Exchange Server 2003 Common Criteria Evaluation

Security Target

Exchange Server 2003 Team

Author: Michael Grimm

Status: Final
Version: 1.9
Revision: 1
Last Saved: 2005-06-21
File Name: MS_EX_ST_1.9.doc

Abstract

This document is the Security Target (ST) for Exchange Server 2003 Common Criteria Certification

Keywords

CC, ST, Common Criteria, Exchange, Security Target

Revision History

Date	Version	Author	Edit
07-Jul-04	1.1	Microsoft Exchange Team	Initial Creation
18-Aug-04	1.2	Microsoft Exchange Team	Revision of SFRs and TSFs
07-Sep-04	1.3	Microsoft Exchange Team	Revision after BSI kick-off meeting
06-Oct-04	1.4	Microsoft Exchange Team	Revision after BSI comments
12-Oct-04	1.5	Microsoft Exchange Team	Revision of TOE description
09-Nov-04	1.6	Microsoft Exchange Team	Revision after TÜViT comments
24-Jan-05	1.7	Microsoft Exchange Team	Revision after BSI/TÜViT comments
23-Feb-05	1.8	Microsoft Exchange Team	Minor correction of two SFRs
21-Jun-05	1.9	Microsoft Exchange Team	Hotfix added (TOE), assumption A.MANAGE extended, revision of SFRs and TSF

This page intentionally left blank

Table of Contents

List of Tables

Page

List of Figures

Page

1 ST Introduction

This chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (chapter 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, chapter 5.

1.1 ST Identification

This chapter provides information needed to identify and control this ST and its Target of Evaluation (TOE).

ST Title:	Exchange Server 2003 Common Criteria Evaluation Security Target
ST Version:	1.9
Revision Number:	1
Date:	2005-06-21
Author:	Microsoft Corporation
TOE Identification:	Microsoft Exchange Server 2003 Enterprise Edition (English)
TOE 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
TOE Platform:	Windows Server 2003 Enterprise Edition (English) RTM – 3790
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408) and all corresponding final interpretations
Evaluation Assurance Level:	EAL4 augmented by ALC_FLR.3
PP Conformance:	none
Keywords:	Message Collaboration Server, Mail Server, Exchange

1.2 ST Overview

The TOE is Exchange Server 2003 Enterprise Edition (English) in its default configuration (hereinafter called Exchange for simplicity), an e-mail and collaboration server that provides secure access to personal and shared data to variety of clients using various 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.

A summary of the TOE security functions can be found in chapter 2, TOE Description. A detailed description of the security functions can be found in chapter 6, TOE Summary Specification.

1.3 CC Conformance

The TOE is CC Part 2 conformant and CC Part 3 conformant at the level of assurance EAL4 augmented with assurance requirement ALC_FLR.3.

2 TOE Description

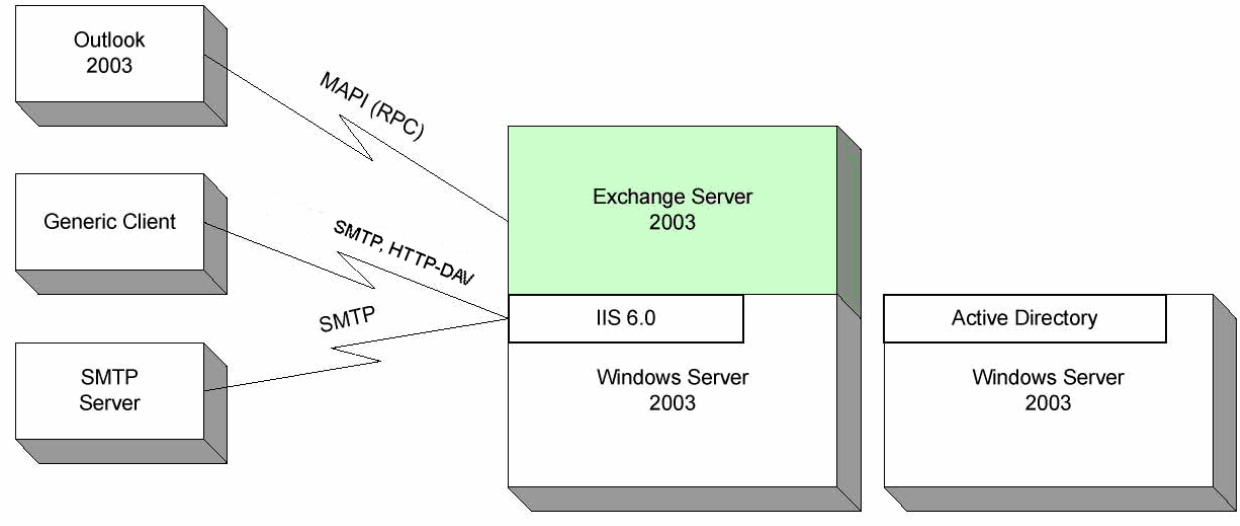
This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

