Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0453-2009

for

## Microsoft Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, Build 5.0.5720.100

from

## Microsoft Corporation

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

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

## BSI-DSZ-CC-0453-2009

**Microsoft Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, Build 5.0.5720.100**

| | |
|---|---|
| from | Microsoft Corporation |
| PP Conformance: | None |
| Functionality: | Product Specific Security Target<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by<br>AVA_VLA.3 and ALC_FLR.3 |

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

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 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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

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

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

Bonn, 9 February 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

# Preliminary Remarks

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

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

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

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

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

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

[1] Act 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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

## 2 Recognition Agreements

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

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

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

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

## 2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 03 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 Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

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

## 2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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

This evaluation contains the component AVA_VLA.3 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 component AVA_VLA.2 is relevant.

# 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 2006 Standard / Enterprise Edition, Build 5.0.5720.100 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, Build 5.0.5720.100 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 28 January 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Microsoft Corporation

The product was developed by: Microsoft Corporation

[6] Information Technology Security Evaluation Facility

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

# 4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

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

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

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

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

# 5 Publication

The product Microsoft Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, Build 5.0.5720.100 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Microsoft Corporation
1 Microsoft Way
Redmond
WA 98052
USA

This page is intentionally left blank.

# B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the Firewall product Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, short: ISA Server 2006 SE/EE (named ISA Server hereinafter).

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 Form Based Authentication. Form Based Authentication is secured by SSL with at least 128 bit encryption which is provided by the IT environment, such is the verification of the user credentials.
- 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.

The product package of ISA Server includes a set of additional tools, graphical taskpads and wizards which are not part of the TOE but which are implemented in the environment, for details please read chapter 2.2 of the Security Target [6].

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_VLA.3 and ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.4.

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

| TOE Security Function | Addressed issue |
|---|---|
| SF1: Web Identification and Authentication | The TOE can be configured that only particular users are allowed to access Web applications through the TOE using Form Based Authentication. |
| SF2: Information Flow Control (Packet and Application Filtering) | The TOE combines security mechanisms to enforce security policies at different network layers. |
| SF3: Audit | The TOE stores logging information in different log files in the environment. |

Table 1: TOE Security Functions

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

There is no strength of functions claim for the TOE.

Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

The TOE ISA Server is a subset of the product package of ISA Server.

For details about the evaluated configurations of the TOE and the configuration options relevant for a user please read chapter 8 of this report, Evaluated Configuration, and the the Security Target [6], chapter 2. 1.3.4 and chapter 5.4.

This certification covers the following configurations of the TOE: Standard Edition (single machine support only) and Enterprise Edition (for large-scale deployments).

ISA Server 2006 Standard Edition shares the feature set of Enterprise Edition, but it is intended for small businesses, workgroups, and departmental environments. Standard Edition provides local policy only, and supports up to four processors. Enterprise Edition has no hardware limits.

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 2006 Standard / Enterprise Edition, Build 5.0.5720.100**

The following table outlines the TOE deliverables:

| No | Type | Deliverables | Version | Comment |
|---|---|---|---|---|
| 1 | SW | ISA 2006 SE Box incl. CD-ROM<br>or<br>ISA 2006 EE Volume Licensing CD-ROM | ISA 2006 SE 5.0.5720.100<br>or<br>ISA 2006 EE 5.0.5720.100 | CD-ROM ISA Server 2006 Standard Edition contains [9]<br>CD-ROM ISA Server 2006 Enterprise Edition contains [9] |
| 2 | DOC | Guidance [9] | File size: 689664 bytes, File date: 2006-07-18 | Microsoft Internet Security and Acceleration Server 2006 manual - Standard Edition & Enterprise Edition, available on CD-ROM (part of ISA Server 2006 SE/EE package) |
| 3 | DOC | Guidance Documentation Addendum (of the Administrator and User Guidance) [10] | 1.6 | Microsoft Internet Security and Acceleration Server 2006 manual addendum – Standard Edition & Enterprise Edition It can be downloaded from the CC ISA page under https://go.microsoft.com/fwlink/?linkid=49507. |
| 4 | SW /<br>DOC | File integrity verification package containing SHA-1 hash values stored in XML files, for<br>- Standard Edition<br>- Enterprise Edition | MS ISA Server 2006 Integrity Check Package, consists of following files<br>(filename/bytes/date/<br>time):<br>integritycheck_ee_ENU.cmd 2541/2008.11.14/08:33<br>integritycheck_se_ENU.cmd 2526/2007.11.14/08.33<br>ISA2K6FPPS_EN.xml 90914/2008.04.09/16:11<br>ISA2K6SELE_EN.xml 90914/2008.04.09/16:11<br>readme.htm 3694/2008.04.09/16:11 | This Package contains SHA-1 hash values stored in XML files which can be used by customers to verify the TOE version. These files contain checkfiles for ISA Server 2006 Standard Edition and ISA Server 2006 Enterprise Edition. For further information see [10, chapter 5]) |
| 5 | SW | FCIV Tool | 2.05 | The FCIV tool is used to verify the integrity of the TOE with the provided integrity check files. It can be downloaded from: http://support.microsoft.com/default.aspx? scid=kb;enus;841290 (for further information see [10, chapter 5]) |

