Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0387-2007

for

Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594

from

Microsoft Corporation

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

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0387-2007

Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594

from

Microsoft Corporation

Common Criteria Arrangement
for components up to EAL4

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) extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 / augmented by** AVA_VLA.3 – Vulnerability Assessment - Moderately resistant ALC_FLR.1 – Flaw Remediation – 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, 21. March 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

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

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

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

2.2 International Recognition of CC - Certificates

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

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

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

This evaluation contains the component AVA_VLA.3 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition, AVA_VLA.2 replaces AVA_VLA.3.

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 Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0262-2005.

The evaluation of the product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 was conducted by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, and vendor and distributor is:

Microsoft Corporation

1 Microsoft Way

Redmond, WA 98052, USA

The certification is concluded with

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

This work was completed by the BSI on 21. March 2007.

The confirmed assurance package is only valid on the condition that

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

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

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

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22.

The product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 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] Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052, USA

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 Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the Firewall product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 (also named ISA Server in short).

ISA Server is a dedicated firewall that acts as the secure gateway to the Internet for internal computers. ISA Server protects all communication between internal computers and the Internet and runs on a Windows 2003 Server operating system.

The basic functions of the ISA Server are:

- Web Identification and Authentication: The TOE can be configured that only particular users are allowed to access the networks through the TOE using Basic authentication or OWA (Outlook Web Access) forms based authentication.

- Information flow control: The TOE combines several security mechanisms to enforce the security policies at different network layers.

- Audit: The TOE generates logging information that is stored in different log files in the environment.

ISA Server is intended to be used as a multi-layered firewall. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application level filtering allows ISA Server to inspect and secure popular protocols.

Graphical taskpads and wizards do not belong to the TOE but are implemented in the environment , they shall simplify navigation and configuration for common tasks.

The operation system Windows 2003 Server maintains security attributes for all administrators. Windows 2003 Server stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorised administrator role. The TOE itself offers no additional identification and authentication methods for firewall administrators.

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 extended.

The IT product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The evaluation was

completed on 02. February 2007. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and vendor and distributor is

Microsoft Corporation

1 Microsoft Way

Redmond, WA 98052, USA

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 part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented).

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: AVA_VLA.3	Vulnerability Assessment - Moderately resistant
+: ALC_FLR.1	Flaw Remediation – Basic flaw remediation

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE provides following functionality:

SFR	Name
Audit Generation	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.3	Action in case of possible audit data loss
Identification and Authentication	
EXT_FIA_AFL.1	Authentication failure handling
EXT_FIA_UID.2	User identification before any action
EXT_FIA_UAU.2	User authentication before any action
Information Flow Control	

[8] Information Technology Security Evaluation Facility

SFR	Name
FDP_IFC.1 (1)	Subset information flow control (1) - UNAUTHENTICATED SFP
FDP_IFC.1 (2)	Subset information flow control (2) - UNAUTHENTICATED_APPL SFP
FDP_IFC.1 (3)	Subset information flow control (3) - AUTHENTICATED SFP
FDP_IFF.1 (1)	Simple security attributes (1) - UNAUTHENTICATED SFP
FDP_IFF.1 (2)	Simple security attributes (2) - UNAUTHENTICATED_APPL SFP
FDP_IFF.1 (3)	Simple security attributes (3) - AUTHENTICATED SFP
FDP_RIP.1	Subset residual information protection
FMT_MSA.3	Static attribute initialization
FPT_RVM.1	Non-bypassability of the TSP

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

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

Security function
SF1: Web Identification and Authentication
SF2: Information Flow Control
SF3: Audit

Table 3: Security Functions

Note: Only the titles of the Security Functional Requirements and of the TOE Security Functions are provided. For more details please refer to the Security Target [6], chapter 5 and 6.

1.3 Strength of Function

There is no strength of functions claim for the TOE.

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

The following list of considered threats for the TOE is defined in the Security Target [6], chapter 3.3:

T.NOAUTH

An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.MEDIAT

An attacker may send impermissible information through the TOE, which results in the exploitation of resources on the internal network and gathering of information he is not authorised for.

T.OLDINF

Because of a flaw in the TOE functioning, an attacker may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

T.AUDFUL

An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

There is one Security policy to be fulfilled by the TOE, please refer to the Security Target [6], chapter 3.2:

P.AUDACC

Persons must be accountable for the actions that they conduct. Therefore audit records must contain sufficient information to prevent an attacker to escape detection.