Exchange Server 2003 is an e-mail and collaboration server that provides secure access to personal and shared data to variety of clients using various protocols including: MAPI (RPC), SMTP, POP3, IMAP4, X.400, and HTTP-DAV[1]. Exchange clients include personal computers running RPC-based applications like Outlook 2003, or Internet-based protocols like SMTP, IMAP4 and POP3. Exchange 2003 includes a HTTP-DAV interface for HTTP access to reading and writing to the Exchange message stores. Non-PC clients such as PDAs and smartphones can also use Exchange 2003 via HTTP-DAV. The platform for Exchange is Windows Server 2003 operating system, which includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

Figure 1 shows Exchange in this environment.

Figure 1 – Exchange and its environment



2.2 Physical Scope and Boundary of the TOE

The TOE consists of the following components:

[1] As the TOE is Exchange in its default configuration, IMAP4, POP3, and X.400 protocols are disabled and out of scope in the evaluation.

1. Admin component, which includes the following sub-components:
    a. Exchange System Manager (ESM), which is a manual administration tool (implemented as a snap-in of the operating system's Management Console, MMC[2]) that provides centralized administration of settings that apply to the entire Exchange organization, an administrative group (a collection machines with similar settings), or a specific Exchange server. For example, using ESM the Exchange Administrator can start and stop the protocol services on a machine and monitor message queues.
    b. Besides the ESM the TOE extends the domain user and computer administration of Windows Server 2003. The domain user and computer MMC snap-in is for example used to assign mailboxes to users or to modify mailbox quotas of Exchange users.
    c. Exchange System Attendant (SA) is a background service that generates offline address books for Outlook, free/busy calendaring information, creates e-mail addresses based on administrator-defined policies, and replicates directory-based administrative information to local data caches on the Exchange server.
    d. Exchange Administration Service. The Exchange Administration Service is a background service. Exchange Administration Service implements a collection of Windows Management Instrumentation (WMI) providers and is also used by the message tracking application within Exchange System Manager[3]. The Exchange Admin Service supplies information about the state of the Exchange server.
2. Store component, which is responsible for storing, retrieving, and regulating access to Exchange store items and folders. An Exchange store item could be an email message, contact, calendar item, or task. A folder can be a folder in a user's private mailbox, or a public folder. Access to mailboxes, folders within a mailbox, and public folders are regulated with access control lists (ACLs).
3. Protocol component, which enhances SMTP and HTTP-DAV protocol functionality in IIS by installing the corresponding protocol filters in the Internet Information Server (IIS) process of Windows Server 2003 operating system.
   The SMTP protocol sub-component of the TOE plugs into protocol filters and transport event sinks that are part of the core Windows Server 2003 operating system. Microsoft Windows Server 2003 includes SMTP and HTTP servers as part of IIS. These are the same, unmodified SMTP and HTTP servers that Microsoft Exchange Server uses. Exchange registers for SMTP or HTTP events (e.g. arrival of a new message), and an IIS event dispatcher notifies the registered Exchange code.
4. HTTP-DAV based applications Outlook Web Access (OWA), Outlook Mobile Access (OMA) and Exchange ActiveSync. These are applications for accessing Exchange data via its HTTP-DAV interface. OWA and OMA are sets of client-side and server-side scripts and applications which are rendered by the IIS web server. A client web browser accesses an HTTP-DAV based application via an HTTP connection and the web browser

[2] See glossary for more details about MMC and MMC snap-ins.

