication if they perform conform to the functional specification.
5. Check of integrity test function if it performs conform to the functional specification.

7.1.2 Test configuration

Tests are performed with the DAC connected to an Océ VarioPrint 2075. The security mode is ‘High’ (factory default).

The following software components are used:

1. The Montvista Linux operating system version 4.0
2. Apache HTTP server with SSL support, Apache 2.0.55, OpenSSL 0.9.7e (used for remote system administration) and OpenSSL 0.9.7d (used for job forwarding), mod_ssl 2.8.22.
3. Adobe PS3-PDF Interpreter, Version 3016.103 v.3.1 build #03
4. DAC version R9.1.6

7.1.3 Coverage

All testing is commensurate with the functional specification and covers all security functions.

The developer has performed all necessary functional tests for the security functions. In addition the developer has performed extensive vulnerability tests that exceeds the attack potential required by EAL2.

7.1.4 Results

The results of the developer testing showed that the security functions perform as expected.

This means that the developer has shown that

1. The TOE protects it’s own integrity against threats from the network to which it is attached and the Digital Copier to which it is attached through use of a firewall and integrity checks on system files upon system reboot.
2. The TOE protects the confidentiality of secure print jobs once they have been received by the DAC by storing them until the user authenticates himself to the DAC via a user interface on the DC. The DAC shreds the data after printing is completed.
3. The TOE does not form a threat to its environment.

7.2 Penetration Testing

Following the developer Vulnerability Analysis, the following penetration testing effort was made.

7.2.1 Testing Approach

The functional specification was the starting point for the identification of which interfaces and which functions need to be tested. Based on the more detailed knowledge of the high-level design some tests are included additionally.

A number of publicly available scanners for obvious vulnerabilities were applied.

7.2.2 Test Configuration

The tests are performed with the DAC connected to an Océ VarioPrint 2075. The security mode is ‘High’ (factory default)

The following software components are used:

1. The Montvista Linux operating system version 4.0
2. Apache HTTP server with SSL support, Apache 2.0.55, OpenSSL 0.9.7e (used for remote system administration) and OpenSSL 0.9.7d (used for job forwarding), mod_ssl 2.8.22.
3. Adobe PS3-PDF Interpreter, Version 3016.103 v.3.1 build #03
4. DAC version R9.1.6
5. The test laptop ran Suse 9.3, Nessus 3.0.1 and the Auditor Security Collection (auditor-200605-02) live CD

7.2.3 Coverage

The penetration testing was commensurate to the functional specification and covered the search for obvious vulnerabilities.

7.2.4 Penetration testing summary

The evaluators had a meeting in which the (possible) vulnerabilities are identified. Each evaluator contributed his perspective on the TOE and the evaluation based on the assurance classes he had executed. The outcome of this meeting is input for the vulnerability analysis.

The following tools are used to perform the tests:

• Openssl (auditor-200605-02)	Open source ssl implementation
• Nessus 3.0.1	Open Source vulnerability scanner
• Amap (auditor-200605-02)	Open source port scanner.
• Xprobe2 (auditor-200605-02)	Open source OS fingerprint, sends ICMP
• Ethereal (auditor-200605-02)	Open Source network sniffer.

7.2.5 Results

The TOE behaved as expected:

1. The security functionality works as expected.
2. The vulnerability test showed that the TOE is resistant against all tested public known vulnerabilities based on recent internet scans.
3. The vulnerability scans did not reveal vulnerabilities that could be exploited on the level of EAL2.

8 Evaluated Configuration

The TOE is identified by the release Océ Digital Access Controller (DAC) R9.1.6.

For setting up and running the TOE according to the evaluated configuration all guidance documents (refer to chapter 6) and the implications given by the Security Target have to be followed. These implications can also be found in chapter 1.5, 1.6 and 4 of this report.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL2+.

