Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0284-2005

for

Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021

from

Microsoft Corporation

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

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0284-2005

Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021

from

Microsoft Corporation

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0 for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 / augmented by** ALC_FLR.3 – Flaw Remediation – Systematic flaw remediation

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

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

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

Bonn, 9th November 2005

The President of the Federal Office
for Information Security

Dr. Helmbrecht / Hange L.S.

IT Security Certified

SOGIS - MRA

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

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

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

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

---

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

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

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

[5] Proclamation of the Bundesministerium des Innern of 22 September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

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

3 Performance of Evaluation and Certification

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

The product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 consists of Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 with Exchange Server 2003 Service Pack 1 installed and Exchange hotfix MS05-021 (KB894549) installed. The TOE is the product in its default configuration and it has undergone the certification procedure at BSI.

The evaluation of the product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 was conducted by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

Microsoft Corporation

1 Microsoft Way

Redmond, WA 98052, USA

The certification is concluded with

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

This work was completed by the BSI on 09. November 2005.

The confirmed assurance package is only valid on the condition that

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

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

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

---

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 has been included in the BSI list of the certified pro-ducts, which is published regularly (see also Internet: http://www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

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

B Certification Results

The following results represent a summary of

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

Contents of the certification results

1 Executive Summary

The TOE is the product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 (English) in its default configuration. It is an e-mail and collaboration server that provides secure access to personal and shared data to variety of clients using different protocols. Exchange clients include personal computers running RPC-based applications like Outlook 2003. Exchange 2003 includes a HTTP-DAV interface for HTTP access to reading and writing to the Exchange data stores. Non-PC clients such as PDAs and smartphones can also use Exchange 2003 via HTTP-DAV.

Components that are disabled in the default configuration of Exchange, such as the IMAP4, POP3, and X.400 protocol, are out of scope of the evaluation.

The security functionality of the TOE comprises access control for mailboxes and public folders, SMTP connection filtering based on domain names and IP addresses, SMTP message filtering based on senders and recipients, restriction of the use of distribution lists, limiting mailbox and public folder sizes (quotas), and security management capabilities.

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/HTTP-DAV to connect to the TOE.
- Outlook client: In contrast to the generic Clients, an Outlook client uses RPC to connect to the TOE.

In addition, the SMTP protocol can be used by an SMTP server to connect to the TOE. All clients (e.g. Outlook) or SMTP servers that may establish a connection to the TOE are outside the scope of the TOE and have not been included in the evaluation.

The IT product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 16.09.2005. The TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and vendor and distributor is:

Microsoft Corporation

1 Microsoft Way

Redmond, WA 98052, USA

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

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

1.2 Functionality

The TOE provides following functionality:

SFR	Name
Class FDP: User Data Protection	
FDP_ACC.1.a	Subset Access Control
FDP_ACC.1.b	Subset Access Control
FDP_ACF.1.a	Security Attribute Based Access Control
FDP_ACF.1.b	Security Attribute Based Access Control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
Class FRU: Resource Allocation	
FRAU_RSA.1.a	Maximum Quotas
FRAU_RSA.1.b	Maximum Quotas
Class FMT: Security Management	
FMT_MSA.1.a	Management of Security Attributes
FMT_MSA.3.a	Static Attribute Initialization
FMT_MSA.3.b	Static Attribute Initialization
FMT_MSA.3.c	Static Attribute Initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1.a	Security Roles

Table 1: TOE Security Functional Requirements

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

Security function
SF.SM: Security Management
SF.AC: Access Control
SF.CF: Connection Filtering
SF.MF: Message Filtering
SF.DLR: Distribution List Restriction
SF.QTA: Mailbox and Public Folder Quota

Table 2: TOE security functions

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

1.3 Strength of Function

There is no strength of functions claim for the TOE.