1.5 Special configuration requirements

There are two versions of ISA Server available: Standard Edition (single machine support only) and Enterprise Edition (can be member of a firewall cluster). The chosen TOE is the Enterprise Edition with local administration.

The Enterprise Edition is designed for large-scale deployments with high-volume Internet traffic environments. It supports multi-server arrays with centralized management as well as enterprise-level and array-level security policy.

Both versions - Standard and Enterprise - can be treated the same way in the scope of this certification because the storage of policy configuration data was not part of the evaluation (Windows Registry and ADAM with the ADAM configuration receiver service are outside the scope of the TOE) and also scalability was not part of the evaluation. The Enterprise Edition has been tested while running on one machine (for details see chapter 7 of this report.)

For the Enterprise Edition security policy configuration data is stored in ADAM (a Lightweight Directory Access Protocol / LDAP directory service). The configuration data is then replicated by a system service into the local Windows registry and file system.

Network Load Balancing is also a feature that is supported by the Enterprise Edition but is disabled by default, the evaluated TOE does not use this interface. No tests according this interface have been performed, therefore it is not included in the evaluation.

The Enterprise Edition with local administration (which means that ADAM is located on the same machine as the TOE) identifies the TOE (see the Security Target [6], chapter 2.1.1).

The evaluated TOE is uniquely named as "Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594". Its evaluated software version is detailed in table 4.

The ISA Server software including Service Pack 2 and the Administrator and User Guidance as parts of the evaluated version for the TOE are provided as a boxed product that is delivered to the sales channels. The additional Guidance Documentation Addendum [9] of the guidance documentation [8] is delivered via the web only.

The Administrator and User Guidance is also available on the internet, however, relevant for the evaluated version of the TOE is the Administrator and User Guidance that is delivered together with the software on CD-ROM [8]. The additional Guidance Documentation Addendum [9] is also part of the evaluated version of the TOE. It is only available as a pdf document via a secure channel on the vendors TOE-internet-homepage.

The TOE is running on a Windows 2003 Server Standard Edition operating system (build 3790, English, SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch KB907865) and was tested using a HP Proliant DL380 G3 hardware platform. For more details please read the Security Target [6], chapter 2.1.2.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [6], chapter 3.1:

A.DIRECT

> The TOE is available to authorised administrators only. Personnel who has physical access to the TOE and can log in the operating system is assumed to act as an authorised TOE administrator.

A.GENPUR

> The TOE stores and executes security-relevant applications only. It stores only data required for its secure operation.

A.NOEVIL

Authorised administrators are non-hostile and follow all administrator guidance.

A.ENV

The environment implements the following functions which are used by the TOE security functions: local identification and authentication of user credentials used for web publishing, reliable time stamp, file protection, cryptographic support, administration access control, reliable ADAM implementation, Network Load Balancing.

A.PHYSEC

The TOE is physically secure. Only authorised personnel has physical access to the system which hosts the TOE.

A.SECINST

Required certificates and user identities are installed using a confidential path.

A.SINGEN

Information can not flow among the internal and external networks unless it passes through the TOE.

A.WEBI&A

User credentials are verified by a Radius Server. The Radius Server returns a value if a valid account exists or not.

A.SSL

All web publishing rules which support Basic authentication have to be configured by the administrator so that strong encryption for SSL is enforced (at least 128bit encryption).

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:

Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594

The following table summarises the TOE components and defines the evaluated configuration of the TOE:

Deliverables	Version	Comment
Product Box	4.0.3443.594	1. CD-ROM ISA Server 2004 - Enterprise Edition 2. CD-ROM ISA Server 2004 - Enterprise Edition Service Pack 2 3. [8] Guidance - included on CD-ROM
Guidance [8]	File properties - name: isa.chm, date: 18.01.2006, size: 1.185.726 bytes	Microsoft Internet Security and Acceleration Server 2004 manual – Enterprise Edition, available on CD-ROM (as part of the TOE package - ISA Server 2004 Enterprise Edition) (available on installed TOE under menu “Help -> Help topics -> Microsoft ISA Server” or directly via “isa.chm”)
Guidance Documentation Addendum (of the Administrator and User Guidance) [9]	1.5	Guidance Documentation Addendum [9] can be downloaded from the ISA Server Common Criteria web page (http://go.microsoft.com/fwlink/?linkid=49507).
File integrity verification package	See right hand column	The package can be used by customers to verify the TOE version. It is a zip file and consists of following files (name, size, date): • integritycheck.cmd, 2501bytes, 2006-08-16 • integritycheck-sp2.cmd, 1469bytes, 2006-09-06 • ISA2004EE-SP2.xml, 167bytes, 2006-09-06 • ISA2K4SELE_EN.xml, 93458bytes, 2006-08-16 • readme.htm, 4053bytes, 2006-09-06