Table 2: Deliverables of the TOE

The TOE deliveries “CD-ROM ISA Server 2006 Standard Edition” and “CD-ROM ISA Server 2006 Enterprise Edition” do not differ from the product deliveries.

The method to examine the ISA Server version number is included in the Microsoft Management Console. The user can identify the version of the TOE in the Help menu (Help -> About ISA Server 2006). The version number presented in the Microsoft Management Console is 5.0.5720.100. That version corresponds to the evaluated version. From that display it is not obvious which configuration of ISA Server 2006 is installed. Therefore, when the left pane of the management console displays the branch “Enterprise” the ISA Server 2006 EE is installed.

Note: Although administration and management tools are delivered together with the TOE, they are excluded from the TOE and are considered part of the environment. 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.

# 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 Form Based Authentication. Form Based Authentication is secured by SSL with at least 128 bit encryption which is provided by the IT environment, such is the verification of the user credentials.

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

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).

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 following functionality: local identification and authentication of user credentials used for web publishing (see A.WEBI&A for Radius identification and authentication; in case of a successful authentication the TOE analyses the returned value and allows or denies the access to network resources depending on that value), reliable time stamp (log file audit), file protection (for log file access protection, registry protection, and ADAM protection), cryptographic support (for SSL encryption), administration access control, reliable ADAM implementation (for EE configuration only), Network Load Balancing (for EE configuration only, disabled by default). (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 Form-based 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.

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 TOE consists of the following components:

- Firewall Service Core: Firewall Service is responsible for the application filtering. It also logs incoming and outgoing traffic on session level.
- ISA Control Service: ISA Server Control Service protocols log failures and events in the Windows Application Event Logfile.
- Web filter: Web filter checks incoming and outgoing web requests (additional filters are accessed using the ISAPI interface by this subsystem).
- Packet Engine: Contains the IP Packet Filter which filters traffic on packet level. Used to manage packets that are transferred to and from the TCP/IP protocol driver. It also logs incoming and outgoing traffic on packet level.
- Log Viewer: Allows querying and sorting of log data.
- Web Application filters: Any application filter for web content is called “Web Application filter”. In ISA Server 2006 evaluation we have: HTTP, FBA, Authentication Delegation Filter, and Radius filter.
- Application Filters: Other application filters for non web content are called simply “Application filters”. In ISA Server 2006 we have: FTP access filter, RPC and SMTP filtering.
- Rules Engine: Implements content and protocol checks Used by the Web filter and some Application filters to perform content checks.

- Logging: Creates log entries in the log database Creates Windows Application Event Logfile.

# 6 Documentation

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

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

# 7 IT Product Testing

## Developer Tests

Test Configuration

The TOE has been tested in both configurations (SE and EE) within a configuration that consists of five networks. The TOE as the centre of the configuration has been connected to the five networks which are:

- the internal network,
- the IntraArray network,
- the external network (internet),
- the DMZ network.
- the second 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 a Dell OptiPlex GX260 hardware, the underlying operation system is Windows 2003 Server Standard Edition (build 3790, English) 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 a vulnerability scanner 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 moderate attack potential.

# 8 Evaluated Configuration

This certification covers two configurations of ISA Server 2006:

- Standard Edition (single machine support only) It is intended for small businesses, workgroups, and departmental environments. Standard Edition provides local policy only.
- Enterprise Edition (for large-scale deployments) 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.

The configuration is chosen by executing the corresponding setup (Standard Edition setup or Enterprise Edition setup).

For the ISA Standard Edition, security policy configuration data is stored in the local Windows registry. 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. Both configurations - Standard and Enterprise - can be treated in the same way because the storage of policy configuration data is not part of this evaluation (Windows Registry and Active Directory are outside the scope of the TOE) and also scalability is not part of the evaluation.

NLB, ADAM, Web Cache, Firewall Client, GUI (except Log Viewer component), RAS & VPN, Storage Service, IDS, Management and Identification & Authentication functionality (other than considered in SF1/2/3), Extensibility Features, Protocol Filters (other than considered in SF2) and the underlying operating system Windows 2003 Server are not part of the evaluation.