[3] See glossary for more information about WMI and WMI providers.

then uses HTTP-DAV requests to fetch mailbox data from the TOE.
HTTP-DAV based applications are not security enforcing, but the underlying HTTP-DAV interface is, and is examined in this evaluation.[4]

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

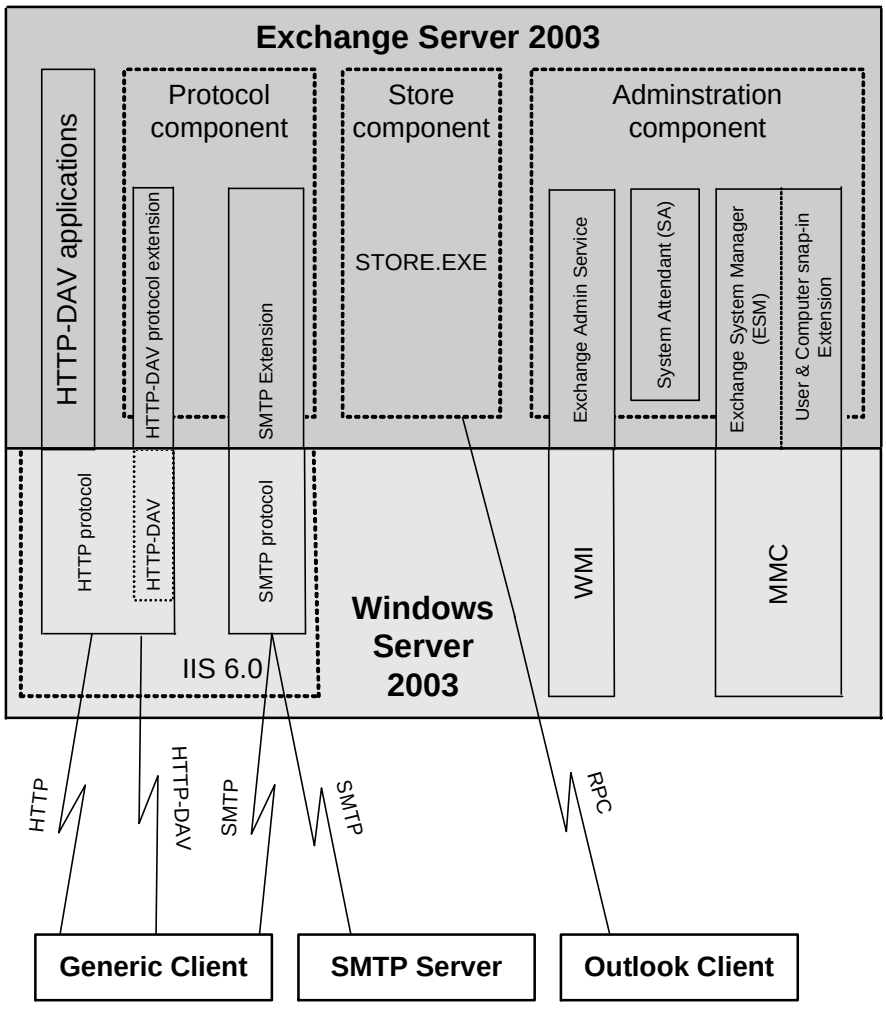
- Generic Client (also known as Internet Client):
  A client of this type could be any mail client that uses SMTP to connect to the TOE or a web browser that uses HTTP/HTTP-DAV to connect to the TOE.
- Outlook client:
  In contrast to the generic Clients, an Outlook client uses RPC to connect to the 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 will not be evaluated.

Figure 2 illustrates the physical scope of the TOE, its separation from the Windows Server 2003 operating system, and its connections to external IT entities.

[4] Separation of the HTTP-DAV based applications from the security enforcing components of the TOE will be discussed in FSP and/or HLD. Security enforcing HTTP-DAV interface will be evaluated and tested exhaustively.

Figure 2 – Physical scope and boundary of the TOE (Exchange Server 2003), its platform (Windows Server 2003), and external IT entities



Version information about the TOE and its platform is given in Table 1.