		The package can directly be downloaded on https://members.microsoft.com/ISACommonCrit/Integrity_Check_ISA_2004_EE.zip (for description how to use see [9], chapter 5) The ISA Server Common Criteria web page (http://go.microsoft.com/fwlink/?linkid=49507) also includes a link to download the package.
FCIV tool	2.05	The FCIV tool is used to verify the integrity of the TOE with the provided integrity check file. It can be downloaded from: http://support.microsoft.com/default.aspx?scid=kb;enus;841290 (for further information see [9], chapter 5)

Table 4: Deliverables of the TOE

Note: Although administration and management tools (e. g. for reporting and alerting, cache, monitoring, logging, remote management) are delivered together with the TOE, they are excluded from the TOE and are considered part of the environment. Graphical taskpads and wizards that simplify navigation and configuration for common tasks do not belong to the TOE because they are supplied with the operating system Windows 2003 Server. The TOE is the ISA Server with Basic authentication or OWA forms based authentication.

The TOE environment also includes applications that are not delivered with the ISA Server, but are used functionality of the underlying operating system Windows 2003 Server (e. g. File System, System Event Log File, Registry, Network Interface, Cryptographic Support Interface, User Account Database, MSDE, MMC, WINAPI, Network Load Balancing).

3 Security Policy

The security policy of the TOE is to provide controlled and audited access to services, both from inside and outside an organisation's network, by allowing, denying, and/or redirecting the flow of data through the firewall.

The TOE allows or denies a set of computers or a group of users to access specific servers. If a rule is defined specifically to users, the TOE checks how the user should be authenticated. The evaluated TOE supports Basic authentication which is the standard method of authentication for Hypertext Transfer Protocol (HTTP) transmissions. Basic authentication sends and receives user information as text characters. The TOE also supports OWA forms based Authentication, which is a filter for form based authentication for Outlook Web Access.

The TOE controls the flow of incoming and outgoing IP packets and controls information flow on protocol level. Information flow control is subdivided into

firewall policy rules, web filters, application filters, system policy rules. It also comprises a lockdown mode when only a restricted set of system policy rules is active.

The TOE also features the generation of different logging information to be stored in the environment.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions, the following usage conditions exist. Please refer to the Security Target [6], chapter 3.1 for more detail:

- Personnel who has physical access to the TOE and can log in the operating system is assumed to act as an authorised TOE administrator. That means that the TOE is available to authorised administrators only (A.DIRECT).

- Authorised administrators are non-hostile and follow all administrator guidance (A.NOEVIL).

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.1):

- Only authorised personnel has physical access to the TOE because the TOE is physically secured (A.PHYSEC).

- The TOE stores and executes security-relevant applications only. It stores only data required for its secure operation (A.GENPUR).

- Information can not flow among the internal and external networks unless it passes through the TOE (A.SINGEN).

- Required certificates and user identities are installed using a confidential path (A.SECINST).

- The environment implements the following functions which are used by the TOE security functions: local identification and authentication of user credentials used for web publishing, reliable time stamp, file protection, cryptographic support, administration access control, reliable ADAM implementation, Network Load Balancing (A.ENV).

- User credentials are verified by a Radius Server that is placed on the internal network server. The Radius Server returns a value to indicate if a valid account exists or not (A.WEBI&A).

- All web publishing rules which support Basic authentication have to be configured by the administrator so that strong encryption for SSL is enforced (at least 128bit encryption) (A.SSL).

Furthermore, the Security Target [6], chapter 3.2 defines an Organisational Security Policy (P.AUDACC) that states that audit records must contain sufficient information to prevent an attacker to escape detection in order to make persons accountable for the actions they conduct.

4.3 Clarification of scope

Additional threats that are not addressed by the TOE and its evaluated security functions were not addressed by this product evaluation.

5 Architectural Information

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the Firewall product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594.

