Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0326-2006

for

Océ Smart Imager 8.3.3.39
as used in the Océ VP 2090 3.3

from

Océ Technologies B.V.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0326-2006

Scanner-Printer-Copier Controller

Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 3.3

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, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

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, March 21st, 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

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 22 September 2000 in the Bundesanzeiger p. 19445

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 Smart Imager 8.3.3.39 has undergone the certification procedure at BSI.

The evaluation of the product Océ Smart Imager 8.3.3.39 was conducted by TNO-ITSEF BV. The TNO-ITSEF BV 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 March 21st, 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 Smart Imager 8.3.3.39 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

The firm Océ produces a wide range of multifunctional devices (MFDs) for copying, printing and scanning for various purposes. One of these MFDs: the VP 2090, uses PC hardware based controller, which is called the Smart Imager (SI).

The TOE is the Océ Smart Imager 8.3.3.39 as used with the Océ VP 2090 R3.3.

The Smart Imager is a PC-based MFD-controller. The SI provides a wide range of printing, scanning and copying functionality to the MFD peripherals to which it is connected. The SI also provides security functionality to the MFD.

The Smart Imager can operate in two different security modes: 'High' and 'Normal'. The Security Target [7] covers the Smart Imager 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 invalidates the claim made in the Security Target [7].

The Smart Imager is located internally in the MFD. The internal configuration helps prevent theft of the Smart Imager, but prevention of theft of the SI is outside the scope of this evaluation. All logical access points (CD-ROM, floppy drives, network ports, USB/serial/parallel ports etc.) are protected from physical access in the internal configuration by a metal casing.

The Smart Imager consists of two parts, the underlying hardware platform which is not part of the TOE and the software which forms the TOE (for further details of TOE boundary see chapter 2.1 of this report and chapter 2.1.1 of the ST [7]).

The IT product Océ Smart Imager 8.3.3.39 was evaluated by TNO-ITSEF BV. The evaluation was completed on March 08th, 2006. The TNO-ITSEF BV 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

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 by ALC_FLR.1 (Basic Flaw Remediation).

[8] Information Technology Security Evaluation Facility

1.2 Functionality

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

The following 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_SEP.1	TSF domain separation
FPT_RVM.1	Non-bypassability of the TSP

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 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.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 Smart Imager interface. If verification is successful, the secure print job is released for printing.
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 2: TOE Security Functions

For more details please refer to the Security Target [7], chapter 6.1.

1.3 Strength of Function

The Strength of Function claim for all the probabilistic functions and mechanisms provided by the TOE is SOF-basic as indicated in the Security Target [7], chapter 5.1.6.

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 (see also ST [7], chapter 3.3 and 3.4):

Threat	Description
T.RESIDUAL_DATA	S.THIEF steals the TOE or parts thereof and retrieves stored or deleted D.SECURE_PRINT_JOB, D.PRINT_JOB, D.SCAN_JOB and D.COPY_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 Smart Imager. 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. 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.PRINT_JOB, D.SCAN_JOB and D.COPY_JOB 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 Smart Imager 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 Smart Imager 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 Smart Imager back into the certified configuration (‘high (factory default)’) by changing the security mode back to 'high'.

1.5.2 E-Shredding

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

The following E-shredding settings can be configured:

- Method (U.S. DoD 5220.22-M (Default), Gutmann, Custom) [13]
- Number of overwrite passes (Default:'3 (U.S. DoD 5220.22-M)') [14].

The remote System administrator must not change the 'Sensitive Jobs' settings. If E-shredding is disabled for 'copy jobs', 'scan jobs‘, 'print jobs' or 'print jobs with PIN', the SI is no longer in the certified configuration and is no longer able to assure the security of copy jobs, scan jobs and print jobs.

1.6 Assumptions about the operating environment

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

Assumptions	Description
A.DIGITAL_PRINTER	Attachment of the TOE to a MFD
A.DIGITAL_SCANNER	Attached Digital Scanner
A.LUI	Attached Local User Interface
A.ENVIRONMENT	Regular office environment
A.SECURITY_POLICY	Existing security policy governing the use of IT products in the customer organisation
A.SLA	Any security flaws discovered in the TOE will be repaired by Océ

Table 5: Assumptions

Note: Only the titles of the assumptions are provided. For more details please refer to chapter 4 of this report or 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 Smart Imager 8.3.3.39

The TOE is a series of software that runs on a generic off-the-shelf PC (underlying platform). Together this is called the Smart Imager. The Smart Imager is a PC-based MFD-controller (Multi Functional Device) that provides a wide range of printing, scanning and copying functionality to the MFD.