The verdicts for the CC, Part 3 assurance components (according to EAL2 augmented by ALC_FLR.1 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Configuration Items	ACM_CAP.2	PASS

Assurance classes and components		**Verdict**
Delivery and operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	CC Class ATE	PASS
Evidence of coverage Functional testing	ATE_COV.1 ATE_FUN.1	PASS PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 6: Verdicts for the assurance components

The focus of this re-evaluation was laid on the examination of the introduction of the following changes

- new Operating System: Montavista Linux 4.0 Professional Version
- only the Ethernet and USB connectors are available (CD-ROM drive removed)
- a fingerprint sensor which is only used during the identification of the user when printing secure print jobs has been added in the environment

as well as on the search for new obvious vulnerabilities and on the correctness of overall functionality of the TOE after the addition of some new not security-relevant features.

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL2 augmented by ALC_FLR.1
- the SFRs FIA_UID.1, FIA_UAU.1, FIA_UID.2 and FIA_UAU.2 require the TOE to provide security functions that provide identification/authentication

functionality that meets a SOF claim of ‘SOF basic’.
A strength of function claim of ‘SOF basic’ is made for the security functions SF.JOB_RELEASE and SF.MANAGEMENT. These are the security functions that implement FIA_UID.1, FIA_UAU.1, FIA_UID.2 and FIA_UAU.2.

The results of the evaluation are only applicable to the Océ Digital Access Controller (DAC) R9.1.6

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

10 Comments/Recommendations

The DAC is intended to provide scan and print functionality to users requiring a low to moderate level of security assurance (Common Criteria Evaluation Assurance Level 2+).

The remote system administrator must not change the security mode. If the security mode is changed, the DAC is no longer in the certified configuration and is no longer able to assure the security of its objects and itself. 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'.

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'.

The employees of the organisation are aware of, are trained in and operate according to the terms and conditions of the policy (see chapter 4.2.1 of this report). The policy also covers physical security and the need for employees to work in a security aware manner including the usage of the DAC. The employees will read the available guidance documentation.

The guidance documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
DAC	Digital Access Controler
DC	Digital Copier
EAL	Evaluation Assurance Level
MFD	Multifunctional Device
IT	Information Technology
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

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

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

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

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

[6] Applicaton Notes and Interpretations of the Scheme AIS33, Version 2 – "Methodologie zur Fehlerbehebung – Flaw Remediation", 26.07.2002

[7] Security Target BSI-DSZ-0370-2006, Version 2.4, August 25th, 2006, The Océ Digital Access Controller (DAC) R9.1.6, as used in the Océ VarioPrint 1055, 1065, 1075, 2062, 2075 printer/copier/scanner products, Océ Technologies B.V.

[8] Evaluation Technical Report, Version 3.0, October 11th, 2006, The Océ Digital Access Controller (DAC) R9.1.6 as used in the Océ VarioPrint 1055, 1065, 1075, 2062,2075 printer/copier/scanner products – EAL2+ (confidential document)

Guidance Documentation

[9] Océ VarioPrint 1055, 1065,1075, 2062, 2075, Common Criteria Certified configuration of the DAC R9.1.6. Edition 2006-05

[10] Océ VarioPrint 1055-75: Job manual Code number 1060028223, Edition 2005-02

[11] Océ VarioPrint 2062: Job manual Code number 1060028188, Edition 2005-02

[12] Océ VarioPrint 2075: Job manual Code number 1060028155, Edition 2005-02

[13] Océ VarioPrint 1055-75: Configuration manual Code number 1060028232, Edition 2005-02

[14] Océ VarioPrint 2062: Configuration manual Code number 1060028188, Edition 2005-02

[15] Océ Varioprint 2075: Configuration manual Code number 1060028167, Edition 2005-02

[16] Océ-Technologies B.V., Océ System Configuration, Version 4.1 On-line help, Revision 4.1, September 2005

[17] Secure Deletion of Data from Magnetic and Solid State Memory, Peter Guttman 1996 (http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)

[18] US Department of Defence Military Standard DOD 5220-22m (http://www.dss.mil/isecnispom_0195.htm)

[19] DAC administration guidance for Océ service engineer “Administrating version R9.1.6 of the Océ DAC” (Lotus Notes Application)

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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