ISA Server 2004 is a firewall that helps to provide secure Internet connectivity. ISA Server protects all communication between internal computers and the Internet and runs on a Windows 2003 Server operating system. As a multi-layered firewall, the TOE provides security at different levels. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application-level filtering allows ISA Server 2004 to inspect and secure popular protocols. The TOE has the possibility to create filters that allow or deny traffic on the packet layer and with data-aware filters to determine if packets should be accepted, rejected, redirected, or modified. The identification and authentication capabilities can be configured separately for incoming and outgoing requests. The TOE also includes the generation of security and access logs. The log files can be configured and enabled for packet and application filters. They are human readable and can be reviewed with additional tools that belong to the TOE environment.

The operating system Windows 2003 Server maintains security attributes for all administrators. Windows 2003 Server stores the identification and authentication data for all known administrators and maintains a method of associating human users with the authorised administrator role. The TOE itself offers no additional identification and authentication methods for firewall administrators.

Figure 2.1 (TOE Demarcation) in the Security Target [6] shows the boundaries of the TOE, whereas the arrows indicate the interfaces between the TOE and the operating system Windows 2003 Server.

The three main security functionality of the TOE are:

- Web Identification and Authentication:

  The web publishing rules of the TOE can be configured to allow or deny a set of computers or a group of users to access specific servers. If the rule applies specifically to users, the TOE checks how the user should be authenticated. It is possible to configure incoming and outgoing Web request settings so that users must always be authenticated. It is possible to choose between different authentication methods and separately for incoming and outgoing requests.

- Information flow control:

  The TOE controls the flow of incoming and outgoing IP packets and controls information flow on protocol level. This control has to be active before any information can be transmitted through the TOE. Information flow control is subdivided into Firewall Policy Rules that consist of Access Rules, Network Rules, Server Publishing Rules, Mail Publishing Rules, Web Publishing Rules. Also, there are Web filters for HTTP and OWA and Application Filters, namely FTP access filter, RPC filter, and SMTP filter. Another part of the security function is the Lockdown mode of the TOE.

- Audit:

  The TOE allows the generation of different log files. Logging information can be stored in Firewall service log file, Web proxy service log files, and Windows application event log files, outside the TOE.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

[8] Microsoft Internet Security and Acceleration Server 2004 manual – Enterprise Edition, available on CD-ROM (part of ISA Server 2004 EE package), File properties - name: isa.chm, date: 2006-01-18, size: 1.185.726 bytes

[9] ISA Server 2004 Enterprise Edition Common Criteria Evaluation, Guidance Documentation Addendum – Enterprise Edition; Version 1.5; Date: 2007-02-09

7 IT Product Testing

Developer Tests

Test Configuration

The TOE has been tested within a configuration that consists of three networks. The TOE as the centre of the configuration has been connected to the three networks which are:

- the internal network,
- the external network (internet),
- and the DMZ network.

Test Approach

The developer's tests were conducted to confirm that the TOE meets the security functional requirements. The developer's strategy was to test the TOE against the specification of all security functions detailed in the developer's functional specification.

The tests cover all security functions defined in the Security Target [6]. The amount of developer tests ensures that the TSF behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

The majority of tests were performed as automated testing using a proprietary automated test tool named Xcite.

Test Results

The developer specified, conducted and documented suitable functional tests for each security function. The test results obtained for all of the performed tests turned out to be as expected. In a few cases retraceable aberrance to the expected results could be explained.

No errors or other flaws occurred with regard to the security functionality described in the functional specification. Consequently, the test results demonstrate that the behaviour of the security functions is as specified.

All security functions could be tested successfully. The manufacturer was able to demonstrate that all security functions behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

Independent Evaluator Tests

Test Configuration

Basis of all test configurations is an installed TOE as identified in the Security Target [6]. For the testing, ISA Server has been installed on HP/Compaq ProLiant DL380 G3 hardware, the underlying operation system is Windows Server 2003 Standard Edition (English) (build 3790) with SP1 including MS05-

042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch KB907865.

For ITSEF's independent testing as well as for the penetration testing, two test configurations including a configuration similar to the developer tests were used. The other configuration consists of an internal and an external network, separated by the TOE.

The evaluator tests have been performed at the ITSEF facility in Essen.

Test Approach:

The evaluation facility included all security functions in its test activities.

For choosing a sample of tests, the ITSEF accompanied all developer tests. All test cases and tests that were already conducted by the developer were taken into consideration, automated tests as well as manual tests.

Additionally, independent tests according to each TOE security function and other miscellaneous tests were conducted by the ITSEF. The objective was to test the functionality of the TOE and to verify the developer's test results.

To verify and reject possible vulnerabilities, the ITSEF performed penetration tests. Additionally, the TOE has been scanned with the vulnerability scanner Nessus and with the Internet Security Scanner (ISS) to identify possible vulnerabilities and to perform a port scan.