2.1 Physical scope of the TOE

The TOE consists of the software parts of the Smart Imager, i.e. the operating system (Microsoft Windows 2000), the Smart Imager-specific software (Océ Smart Imager 8.3.3.39) and the third-party software (Adobe PS3-PDF Interpreter, Version 3016.103 build #03; PCL5 interpreter, Version ME6.0.1/4; Microsoft IIS web server with SSL support, Version 5.0). The underlying PC infrastructure is not part of the TOE (see also figure 1 below).

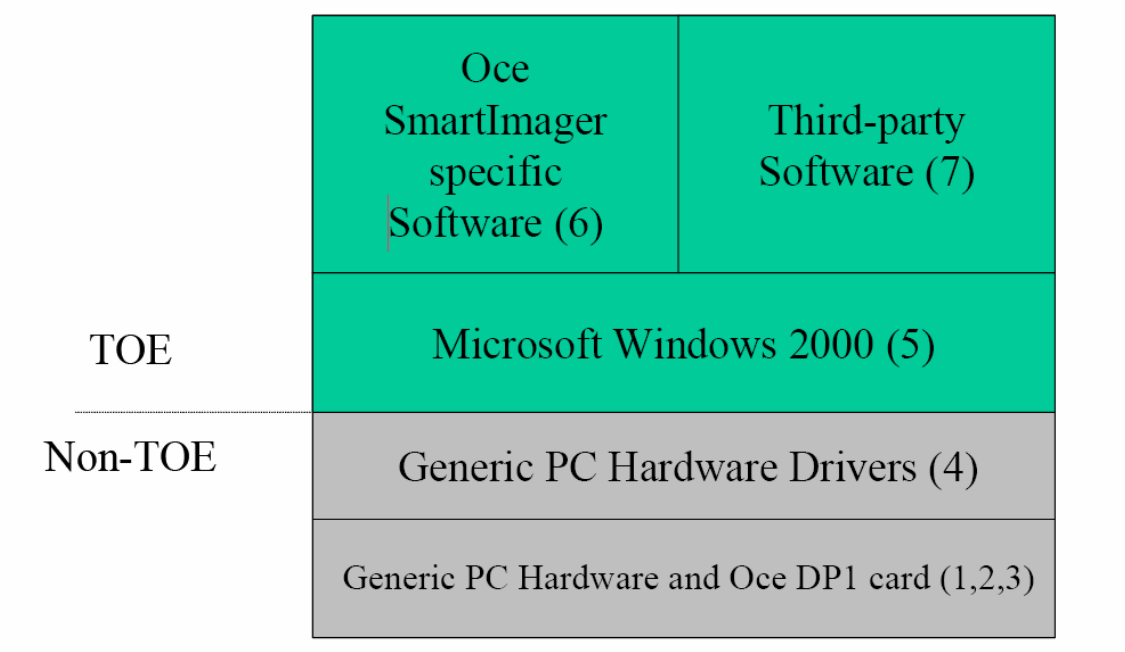

Figure 1: Physical scope of the TOE

2.2 TOE deliverables

The following TOE deliverables are provided for a customer who purchases the Océ Smart Imager 8.3.3.39:

Underlying platform:

1. A generic off-the-shelf PC comprising at a minimum a 1.5GHz Celeron processor, 512MB internal RAM, a DVI output (graphical I/O), two 40GB

hard drives, two USB ports, one serial port, internal floppy and CD-ROM drive.

2. Generic graphics card and network card supporting 10/100/1000Mbs Ethernet UTP.
3. An Océ DP1 card for communication between the Smart Imager and it's attached peripherals.
4. Drivers for the PC, graphics card and network card

Océ Smart Imager 8.3.3.39

1. The Microsoft Windows 2000 operating system with service pack 4 (operating system version 5.00.2195) plus the following patches:
   Q823559 (MS03-023), Q828749 (MS03-049), Q835732 (MS04-011), Q828741 (MS04-012), Q837001 (MS04-014), Q893066 (MS04-010) v2
2. Océ Smart Imager-specific software release 8.3.3.39.
3. Third-party developed software: Adobe PS3-PDF Interpreter, Version 3016.103 build #03; PCL5 interpreter, Version ME6.0.1/4; Microsoft IIS web server with SSL support, Version 5.0.

