Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0436-2009

for

Microsoft Exchange Server 2007 Enterprise Edition (English)

Version/Build 08.02.0176.002

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-0436-2009

e-mail Server

Microsoft Exchange Server 2007 Enterprise Edition (English)
Version/Build 08.02.0176.002

from	Microsoft Corporation
PP Conformance:	None
Functionality:	product specific Security Target; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria
Recognition
Arrangement

Common Criteria

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

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

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

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

Bonn, 16 November 2009
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

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)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

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

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

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

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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

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

2.2 International Recognition of CC - Certificates

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

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Microsoft Exchange Server 2007 Enterprise Edition (English) Version/Build 08.02.0176.002 has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Exchange Server 2007 Enterprise Edition (English) Version/Build 08.02.0176.002 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 01 October 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.

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

[6] Information Technology Security Evaluation Facility

4 Validity of the certification result

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

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

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

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

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

5 Publication

The product Microsoft Exchange Server 2007 Enterprise Edition (English) Version/Build 08.02.0176.002 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Microsoft Corporation
One Microsoft Way
Redmond
WA 98052-6399
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 TOE is the product Microsoft Exchange Server 2007 Enterprise Edition (English) Version/Build 08.02.0176.002 (hereinafter called “Exchange 2007“). The TOE is a messaging system, more precisely an e-mail and collaboration server providing secure access to personal and shared data to a variety of clients using various protocols. Using Exchange 2007, users throughout an organization can access e-mail, voice mail, calendars, and contacts from a ariety of devices and from any location.

It is possible to connect to the TOE by using different clients. The different clients are categorised into the following groups:

- Generic Client (also known as Internet Client): A client of this type could be any mail client that uses SMTP to connect to the TOE or a web browser that uses HTTP or Web Services to connect to the TOE.
- Outlook client: In contrast to the generic Clients, an Outlook client uses RPC (or RPC over http) to connect to the TOE.

In addition to the above clients, the TOE allows users to connect using a standard or IP telephone via Outlook Voice Access. To use standard telephones, a PBX must be connected to the TOE. A PBX may also forward IP calls.

The Unified Messaging server role in Exchange 2007 lets users access voice mail, e-mail, fax messages, and calendar information located in their Exchange 2007 mailbox from an e-mail client such as Microsoft Outlook or Outlook Web Access, from a mobile device that has Microsoft Exchange ActiveSync enabled.

Furthermore, the SMTP protocol can be used by a SMTP server to connect to the TOE.

The scope of the TOE ends at the interfaces where it provides its services and does not include any functionality of any client. Therefore all clients that can be used to connect to the TOE are not addressed during the evaluation.

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 EAL4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. 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 5.3.

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

TOE Security Function	Addressed issue
SF.SM	Security Management
SF.AC	Access Control
SF.CF	Connection Filtering

TOE Security Function	Addressed issue
SF.MF	Message filtering
SF.AF	Attachment Filtering
SF.TF	Transport Filtering
SF.I&A	Identification and Authentication
SF.DGR	Distribution Group Restriction
SF.QTA	Mailbox and public folder quota

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The claimed TOE's Strength of Functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 5.4 is confirmed.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. 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 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 Exchange Server 2007 Enterprise Edition (English)
Version/Build 08.02.0176.002

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Base TOE Binaries: Microsoft Exchange Server 2007 Enterprise Edition (English)	Version/Build 08.02.0176.002	DVD-ROM (boxed, COTS software)
2	SW	TOE update: Service Pack 2 of Microsoft Exchange Server 2007 Enterprise Edition (English)	File name: E2K7SP2EN64.exe File size: 927.226.128 Bytes SHA-1 hash value: B302A90819DE0217545D63E511591F3A5B3D9F43	Download from website: https://secure.tuvit.de
3	DOC	Microsoft Exchange Server 2007 Enterprise Edition Common Criteria Evaluation – Guidance Addendum [9].	Version 1.10 Date: 2009-09-28	Download from website: https://secure.tuvit.de