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

The following list of considered threats for the TOE is defined in the Security Target [5], chapter 3.2:

T.UNAUTH_DAC

A user who is not authenticated may attempt to read, create, modify or delete information contained in private stores (i.e. mailboxes) or public stores (i.e., public folders), which are managed by the TOE. An attacker may try to acquire access to mailboxes or public folders although he has no account information and is not authenticated.

T.AUTH_DAC

A user who has been authenticated may attempt to read, delete or modify information contained in another user's private store for which this user has not been authorized, e.g., no permissions to open the mailbox.

T.UNAUTHUSE

An authenticated user may attempt to read, delete or modify information contained in a public folder (e.g. shared folders and documents) that belongs to a group the user is not a member of or is not authorized to use.

T.SPAM

Unsolicited Commercial email (UCE or spam), which is known to be from unsolicited senders (based on the sender IP address of the corresponding SMTP connection or the sender/recipient email addresses within the mails), are delivered to mailboxes controlled by the TOE.

T.DL_MISUSE

An unauthenticated user or an authenticated but unauthorized user may send messages through a distribution list consuming TOE resources delivering inappropriate email, such as UCE or improper employee use.

T.OVERFLOW

An attacker may attempt a denial of service attack by attempting to overflow an individual's mailbox or a mail-enabled public folder by sending a large amount of mail to the corresponding email address(es).

1.5 Special configuration requirements

The security target [5] has identified the configuration of the TOE in evaluation: Exchange Server 2003 Enterprise Edition (English), Version/Build 6.5.7226.0 (i.e. Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 with Exchange Server 2003 Service Pack 1) and Exchange hotfix MS05-021 (KB894549) installed, achieved by and detailed in the guidance documentation addendum [8] which is also part of the TOE.

The TOE is the Exchange Server 2003 in its default configuration.

The Exchange Server 2003 software and the Guidance documentation as parts of the evaluated version for the TOE are provided as a boxed product that is delivered to the sales channels.

Relevant for the evaluated version of the TOE is the Guidance Documentation that is delivered together with the software on CD-ROM [7]. The Guidance Addendum [8] is also part of the evaluated version of the TOE. It is only available as a Word document via a secure channel on the vendors TOE-internet-homepage. The Service Pack and the Hotfix that are part of the TOE are delivered via the web only.

The TOE runs on the platform Windows Server 2003 operating system (exact denotation/version: Windows Server 2003 Enterprise Edition (English) (incl. IIS 6.0 and Active Directory), Version/Build RTM – 3790), which includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

The following security functionality of Windows Server 2003 (i.e. the TOE environment) is used by the TOE: Identification and Authentication, Communications Security, TOE Data Protection. For details please see Security Target, chapter 2.3 [5].

The clients or SMTP servers that may establish a connection to the TOE are outside the scope of the TOE and were not evaluated.

The features “handling of IMAP4, POP3 and X.400 protocols” are outside the logical scope of the TOE due to the fact that they are disabled in the default configuration of Exchange.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [5], chapter 3.1:

A.I&A

The platform upon which the TOE resides (Windows Server 2003 operating system) provides methods to identify and authenticate users and to provide the TOE with corresponding user IDs and attributes.

A.ACCESS_CONTROL

The platform upon which the TOE resides (Windows Server 2003) will be configured to restrict modification to TOE executables, the platform itself, configuration files, databases (mailboxes and public folders) and cryptographic keys to only the authorized administrators.

A.COM_PROT

The platform upon which the TOE resides provides methods to protect communications between the TOE and remote trusted IT products in terms of authenticity and confidentiality. This includes an adequate key management for Internet protocols.

A.INSTALL

The TOE will be delivered, installed, configured and setup in accordance with documented delivery and installation/setup procedures. In the default installation procedure of the TOE IMAP4, POP3 and X.400 protocols are disabled and it is assumed that the administrator does not enable them after installation. The administrator has to ensure that connection/sender/recipient filtering functionality is enabled. The administrator has to ensure that quota functionality is enabled and that reasonable quotas have been configured with respect to the number of mailboxes and mail-enabled public folders and available disk space.