Table 1 – Evaluation Configuration

	Description	Version/Build
TOE	Exchange 2003 Enterprise Edition (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) and Exchange hotfix MS05-021 (KB894549) installed
Platform of the TOE	Windows Server 2003 Enterprise Edition (English) (incl. IIS 6.0 and Active Directory)	RTM – 3790

2.3 Logical Scope and Boundary of the TOE

The TOE logical boundary is defined by the following security functions provided by the TOE:

- Security Management (**SF.SM**) – provides administrative functionality for the TOE
- Access Control (**SF.AC**) – protects mailboxes and public folders from unauthorized access.
- Connection Filtering (**SF.CF**) – protects from unwanted spam or Unsolicited Commercial E-mail (UCE) by blocking messages from specified IP addresses or domains.
- Message Filtering (**SF.MF**) – filters SMTP messages based on the FROM: field of the message (Sender Filtering) or the RCPT TO: field of the message (Recipient Filtering).
- Distribution List Restriction (**SF.DLR**) – requires users of a distribution list to be successfully authenticated and to be authorized.
- Mailbox and public folder quota (**SF.QTA**) – allows Exchange Administrators to set quotas on the size of mailboxes and public folders.

The following features are included in the Exchange product, but outside the logical scope of the TOE:

- Handling of IMAP4, POP3 and X.400 protocols (disabled in the default configuration of Exchange)

The following security functionality of Windows Server 2003 (i.e. the TOE environment) is used by the TOE:

- **Identification and Authentication** – provided by the Active Directory component of Windows Server 2003. The TOE relies on Active Directory authenticating users when these want to access the TOE via RPC (MAPI), HTTP/HTTP-DAV or SMTP interfaces. After Windows Server 2003 performed identification and authentication it provides information about the corresponding user ID and attributes. On the basis of this information the TOE decides whether access is granted or denied.
- **Communications Security** – provided by Windows Server 2003. To ensure communication security, the TOE uses two security functionalities of Windows Server 2003: (1) The basic SMTP, HTTP and RPC protocols do not provide a confidential communication path as the data is transmitted in clear text. SMTP-TLS, HTTP/SSL and encrypted RPC are needed to provide confidential communications. Secure SMTP connections can be used to establish secured connections between SMTP servers during mail delivery. The protected RPC or HTTP connections are used to establish secured client connections. (2) In order to provide confidentiality for SMTP and HTTP communications security using SSL/TLS connection, Windows must manage the certificates used in these protocols.
- **TOE Data Protection** – provided by Windows Server 2003 discretionary access control. During common operation it is necessary to restrict the access to TOE items

such as binaries, configuration data, and user data (mailboxes and public folder items). This is essential to maintain the confidentiality of the stored objects that are managed by the TOE and to prevent the TOE from unauthorized changes. For each of these objects, the administrator can define who is allowed to access (e.g. to read or change the files) on the operating system level. The discretionary access control of Windows Server 2003 is needed to prevent the binaries and configuration files of the TOE itself as well as its stored data from unauthorized access even if a user has access to the system on operating system level.

3 TOE Security Environment

As a mail and collaboration server, Exchange may be used in many different environments. The assets to be protected (such as an employee's mailbox and messages included in there) therefore may be very different concerning their sensitivity, depending on the organization Exchange is used in. Therefore it is impossible to determine values of the information assets beforehand. As a consequence, the motivation of possible attackers could scale with the importance, sensitivity and value of the information assets, and therefore the attack potential could range from low one to high one.

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.

3.1 Assumptions

This chapter describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

The operational environment must be managed in accordance with the delivered guidance documentation. The following specific conditions are assumed to exist in an environment where this TOE is employed:

Table 2 - Assumptions

Assumption	Description
A.I&A	The platform[5] upon which the TOE resides provides methods to identify and authenticate users and to provide the TOE with corresponding user IDs and attributes. (When the user attempts to perform an operation, which is access-controlled by the TOE, such as opening a mailbox or public folder, he has to be authenticated first. When a user accesses Exchange via an Outlook client while not already being authenticated (e.g. via network logon), Outlook will have to ask for the user credentials and initiate the authentication procedure before the TOE resources can be accessed. When accessing Exchange via a web browser with an HTTP-DAV application like OWA, the web server running Exchange will ask for the user credentials and initiate authentication. When accessing Exchange via SMTP, methods for identification and authentication are provided as part of SMTP.

[5] Platform denotes to Windows Server 2003 operating system.