No	Type	Identifier	Release	Form of Delivery
4	DOC	Guidance: Microsoft Exchange Server 2007 Help [10]	File name: ExchHelp.chm SHA-1: 89C3A03E89B64E224A0D26E24B94B77C2E2264BC File size: 22.662.404 Bytes August 2009	Download from website: https://secure.tuvit.de
5	SW	TOE verification tool: File Checksum Integrity Verifier (FCIV) utility	File name: windows-kb841290-x86-enu.exe Version 1.4 File size: 119.600 bytes SHA-1 hash value: 99fb35d97a5ee0df703f0cdd02f2d787d6741f65	Download from website: https://secure.tuvit.de
6	DATA	Checksums to be verified by FCIV: Integrity Check Validation Data: SHA-1 hash values for Exchange Server 2007 Enterprise Edition and SP2	File name: checkfiles_ex2k7(sp2).zip File size: 109.770 bytes SHA-1 hash value: 19F62B8B115C0B5D0E3B3F1FA3AF0C61A2893D84	Download from website: https://secure.tuvit.de

Table 2: Deliverables of the TOE

Note that a help file is already delivered on the product-DVD. Nevertheless a newer version which also covers the issues of SP2 is released on the internet. That help-file [10] is the main guidance documentation for the purposes of this certification aspect whereas the addendum [9] extends [10] to CC related issues.

Please note that the DVD contains elements that exceed the TOE and that are not part of the evaluation. For the evaluated scope please read the Security Target [6] as well as the Guidance Addendum [9].

To identify the TOE use the Exchange Management Shell and execute the command ‘get-ExchangeServer | fl‘. Within the field ‘AdminDisplayVersion’ as part of the returned attributes the TOE will display ‘Version 8.2 (build 176.2)’ which corresponds with build 08.02.0176.002. Within the field ‘Edition’ as part of the returned attributes the TOE will display the information ‘Enterprise’. The Enterprise Edition marks the TOE.

The Exchange Server package shipped physically is equipped with a label, i.e. the Certificate of Authenticity (COA) label, particularly including the identifier ‘EXCHANGE SVR ENT 2007 X64 ENGLISH’ for Exchange Server 2007 Enterprise Edition (English). This package labelling ensures the TOE identification for consumers at the point of receipt of the DVD. Additionally, according to the instructions in the Guidance Addendum [9] and on the web page https://secure.tuvit.de, hash values ensure the integrity of the product components.

3 Security Policy

The security policy of the TOE provides different aspects of security management through the Exchange Management Shell that is a task-based command line shell which exposes administration functionality necessary for administering the TOE.

The TOE controls access of users to the types of Exchange Server 2007 data stores which are mailboxes and public folders. Connection filtering is done by using allow and block lists which may contain IP addresses, IP address ranges. Message filtering will accept or reject messages based different rules configurable by the administrator. Attachment filtering provides the ability to specify that messages which contain a specified attachment or attachment type will be subject to a predefined action. Transport filtering allows to configure a set of ordered rules that can be applied to all messages passing through the Hub Transport server role. Identification and Authentication identifies and authenticates all users connecting via non-TLS secured Outlook Voice Access. The identity of the user is represented by the user's mailbox number or a telephone number that is transmitted from the PBX to the TOE. Furthermore the TOE supports the restriction of distribution groups by several security attributes. Another security policy of the TOE is to allow the Exchange Administrator to set different levels of quotas for size restrictions on a mailbox.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The security objectives related to the environment of the TOE can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The TOE comprises software installed on Windows servers and its related guidance documentation. An installation of the TOE can be found in figure 1 of the Security Target [6] and consists of the following server roles components:

Mailbox Server Role:The Mailbox server role hosts mailbox and public folder databases.

Client Access Server Role: This is the server that hosts the client protocols.

Unified Messaging Server Role: Unified Messaging combines voice messaging, fax, calendaring and e-mail, which are accessible from a telephone or a computer.

Hub Transport Server Role: This is the mail routing server that routes mail within the Exchange organization.

Edge Transport Server Role: This is the mail routing server that sits at the perimeter of the network topology and routes mail into and out of the Exchange organization.

For more information and for a graphical overview of the TOE please read chapter 2.2 of the Security Target [6].