Accompanying manuals – administrator guidance:

1. Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39 [9]
2. The Smart Imager administration guidance for the customer system administrator takes the form of HTML pages. These are part of the Océ Smart Imager-specific software, release 8.3.3.39 [10]
3. The Smart Imager administration guidance for the Océ service engineer takes the form of an application called the Technical Service Manual (TSM) that is installed on the service engineer's laptop. The guidance contains an appendix that is identified as VP 2090 Smart Imager Security Service documents in the TSM: System Software – Installation and is a frozen version of the Océ service engineer application made at the time of product release [12].

Accompanying manuals – user guidance:

1. Océ VP2090 User manual [11]
2. Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39 [9]

For the delivery the Smart Imager software is installed on the Smart Imager PC (underlying platform), then the Varioprint 2090 and the SI are packed to one package and are labeled. When they arrive at the customer the package is checked by the Océ service engineer and then installed according the installation guidance.

3 Security Policy

The Smart Imager provides a wide range of printing, scanning and copying functionality to the MFD peripherals to which it is connected. The Smart Imager 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 Smart Imager does this by e-shredding the data after they are deleted.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

4.1.1 Remote system administrator

It is assumed that the SI is used in the security level 'High (factory default)'. The security level will not be changed.

The remote System administrator will read the available System administrator documentation 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 SI.

4.1.2 Local and remote users

When secure print jobs are sent to the SI, the user will specify a PIN of at least 4 digits and a maximum of 5 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 SI.

4.1.3 E-shredding

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

4.1.4 Authentication

4.1.4.1 Remote system administrator

The Océ VarioPrint 2090 Settings Editor application is password protected.

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

The remote System administrator must not use a short or easy-to-guess password. Use a non-predictable sequence of at least 8 characters (ASCII[32-127]). Additionally, 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.

4.1.4.2 Service engineer

These are local administrators, and are typically employed by Océ. They have access through an USB connection to a wide range of settings on the TOE. The TOE connection is PIN code protected and service license protected and access to the management functions provided to the service engineer require specific hardware and software. It is not possible to access the management functions made available to the service engineer without the software that is installed on the service engineer laptop.

4.2 Environmental assumptions

4.2.1 Security Policy

It is assumed that the customer will have a Security Policy governing the use of IT products by employees in the customer organisation. The TOE assumes that the network to which it is attached is protected by security measures that are intended to prevent mal-ware, 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 customer organisation. The organisation’s employees 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 TOE. The Security Policy describes and requires a low to medium level of assurance (EAL2) for the TOE.

4.2.2 Environment

The TOE assumes that its operational environment is a regular office environment. Physical access to the operational environment is restricted. The environment contains non-threatening office personnel (S.LOCAL_USER, S.REMOTE_USER, S.REMOTE_SYSADMIN and S.SERVICE_ENGINEER). S.THIEF is only rarely present in this environment and not on a recurring basis.

4.2.3 Attached devices

It is assumed that the TOE has a S.DIGITAL_PRINTER device attached to it. S.DIGITAL_PRINTER is part of the Océ VarioPrint 2090 MFD. For all print jobs that are sent to the mailbox, whether the job is printed or not, the job will be deleted on the same workday. Employees are aware of this requirement. It is assumed that for EAL2, the interface from the Smart Imager to the S.DIGITAL_PRINTER will not be used to mount an attack and that the interface is only used for the purposes of printing.

It is assumed that the TOE has a S.DIGITAL_SCANNER device attached to it. S.DIGITAL_SCANNER is part of the Océ VarioPrint 2090 MFD. It is assumed for EAL2, that the interface from the Smart Imager to the S.DIGITAL_SCANNER will not be used to mount an attack and that the interface is only used for the purposes of scanning.

It is assumed that the TOE has a S.LUI device attached to it. S.LUI is part of the Océ VarioPrint 2090 MFD. It is assumed for EAL2, that the interface from the LUI to the Smart Imager will not be used to mount an attack and that the interface is only used for the purposes of printing, scanning and copying.

4.2.4 Flaw Remediation

It is assumed that any security flaws discovered in the TOE will be repaired by Océ (possibly as part of an agreed service level agreement).

5 Architectural Information

The following diagram indicates the subsystems of the TOE that implement the security functionality.