A.MANAGE

There will be one or more competent administrator(s) assigned to manage the TOE and its platform and the security of the information both of them contain.

A.NO_EVIL_ADM

The administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.

A.PHYS_PROTECT

The TOE and its platform will be located within facilities providing controlled access to prevent unauthorized physical access.

A.CORRECT_HW

The hardware/firmware that runs the operating system operates correctly and as the operating system expects.

1.7 Disclaimers

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

2 Identification of the TOE

The TOE is the product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 (English) in its default configuration and consists of Exchange Server 2003 Enterprise Edition (English), Version/Build 6.5.7226.0 (i.e. Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 and Exchange Server 2003 Service Pack 1 installed) and Exchange hotfix MS05-021 (KB894549) installed.

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

Deliverables	Version	Comment
Microsoft Exchange Server 2003 Enterprise Edition (English)	6.5.6944.0	Box with CD-ROM Exchange Server 2003 Enterprise Edition including Guidance Documentation [7]
Guidance Documentation	File properties - name: exadmin.chm, date: 24.06.2003, size: 957.988	Guidance Documentation: Exchange Server 2003 Administration Guide and Exchange Server 2003 product help (as part of Exchange Server 2003 Enterprise Edition package; available on CDROM) (available on installed TOE under menu “Help -> Help

Deliverables	Version	Comment
	Bytes	topics -> Microsoft Exchange Server 2003”)
Guidance Addendum	1.13	The Guidance addendum [8] has to be directly downloaded from the Microsoft Exchange Server 2003 Common Criteria webpage. The general Exchange Server 2003 Common Criteria web page can be reached as follows: 1. enter: http://www.microsoft.com/exchange (Exchange Server main page) 2. go to: Product Information 3. go to: Certification
Exchange 2003 Service Pack 1 (English)	6.5.7226.0 (i.e. Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 and Exchange Server 2003 Service Pack 1 installed)	Downloadable under: http://www.microsoft.com/downloads/details.aspx?FamilyID=42656083-784d-4e7e-b032-2cb6433bec00&DisplayLang=en
Hotfix	MS05-021	Downloadable under: http://www.microsoft.com/downloads/details.aspx?FamilyID=35bce74a-e84a-4035-bf18-196368f032cc&DisplayLang=en
SHA-1 hash values for Exchange Server 2003 EE, SP1, and Hotfix MS05-21	Files contain SHA-1 values of the evaluated version only	Files containing SHA-1 hash values which can be used by customers to verify the integrity of TOE (for description how to use see Guidance Addendum [8], chapter 7.4]). The three Integrity Check Files can be directly downloaded from the Microsoft Exchange Server 2003 Common Criteria webpage. The general Exchange Server 2003 Common Criteria web page can be reached as follows: 1. enter: http://www.microsoft.com/exchange (Exchange Server main page) 2. go to: Product Information 3. go to: Certification
FCIV tool	2.05	The FCIV tool is used to verify the integrity of the TOE with the provided integrity check file.

Deliverables	Version	Comment
		It can be downloaded from: http://support.microsoft.com/default.aspx?scid=kb;en-us;841290 (for further information see [8], chapter 7.4)

Table 3: Identification of the TOE

3 Security Policy

The security policy of the TOE provides different aspects of security management by requiring administrator privileges for all server configuration and maintenance tasks and by defining multiple classes of user.

The TOE controls access of users to the types of Exchange Server 2003 data stores which are mailboxes and public folders.

Connection filtering is done by using Accept Lists and Deny Lists which may contain IP addresses, IP address ranges, or domains.

Message filtering is done by using a Sender Filtering List, and a Recipient Filtering List configurable by the administrator

Furthermore the TOE supports the restriction of distribution lists by security attributes connected to distribution lists.