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 developer testing was performed on two different configurations. For automated tests the TOE was configured such that the Edge role was installed on one machine and all other roles (Unified Messaging, Client Access, Mailbox and Hub Transport) were installed on another machine. For manual tests the configuration consisted of a network with the following components (each component is realised on a separate machine): Client Access, UM & Mailbox, Hub Transport, Firewall, Active Directory, Edge, Test Client, and SIP Client. All components were connected through hubs.

Test Approach

The developer's tests were conducted to confirm that the TOE meets the security functional requirements. The tests include both automated tests and manual tests. The developer's strategy was to test the TOE against the specification of all security enforcing functions detailed in the developer’s functional specification. The tests cover all security functions defined in the ST [6].

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 were as expected. No errors or other flaws occurred with regard to the security functionality or the mechanisms defined in the developer’s functional specification. The test results demonstrate that the behaviour of the security functions is as specified.

All security functions could be tested successfully and the manufacturer provided sufficient information to describe the realisation of the security functions. The manufacturer was able to demonstrate that all security functions operate as specified in the developer’s functional specification.

Independent Evaluator Tests

Test Configuration

The test configuration is similar to the developer’s test configuration and is running on Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English) with the patches according to [9], chapter 7.1.

Test Approach

The evaluator aimed to cover all Security Functions which are mentioned in the Security Target. The evaluator selected test cases addressing the main security features of the security function. The selected test cases assure that all security functions (as defined in the ST [6] and described in the developer’s functional specification) are tested regarding their functional behaviour and all TSP-enforcing subsystems are covered. Additionally the evaluator conducted independent tests according to each TOE security function as well as miscellaneous tests, performed manually.

The evaluator's objective regarding these tests was to test the functionality of the TOE as described in the developer documents and to verify the developer’s test results.

To verify and reject possible vulnerabilities, the ITSEF also performed a set of penetration tests based on the developers and the independent vulnerability analysis and containing proprietary test scripts, different e-mail clients, and third-party penetration testing tools including a vulnerability scanner to identify possible known vulnerabilities.

Test Results

The independent tests as well as the repeated developer tests confirmed the TOE functionality as described in the developer documents. Some findings during the testing lead to minor changes of the test- and guidance documentation and to some clarifications in the developer's design documentation upon which the test cases had been created. Beside this no hints to any errors were given.

Penetration tests have been performed by the evaluation facility with the result that the TOE is resistant against attacks based upon the level of low attack potential.

According to the intended operational environment, typical attackers possessing basic attack potential will not be able to exploit the vulnerabilities of the TOE.

8 Evaluated Configuration

Although a help-file (i.e. Guidance) is delivered within the product package DVD, consumers need to download the evaluated version of the Guidance [10] as well as the addendum [9]. They need to be downloaded from the secure web-site https://secure.tuvit.de. Both documents are part of the certified version as they are relevant for administration and usage of the TOE in the certified version and configuration. The version of the help-file on the product DVD is out of scope of the certification.

The TOE has to be installed and configured according to the Guidance Addendum [9] which covers the certified version of the TOE. The certified version includes SP2 of the product. SP2 is not part of the product package DVD and has to be downloaded from the secure web-site https://secure.tuvit.de.

The secure product homepage https://secure.tuvit.de gives instructions for the secure download and verification of all components of the TOE and should be followed. The Guidance Addendum [9] gives more detailed information about the download of all components, the verification of the TOE integrity by hash values, the secure installation of all components, and the certified configuration of the TOE.

Please note that there exists a Standard Version of the product, too. Only the Enterprise Edition marks the TOE. The Standard Edition is not included in the certificate. Neither is a 32 bit version of the product (which, however, is not contained in the product DVD anyway.)

The platform for the TOE is Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English) operating system with patches. The Guidance Addendum [9] chapter 7.1. gives information about the required patches for the TOE platform.

The platform includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

For administration of the product package, Exchange Server 2007 includes graphical task pads and wizards. These features simplify navigation and configuration for common tasks. They are embedded in the Exchange Management Console and do not belong to the TOE. Therefore the user is advised to use the corresponding cmdlets (A "cmdlet," pronounced

"command-let", is the smallest unit of functionality of the Exchange Management Shell) for administrating purposes (see [9] chapter 5.2.2.).