Assumption	Description
	In case of a successful authentication the TOE analyzes the provided user ID and attributes and allows or denies the access to an object depending on these 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. (This is in order to prevent unauthorized changes concerning the platform as well as the TOE and its configuration.)
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 as the basis for the protection of the communication.
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. The administrator(s) ensure that the platform the TOE is running on allows secure operation of the TOE. Once vulnerabilities of the platform are known, which are relevant for TOE operation, these have to be removed (e.g. by installing corresponding hotfixes) or protected by appropriate external security measures.
A.NO_EVIL_ADM	The administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.

Assumption	Description
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.

3.2 Threats

Table 3 identifies the threats to the TOE. The potential attackers of the TOE are considered to be users with public knowledge of how the TOE operates. However, as stated above, this TOE is explicitly intended for use cases and environments, where a low attack potential is present and therefore attackers are not considered to possess access to the resources necessary to perform attacks like cryptanalysis on the algorithms used or disassembling and reverse engineering the TOE. The attackers have only network access to the TOE, not physical access (see A.PHYS_PROTECT). Countering/mitigation of the threats are through the objectives identified in chapter 4, Security Objectives.

Table 3 - Threats to the TOE

Threat	Description
T.UNAUTH_DAC[6]	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)[7], 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[6]	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. For example: A user could use his account information to authenticate against Windows Server 2003 (the TOE relies on identification and authentication of the operating system). Once authenticated he could try to get unauthorized access to

[6] Exchange Server 2003 has two kinds of data stores: mailboxes – also known as a private store – that are specific to an individual mailbox-enabled user and public folders for shared folders and documents. Please find more details about the access control of the TOE in chapter 6.1.2 of this document.

[7] The access to public folders is usually restricted to one or more users or user groups. Public folders usually do not provide unrestricted access to the folder for all users (authorized as well as unauthorized users) since they are usually used by specific work groups in an organization.

Threat	Description
	mailboxes belonging to other users of the TOE.
T.UNAUTHUSE[6]	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. This scenario is similar to the scenario described in T.AUTH_DAC but now the authenticated user tries to get unauthorized access to a public folder instead of a private folder, although he is not a member of a group that is allowed to access the folder 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. The threat is an external entity that may send unsolicited messages to TOE users consuming TOE resources or delivering unwanted information to TOE users.
T.DL_MISUSE	An unauthenticated user or an authenticated but unauthorized user may send messages through a distribution list[8] consuming TOE resources delivering inappropriate email, such as UCE or improper employee use. A distribution list may be restricted in a way that only authenticated and authorized users shall be allowed to send messages to a distribution list. An attacker may send mail for such a distribution list although he is not allowed to deliver email to this distribution list.
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). The main purpose of the TOE is to deliver email. Therefore all incoming mail that is addressed to a valid user or mail-enabled public folder should be stored in the recipient's mailbox or in the corresponding public folder, respectively. An attacker could send a large amount of mail to the TOE, trying

[8] A distribution list may be either a statically defined group of users and/or groups in the Active Directory, or created dynamically based on a LDAP query.

Threat	Description
	to force an overflow of the mail-storage and/or public folder storage to disturb the availability of the mail services because of the lack of resources. Furthermore regular users that keep all of their received messages could also cause an overflow of the mail system. In the course of time the storage of all of their mail may result in mailboxes of exorbitant size. Both may also result in a lack of resources (e.g. lack of hard disk space).

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This chapter identifies the organizational security policies applicable to the TOE.

Policy	Description
	There are no organizational security policies in this ST.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

This chapter identifies and describes the security objectives of the TOE. The TOE accomplishes the security objectives defined in Table 4.

Table 4 - Security Objectives for the TOE

Objective	Description
O.DAC	The TOE shall prevent unauthorized access to objects maintained in the Exchange Store (i.e. mailboxes, public folders). Therefore the TOE shall provide discretionary access controls to private mailboxes and public folders so that only authorized users can read, modify or delete messages. (This implies that the user has to authenticate successfully before he can get access to the mail data. To authenticate a user the TOE relies on the identification and authentication functionality of Windows Server 2003 – see OE.I&A described in chapter 4.2).
O.CONBLK	To keep the level of spam as low as possible the TOE shall provide the ability to reject an SMTP connection based on the IP address of the remote SMTP sender using accept and deny lists configurable by the administrator.
O.RESTDIST	The TOE shall allow Exchange Administrators to restrict distribution lists[9] to only allow sending mail from authenticated and authorized users. Also, Exchange Administrators can specify which users can or cannot send to specific distribution lists. It should not be possible to bypass this restriction and to send mail unauthenticated to a distribution list by delivering mail to users.
O.FILTER_EMAIL	The TOE shall allow Exchange Administrators to eliminate unwanted or unsolicited mail (UCE or spam) by evaluating the sender and receiver information of an email (RCPT TO: and FROM: fields of the RFC821 payload envelope of a message).