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

4.1 Usage assumptions

The Security Target does not contain usage assumptions.

4.2 Environmental assumptions

All assumptions are assumptions about the environment of use and can be classified as physical aspects, personnel aspects, or connectivity aspects.

They are defined by the Security Target (refer to Security Target [5], chapter 3.1):

- The platform upon which the TOE resides (Windows Server 2003 operating system) provides methods to identify and authenticate users and to provide the TOE with corresponding user IDs and attributes (A.I&A).
- The platform upon which the TOE resides (Windows Server 2003) will be configured to restrict modification to TOE executables, the platform itself,

configuration files, databases (mailboxes and public folders) and cryptographic keys to only the authorized administrators (A.ACCESS_CONTROL).

- The platform upon which the TOE resides provides methods to protect communications between the TOE and remote trusted IT products in terms of authenticity and confidentiality. This includes an adequate key management for Internet protocols (A.COM_PROT).

- The TOE will be delivered, installed, configured and setup in accordance with documented delivery and installation/setup procedures. In the default installation procedure of the TOE IMAP4, POP3 and X.400 protocols are disabled and it is assumed that the administrator does not enable them after installation. The administrator has to ensure that connection/sender/recipient filtering functionality is enabled. The administrator has to ensure that quota functionality is enabled and that reasonable quotas have been configured with respect to the number of mailboxes and mail-enabled public folders and available disk space (A.INSTALL).
- There will be one or more competent administrator(s) assigned to manage the TOE and its platform and the security of the information both of them contain (A.MANAGE).
- The administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation (A.NO_EVIL_ADM).
- The TOE and its platform will be located within facilities providing controlled access to prevent unauthorized physical access (A.PHYS_PROTECT).
- The hardware/firmware that runs the operating system operates correctly and as the operating system expects (A.CORRECT_HW).

4.3 Clarification of scope

This TOE is explicitly intended for use cases and environments, where a low attack potential is present due to either the low value of the assets or additional protection measures in the environment. By itself, the TOE is not intended to provide appropriate protection when mid- or high-level protection of the assets is needed; in these cases it should be combined with additional environmental protection measures.

Furthermore, the evaluation does not cover threats that are related to functions of the operating system which are used by the TOE, i.e.: Identification and Authentication, Communications Security, TOE Data Protection.

Components that are disabled in the default configuration of Exchange, such as the IMAP4, POP3, and X.400 protocol, are out of scope of the evaluation, too.

5 Architectural Information

The TOE is an e-mail and collaboration server, which runs on servers that enable users to send and receive e-mail and other forms of interactive communication (such as sharing data via public message folders) through computer networks. It interoperates with different software client applications (like Microsoft Outlook 2003 and other e-mail client applications) and provides secure access to personal and shared data using different protocols. The supported protocols for client access include MAPI (RPC), SMTP, POP3, IMAP4, X.400, and HTTP-DAV, whereas in the evaluated default configuration of Exchange 2003 the components IMAP4, POP3, and X.400 protocol are disabled and therefore out of scope of the evaluation.

The TOE runs on the platform Windows Server 2003 operating system (exact denotation/version: Windows Server 2003 Enterprise Edition (English) (incl. IIS 6.0 and Active Directory), Version/Build RTM – 3790), which includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

Figure 1 below gives an overview of the TOE and its environment.