For the ISA Enterprise Edition, local administration (single machine) has been chosen as the evaluated TOE configuration. Therefore, as said above, Network Load Balancing is disabled by default.

The document „Microsoft Internet Security and Acceleration Server 2006 manual addendum – Standard Edition & Enterprise Edition, Version 1.6“ [10] describes the evaluated configuration and the necessary setup to achieve the evaluated configuration.

The product homepage is

https://go.microsoft.com/fwlink/?linkid=49507

It gives instructions for a secure download and delivery of all TOE deliverables and gives necessary hash values for a verification of the TOE integrity. It also links to the downloads of all TOE deliverables that are additional to the boxed CD.

The TOE itself has to be installed and configured following all instructions given in [10].

The TOE is running on a Windows 2003 Server Standard Edition (build 3790, English) SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch KB907865 and was tested using a Dell OptiPlex GX260 hardware platform.

For more details please read the Security Target [6], chapter 2.

# 9 Results of the Evaluation

## 9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL4 and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)

- The components AVA_VLA.3 and ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VLA.3 and ALC_FLR.3

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

### 9.2 Results of cryptographic assessment

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

## 10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 of this report contain necessary information about the usage of the TOE and all security hints therein have to be considered. 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 administrator should verify that all software installed on the TOE server (other than the TOE itself) operates as intended.

The user of the TOE has to be aware of the existence and purpose of the Guidance Addendum Document “Microsoft Internet Security and Acceleration Server 2006 manual addendum – Standard Edition & Enterprise Edition, Version 1.6” [10]. Therefore, the TOE’s Internet product homepage (see below) 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 document contains necessary information about the usage of the TOE and all security hints therein have to be considered.

The TOE itself has to be installed and configured following all instructions given in [10].

The TOE is running on a Windows 2003 Server Standard Edition (build 3790, English) SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch KB907865.

The developer must publish the secure product homepage

https://go.microsoft.com/fwlink/?linkid=49507

The product homepage must contain all information for a secure download and verification of the TOE items including hash values as specified in this report and all links to the TOE items as specified in this report, see table 2 in chapter 2.

The links as well as the hash values are required for verification of the components along with the descriptions for a secure download and the FCIV tool. They have to be present throughout the validity of this certificate.

# 11 Security Target

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

# 12 Definitions

## 12.1 Acronyms

| | |
|---|---|
| **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 |
| **FCIV** | File Checksum Integrity Verifier |
| **FTP** | File Transfer Protocol |
| **GUI** | Graphical User Interface |
| **HTTP** | Hypertext Transfer Protocol |
| **IDS** | Intrusion Detection System |
| **ISA-Server** | Internet Security and Acceleration Server |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **LDAP** | Lightweight Directory Access Protocol |
| **MMC** | Microsoft Management Console, a configuration management tool supplied with Windows 2003 Server that can be extended with plugins |
| **NLB** | Network Load Balancing |
| **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 |

## 12.2 Glossary

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

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

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

**Informal** - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

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

[6] ISA Server 2006 SE/EE Common Criteria Evaluation - Security Target, Version 1.1, Date 2007-06-05, Microsoft Corporation

[7] EVALUATION TECHNICAL REPORT (ETR), Version: 2, Date: 2009-01-05, Certification ID: BSI-DSZ-CC-0453, Internet Security and Acceleration Server 2006 Standard / Enterprise Edition (confidential document)

[8] ISA Server 2006 SE/EE Common Criteria Evaluation - ISA Server 2006 - Executable and DLL Reference, Version 1.3, 2007-10-25, Microsoft Corp.; ISA Server 2006 SE/EE Common Criteria Evaluation - Configuration Management / Delivery and operation, Version 1.4, 2008-11-12, Microsoft Corp.; ISA Server 2006 SE/EE Common Criteria Evaluation - Reference List, Version: 1.8, Microsoft Corp. (confidential document)

[9] Microsoft Internet Security and Acceleration Server 2006 manual - Standard Edition & Enterprise Edition, available on CD-ROM (part of ISA Server 2006 SE/EE package), File size: 689664 bytes, File date: 2006-07-18, Microsoft Corporation

[10] Microsoft Internet Security and Acceleration Server 2006 manual addendum – Standard Edition & Enterprise Edition, Version 1.6, Date 2008-11-12, Microsoft Corporation

[8] specifically

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

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

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

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

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

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

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

CC Part 3:

**Protection Profile criteria overview** (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

**Security Target criteria overview** (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

**Assurance categorisation** (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

**Evaluation assurance levels** (chapter 11)

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

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

**Evaluation assurance level (EAL) overview** (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

**Vulnerability analysis (AVA_VLA)** (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

# D Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.