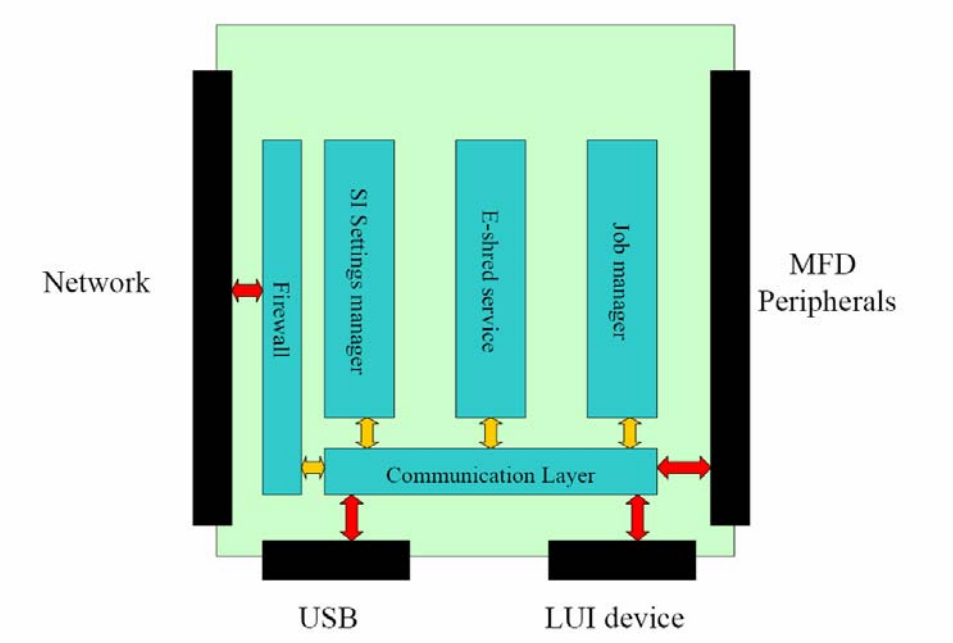

Figure 2: Overview of the TOE subsystems

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 2000 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.

Job Manager: The job manager server manages the print and scan jobs that are handled by the Smart Imager.

Smart Imager Settings manager: The Smart Imager Settings manager subsystem manages a number of settings that are related to its operation. This subsystem manages security related settings of the Smart Imager. 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 that are handled by the Job Manager subsystem (Standard Print Job, User associated Print Job, User associated print job with unique PIN, Scan job and Copy job).

6 Documentation

The documentation [9] – [11] 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:

The user guidance for the TOE consists of:

- Océ VP2090 User manual [11]
- Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39 [9].

The administrator guidance for the TOE consists of:

- Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39 [9]
- The Smart Imager administration guidance for the customer system administrator takes the form of HTML pages. These are part of the Océ Smart Imager-specific software, release 8.3.3.39 [10].

Additionally the developer has a specific guidance for the Océ service engineer, which is not provided to the customer. The Smart Imager administration guidance for the Océ service engineer takes the form of an application called the Technical Service Manual (TSM) that is installed on the service engineer's laptop. The guidance contains an appendix that is identified as:

- VP 2090 Smart Imager Security Service documents in the TSM: System Software – Installation [12]

and is a frozen version of the Océ service engineer application made at the time of product release.

7 IT Product Testing

7.1 Developer Testing

7.1.1 TOE Test Configuration

- A VP2090 R3.3 has been used for tests.
- A service laptop running under Windows XP plus relevant cable with USB to Ethernet adapter
- A PC running under windows XP has been used to scan the SI's hard disk.

7.1.2 Testing Approach

Tests are executed according to the tests specifications mentioned in Test Specification.

The tests are built upon the security functions as defined in the ST. All security functions have associated tests. The security functions are:

- SF.FILTERING
- SF.JOB_RELEASE
- SF.SHREDDING
- SF.MANAGEMENT

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

- Check that filtering performs conform to the Functional Specification. With all network functionality enabled in security level High, the firewall should be properly configured. Check that on the external Ethernet connector the firewall only allows certain defined ports.
- Check that security printing performs conform to the Functional Specification.
- Check that shredding performs conform to the Functional Specification.
- Check that System Administrator authentication and Service Engineer authentication perform conform to the Functional Specification.

7.1.3 Coverage

All testing 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 test 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:

- The TOE protects it's own integrity against threats from the network to which it is attached through use of a firewall.
- The TOE protects the confidentiality of secure print jobs once they have been received by the SI by storing them until the user authenticates himself to the SI via a user interface on the MFD. The SI shreds the data after it is deleted.
- The TOE does not form a threat to its environment.

7.2 Independant Testing

7.2.1 Test configuration

Tests are performed with the SI connected to the Océ digital copiers Océ VarioPrint 2090 R3.3.

The security mode is 'High' (factory default).