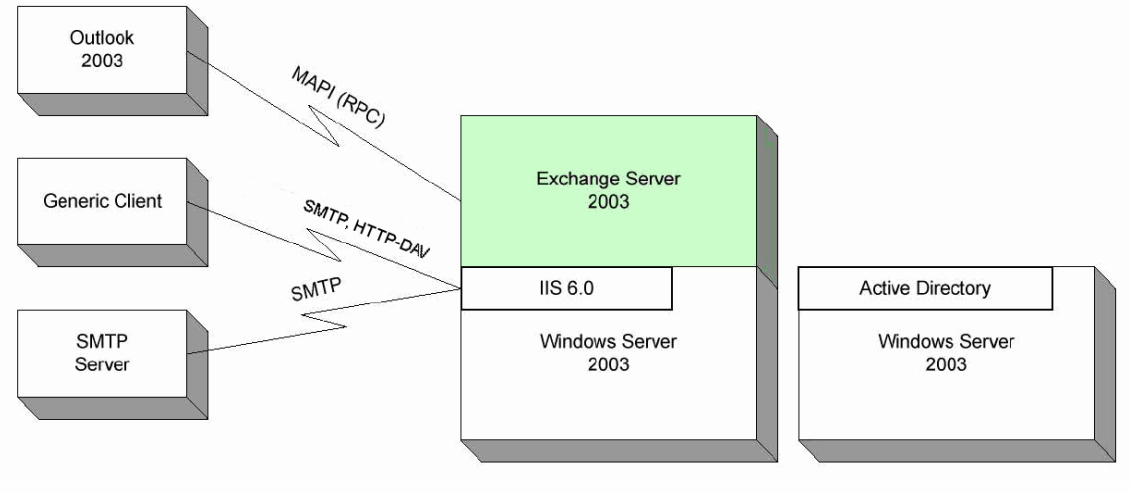

Figure 1: Exchange Server 2003 and its environment

The TOE supports different types of clients that can be used to establish a connection to the TOE. These clients are classified as:

- Generic Client (Internet Client): this could be any mail client that uses SMTP to connect to the TOE or a web browser that uses HTTP/HTTP-DAV to connect to the TOE.
- Outlook client: In contrast to the generic Clients, an Outlook client uses RPC to connect to the TOE.

In addition, the SMTP protocol can be used by an SMTP server to connect to the TOE. These clients or SMTP servers, that may establish a connection to the TOE, are outside the scope of the TOE and were not evaluated.

6 Documentation

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

[7] Guidance Documentation: Exchange Server 2003 Administration Guide and Exchange Server 2003 product help (part of the Exchange Server 2003 package); File properties - name: exadmin.chm, size: 957.988 Bytes; Date: 24.06.2003

[8] Guidance Addendum: Exchange Server 2003 Common Criteria Evaluation – Guidance Documentation / Installation, Generation, Startup / Flaw Remediation Guidance; Version: 1.13; Date: 17.08.2005

7 IT Product Testing

Developer Tests

Test Configuration

The TOE has been tested within a configuration that consists of a network of the following components (each component is realised on a separate machine):

- The TOE as the centre of the configuration,
- Active Directory
- Client A
- Client B.

All components were connected through a hub.

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 enforcing functions detailed in the developer’s functional specification. The tests cover all security functions defined in the ST [5].

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 actually have the effects as specified in the developer's functional specification.

Independent Evaluator Tests

Test Configuration

Exchange Server 2003 Enterprise Edition, Version 6.5.7226.0 (i.e. Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 and Exchange Server 2003 Service Pack 1 installed) with Hotfix MS05-021 (KB894549) installed on Windows Server 2003 with Service Pack 1.

The test configuration is similar to the developer's test configuration. Employed were standard PCs.

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 [5] 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 several miscellaneous tests.

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 penetration tests. Additionally, the TOE has been scanned with the vulnerability scanner Nessus and with the Internet Security Scanner (ISS) to identify possible vulnerabilities.

Test Results

The independent tests as well as the repeated developer tests confirm 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 are 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

The TOE is the Exchange Server 2003 Enterprise Edition (English), Version/Build 6.5.7226.0 (i.e. Exchange Server 2003 Enterprise Edition RTM 6.5.6944.0 with Exchange Server 2003 Service Pack 1) and Exchange hotfix MS05-021 (KB894549) installed, achieved by and detailed in the guidance documentation addendum [8] which is also part of the TOE.

The TOE is the Exchange Server 2003 in its default configuration.