Test Results

The independent tests as well as the repeated manufacturer tests confirmed that the TOE's security functions behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

Penetration tests have been performed by the evaluation facility to assess possible vulnerabilities found during the evaluation of the different CC assurance classes. The TOE withstood the penetration efforts of attackers possessing basic or medium attack potential.

8 Evaluated Configuration

The TOE configuration consists of the software package "Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594". Web Cache, GUI (except Log Viewer component), RAS & VPN, Storage Service, IDS, other Management and Identification & Authentication functionality, Extensibility Features, some protocol filters and the used functionality of the underlying operating system and IT environment are not part of the evaluation.

Graphical taskpads and wizards do not belong to the TOE but are implemented in the environment , they shall simplify navigation and configuration for common tasks.

The operation system Windows 2003 Server maintains security attributes for all administrators. The TOE itself offers no additional identification and authentication methods for firewall administrators.

The storage of policy configuration data was not part of the evaluation (Windows Registry and ADAM with the ADAM configuration receiver service are outside the scope of the TOE), also scalability was not part of the evaluation.

The Enterprise Edition has been tested while running on one machine.

The evaluated TOE does not use Network Load Balancing, therefore it is not included in the evaluation.

The Enterprise Edition with local administration (which means that ADAM is located on the same machine as the TOE) identifies the TOE.

The ISA Server software including Service Pack 2 and the Administrator and User Guidance as parts of the evaluated version for the TOE are delivered on CD-ROM through the sales channels. The guidance documentation [8] that is used for the evaluation is present on the distributed CD-ROM. The additional Guidance Documentation Addendum [9] of the guidance documentation [8] is delivered via the web only.

The TOE is running on a is Windows Server 2003 Standard Edition (English) (build 3790) with SP1 operating system with additional corrections and was tested using a HP Proliant DL380 G3 hardware platform. For more details please read the Security Target [6], chapter 2.1.2. The TOE comprises the Enterprise Edition of the ISA Server 2004 with local administration.

9 Results of the Evaluation

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

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented 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
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Evaluation of flaw remediation	ALC_FLR.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS

Assurance classes and components		Verdict
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Moderately resistant	AVA_VLA.3	PASS

Table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_VLA.3 and ALC_FLR.1.
- there is no rateable security function within the TOE, therefore there is no strength of function claim.

This is a re-certification based on BSI-DSZ-CC-0262-2005 which is the standard edition of ISA Server 2004. The results of the evaluation are only applicable to the product Microsoft Internet Security and Acceleration Server 2004 - Enterprise Edition - Service Pack 2 - Version 4.0.3443.594 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] and the chapters 2, 4 and 8 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 User 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 [6] 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. Please read also chapter 8 of this report.

The user of the TOE has to be aware of the existence and purpose of the Guidance Documentation Addendum [9]. Therefore, the TOE's Internet product homepage has to provide information about the existence of the document and describe how to access the document. The reference has to be unambiguous and permanent.

The guidance and the Guidance Documentation Addendum contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ADAM	Active Directory Application Mode
AGD	Guidance Documentation (according to the CC assurance class “ Guidance Documentation”)
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
DMZ	Originally an abbreviation for demilitarised zone. In firewall terms a DMZ separates the internal network from the hostile forces of the Internet.
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ISA-Server	Internet Security and Acceleration Server
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console, a configuration management tool supplied with Windows 2003 Server that can be extended with plugins
MSDE	Microsoft Database Engine
OWA	Outlook Web Access

PP	Protection Profile
RAS	Remote Access Service
RPC	Remote Processor Call
SF	Security Function
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer, a protocol that supplies secure data communication.
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VPN	Virtual Private Network

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] ISA Server 2004 Common Criteria Evaluation - Security Target, Version 1.1, Date 2006-05-11, Microsoft Corporation

[7] Evaluation Technical Report, BSI-DSZ-CC-0387-2007, Version 3, Datum 2007-02-22, TÜV Informationstechnik GmbH (confidential document)

[8] Microsoft Internet Security and Acceleration Server 2004 manual – Enterprise Edition, available on CD-ROM (part of ISA Server 2004 EE package), File properties - name: isa.chm, date: 2006-01-18, size: 1.185.726 bytes

[9] ISA Server 2004 Enterprise Edition Common Criteria Evaluation, Guidance Documentation Addendum – Enterprise Edition; Version 1.5; Date: 2007-02-09

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.”