The features “IMAP4 and POP3 protocols” are included in the Exchange product package but outside the logical scope of the TOE. Further, the logical scope of the TOE does not include any functionality of any client. The way external lists for filtering of messages are compiled and transferred is also out of scope of the evaluation.

Some security functionality of the TOE environment, namely of the operating system, is used by the TOE which includes aspects of Identification and Authentication, TOE Data Protection, and TOE Data Management. For details please read the Security Target [6] which gives information about product features that are excluded from the certification (chapter 2.3.3) and important functionality of the environment (chapter 2.3.4).

In general, for installation, configuration, and administering the TOE please follow the Guidance Addendum [9] with its framed important notes.

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 EAL4 package as defined in the CC (see also part C of this report)
- The component ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: product specific Security Target;
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3
- The following TOE Security Functions fulfil the claimed Strength of Function: medium SF.I&A (realised by a probabilistic or permutational mechanism)

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 cryptographic algorithms. 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 Guidance Addendum Document [9] contains necessary information about the usage of the TOE and all security hints therein have to be regarded. This mainly (but not entirely) comprises the following aspects:

- Assumptions/security objectives of the environment, particularly the requirements for physical protection of the TOE, protection of the communication channel, secure installation of the TOE (no untrusted software shall be installed on the machines the TOE is installed on), secure installation of the platform the TOE is running on and usage of third party block/allow lists from trustworthy sources only.
- Instruction how to verify the integrity of the TOE deliverables. The informations are supplemented by the secure Exchange Server 2007 common criteria web page https:// secure.tuvit.de.
- Disabling ExOLEDB, CDOEX and WebDAV.
- Preventing local logon for non-administrators on the TOE systems.
- Not enabling IMAP4/POP3.
- Setting the minimum Outlook Voice Access PIN length to 8.

The user of the TOE has to be aware of the existence and purpose of the Guidance Addendum Document [9]. Therefore, the TOE's Internet product homepage (https://secure.tuvit.de) 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 TOE itself has to be installed and configured following all instructions given in [9].

The TOE is running on a Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English) operating system with all patches as listed in the Guidance Addendum [9] chapter 7.1.

The developer must publish the secure product homepage

https://secure.tuvit.de

The product homepage must contain all information for a secure download and verification of the TOE items including SP2, documents, and 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

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
CDOEX	Component Object Model for Exchnge
COA	Certificate of Authenticity
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ExOLEDB	Exchange OLE DB Provider
FCIV	File Checksum Integrity Verifier
HTTP	Hypertext Transfer Protocol
HTTP-DAV	Hypertext Transfer Protocol Distributed Authoring and Versioning
IMAP4	Interactive Mail Access Protocol Version 4
IIS	Internet Information Service
IP	Internet Protocol
IT	Information Technology
OLE DB	Object Linking and Embedding, Database
OWA	Outlook Web Access
PBX	Private Branch eXchange
PDA	Personal Digital Assistant
PIN	Personal Identification Number
POP3	Post Office Protocol Version 3
PP	Protection Profile
RPC	Remote Procedure Call
RTM	Release to Manufacturing
SF	Security Function
SFP	Security Function Policy
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SOF	Strength of Function
SP	Service Pack
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WebDAV	Web-based Distributed Authoring and Versioning

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] Exchange Server 2007 Common Criteria Evaluation, Security Target, Version 1.38, Date 2009-09-28

[7] Microsoft Exchange Server 2007 Enterprise Edition (English) Version/Build 08.02.0176.002, EVALUATION TECHNICAL REPORT, Version 3, Date 2009-10-01, TÜV Informationstechnik GmbH (confidential document)

[8] Configuration list for the TOE: Exchange Server 2007 Common Criteria Evaluation, Configuration management Exchange Server, Version: 1.05, Date: 2009-09-28; including all document as referenced in chapter 3.2. (confidential documents)

[9] Microsoft Exchange Server 2007 Enterprise Edition Common Criteria Evaluation – Guidance, Addendum, Version 1.10, Date 2009-09-28

[10] Microsoft Exchange Server 2007 Help, File name ExchHelp.chm, SHA-1 value 89C3A03E89B64E224A0D26E24B94B77C2E2264BC, File size 22.662.404 Bytes, Date: August 2009

[8] specifically

- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

This page is intentionally left blank.

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.