Components that are disabled in the default configuration of Exchange, such as the IMAP4, POP3, and X.400 protocol, are out of scope of the evaluation.

The relevant Guidance Documentation is delivered together with the software on CD-ROM [7]. The Guidance Addendum [8] is also part of the evaluated version of the TOE. It is only available as a Word document via a secure channel on the vendors TOE-internet-homepage. The Service Pack and the Hotfix that are part of the TOE are delivered via the web only.

The TOE runs on the platform Windows Server 2003 operating system (exact denotation/version: Windows Server 2003 Enterprise Edition (English) (incl. IIS 6.0 and Active Directory), Version/Build RTM – 3790), which includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

The clients or SMTP servers that may establish a connection to the TOE are outside the scope of the TOE and were not evaluated.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 33]).

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS

Assurance classes and components		Verdict
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Systematic flaw remediation	ALC_FLR.3	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS

Assurance classes and components		Verdict
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 4: Verdicts for the assurance components

The evaluation has shown that:

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

The results of the evaluation are only applicable to the product Microsoft Exchange Server 2003 Enterprise Edition, Version/Build 6.5.7226.0 and Hotfix MS05-021 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [5] and the chapters 2, 4 and 8 of this report).

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

10 Comments/Recommendations

For secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [5] and the Security Target as a whole have to be taken into account.

The guidance documentation and the Guidance Addendum contain necessary infor-mation about the installation and usage of the TOE (including the service pack and the hotfix) and all security hints therein have to be considered. The user of the TOE has to be aware of the existence and purpose of the Guidance Addendum [8].

Therefore, the TOE's Internet product homepage has to provide information about the existence of the document and describe how to access the document. The reference has to be unambiguous and permanent.

A user/administrator has to follow the guidance in these documents.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [5] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

AGD	Guidance Documentation (according to the CC assurance class “ Guidance Documentation”)
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
HTTP	Hypertext Transfer Protocol
HTTP-DAV	Hypertext Transfer Protocol Distributed Authoring and Versioning
IMAP4	Interactive Mail Access Protocol Version 4
IIS	Internet Information Service
IT	Information Technology
MAPI	Message Application Programming Interface
PDA	Personal Digital Assistant
POP3	Post Office Protocol Version 3
PP	Protection Profile
RPC	Remote Procedure Call
RTM	Release to Manufacturing
SF	Security Function
SFP	Security Function Policy
SMTP	Simple Mail Transport Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

TSFI TSF Interface

TSP TOE Security Policy

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, Annotated with interpretations as of 2003-12-31, August 1999

[2] Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and general model, version 0.6, revision 11.01.1997, Part 2: Evaluation Methodology, CEM-99/045, version 1.0, Annotated with interpretations as of 2003-12-31, August 1999

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

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

[5] Exchange Server 2003 Common Criteria Evaluation – Security Target, Version: 1.9, Date: 21.06.2005, Microsoft Corporation

[6] Evaluation Technical Report, BSI-DSZ-CC-0284-2005, Version 1, Datum 2005-09-16, TÜV Informationstechnik GmbH (confidential document)

[7] Exchange Server 2003 Administration Guide and Exchange Server 2003 product help (part of the Exchange Server 2003 package); File properties - name: exadmin.chm, size: 957.988 Bytes; Date: 24.06.2003

[8] Exchange Server 2003 Common Criteria Evaluation – Guidance Documentation / Installation, Generation, Startup / Flaw Remediation Guidance; Version: 1.13; Date: 17.08.2005

C Excerpts from the Criteria

CC Part 1:

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

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 2.5)

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

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

Table 2.1: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

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

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

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

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

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

Table 6.1: Evaluation assurance level summary

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

"Objectives

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

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

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

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

"Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

"Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

"Objectives

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

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

"Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

"Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

"Objectives

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

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

"Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

"Objectives

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

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

"Application notes

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

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

This page is intentionally left blank.