The following software components are used:

- The Microsoft Windows 2000 operating system with service pack 4 (operating system version 5.00.2195) plus patches (see chapter 2.2)
- Océ Smart Imager-specific software release 8.3.3.39
- Adobe PS3-PDF Interpreter, Version 3016.103 build #03
- PCL5 interpreter, Version ME6.0.1/4
- Microsoft IIS web server with SSL support, Version 5.0

7.2.2 Testing Approach

The tests are built upon the security functions as defined in the ST. The evaluators ran all of the developer tests specified in the Developer Test Specification as well and independent evaluator tests.

In total the following security functions have been tested:

- SF.FILTERING,
- SF.JOB_RELEASE,
- SF.SHREDDING,
- SF.MANAGEMENT.

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

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

- Check that security printing performs conform to the Functional Specification.
- Check that shredding performs conform to the Functional Specification.
- Check that System Administrator authentication and Service Engineer authentication perform conform to the Functional Specification.

7.2.3 Coverage

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

The evaluator has performed all necessary functional tests for the security functions.

7.2.4 Results

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

This means that the evaluator has shown that:

- The TOE protects it's own integrity against threats from the network to which it is attached through use of a firewall.
- The TOE protects the confidentiality of print, copy and scan job data after they are no longer needed. The SI shreds the data after they are deleted.

7.3 Penetration Testing

7.3.1 Test Configuration

Tests are performed with the SI connected to the Océ VarioPrint 2090 R3.3.

The security mode is 'High' (factory default).

The following software components are used:

- The Microsoft Windows 2000 operating system with service pack 4 (operating system version 5.00.2195) plus patches (see chapter 2.2)
- Océ Smart Imager-specific software release 8.3.3.39
- Adobe PS3-PDF Interpreter, Version 3016.103 build #03
- PCL5 interpreter, Version ME6.0.1/4
- Microsoft IIS web server with SSL support, Version 5.0

The test laptop ran Suse 9.3, Nessus 2.2.5 and the Auditor Security Collection (auditor-200605-02) live CD.

7.3.2 Testing Approach

The evaluators took the functional specification as 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.

The evaluators applied a number of publicly available scanners for obvious vulnerabilities.

7.3.3 Coverage

All testing commensurate with the functional specification and covers all security functions and included the search for obvious vulnerabilities.

The evaluators have 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 tests are performed:

- Openssl (auditor-200605-02) Open source ssl implementation
- Nessus 2.2.5 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

7.3.4 Results

The TOE behaved as expected:

- The security functionality works as expected.
- The vulnerability test 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

The TOE is identified by the release Océ Smart Imager 8.3.3.39

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. For the augmented component ALC_FLR.1 the AIS33, Version 2 – "Methodologie zur Fehlerbehebung – Flaw Remediation", 26.07.2002 [6] was used.

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
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

Assurance classes and components		Verdict
Tests	CC Class ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	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 evaluation has shown that:

- the 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_UID.2, FIA_UAU.1 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_UID.2, FIA_UAU.1 and FIA_UAU.2.

The results of the evaluation are only applicable to the Océ Smart Imager 8.3.3.39 (see also chapter 2 of this report).

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

10 Comments/Recommendations

The guidance documentation [9] - [11] (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
EAL	Evaluation Assurance Level
IT	Information Technology
LUI	Local User Interface
MFD	Multifunctional Device
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SI	Smart Imager
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 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[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-CC-0326-2006, Version 2.1, 16.02.2006, Security Target, The Océ Smart Imager 8.3.3.39 as used in the Océ VP 2090 3.3, Océ Technologies BV

[8] Evaluation Technical Report, The Océ Smart Imager V8.3.3.39 as used in the Océ VP 2090 3.3, Version 2.0, 07.03.2006, (confidential document)

Guidance Documentation

[9] Océ VP2090 Common Criteria certified configuration of the SI v8.3.3.39, Edition 10-2005

[10] Online Help for Océ VarioPrint® 2090 Settings Editor, Version 10-2005

[11] Océ VarioPrint® 2090 User Manual, Edition 02-2004

[12] VP 2090 Smart Imager Security Service documents in the TSM: System Software – Installation, 07.12.2005

Technical Papers

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

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

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 2.1."

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class 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 map

Evaluation assurance levels (chapter 6)

"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 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 6.1)

Table 6.1 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 2 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 CC 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 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

"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 6.2.2)

"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 6.2.3)

"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 6.2.4)

"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 6.2.5)

"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 6.2.6)

"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 6.2.7)

"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 14.3)

AVA_SOF Strength of TOE security functions

"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 14.4)

AVA_VLA Vulnerability analysis

"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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“