[9] A distribution list may be either a statically defined group in the Active Directory, or created dynamically based on a LDAP query.

Objective	Description
O.QUOTA	The TOE shall allow Exchange Administrators to restrict the size of user mail boxes and public folders to avoid denial of service (here: resource overflow) attacks against the Exchange storage. If a user's mailbox reaches a size defined by the Exchange Administrator, the delivery of further mails will be stopped and the user informed about the actual mailbox size. In this case only one user is no longer able to receive further mail. Other users should not be affected and should be able to receive mail as usual. If a public folder reaches a size defined by the Exchange Administrator, no more posting (creation of new items) is possible for this folder.

4.2 Security Objectives for the Environment

The security objectives for the TOE Environment are defined in Table 5.

Table 5 - Security Objectives for the TOE Environment

Objective	Description
OE.I&A (IT)	The TOE environment has to provide methods to identify and authenticate users and to provide the TOE with corresponding user IDs and attributes. (User ID and attributes (e.g. group membership) provided by the operating system are used by the TOE to determine if the access to an object is granted or denied.)
OE.DAC (IT)	The TOE environment must provide discretionary access control (DAC) on the operating system level to protect TOE executables and TOE data (e.g. mailboxes, public folders and configuration data). The access control on operating system level is important to avoid unauthorized changes to TOE executables, the platform itself, configuration data, mailboxes and public folders, and cryptographic keys even if a user not being the Exchange Administrator could authenticate against the operating system.

Objective	Description
OE.COM_PROT (IT)	The TOE environment must provide methods to protect communication of the TOE and remote trusted IT products in terms of authenticity and confidentiality. This includes an adequate key management for Internet protocols as the basis for the protection of the communication.
OE.PLATFORM_SUPPORT (Non-IT)[10]	The TOE environment must provide reliable platform functions including: correct hardware operation and functionality and correct firmware operation and functionality. This is necessary to ensure a stable operation of Windows 2003 Server and the TOE and to avoid any side effects due to an improper hardware/firmware platform.
OE.PHYSICAL (Non-IT)	Those responsible for the TOE must ensure that those parts of the TOE and its platform critical to security policy are protected from any physical attack.
OE.INSTALL (Non-IT)	Those responsible for the TOE must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which is consistent with IT security. After installation (in the default configuration) the administrator shall not enable IMAP4, POP3 and X.400 support, as otherwise the TOE is no longer running in the evaluated configuration. After installation (in the default configuration) the administrator shall enable connection/sender/recipient filtering functionality. After installation (in the default configuration) the administrator shall enable quota functionality and assign reasonable size limits with respect to the number of mailboxes and mail-enabled public folders and available disk space. The administrator(s) shall ensure that the platform the TOE is running on allows secure operation of the TOE. Once vulnerabilities of the platform are known, which are relevant for TOE operation, these have to be removed (e.g. by installing corresponding hotfixes) or protected by appropriate external security measures.

[10] OE.PLATFORM_SUPPORT is an objective to the Non-IT environment of the TOE, because the reliable platform has to be provided by organizational means (i.e. by the organization operating the TOE) and OE.PLATFORM_SUPPORT cannot be fulfilled by SFRs as defined by CC part 2.

5 IT Security Requirements

This chapter defines the IT security requirements that shall be satisfied by the TOE or its environment:

The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subchapters.

5.1 TOE Security Functional Requirements

The TOE satisfies the SFRs delineated in Table 6. The rest of this chapter contains a description of each component and any related dependencies.

Table 6 - TOE Security Functional Requirements

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	
FRU_RSA.1.a	Maximum quotas
FRU_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

5.1.1 Class FDP: User Data Protection

FDP_ACC.1.a Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1.a The TSF shall enforce the [discretionary access control policy] on [

subjects – processes acting on behalf of users

objects – mailbox and public folder items and (sub)folders

mailbox operations – List folder; Create subfolder, Create item, Read item, Edit item, Delete item, Modify folder permissions

public folder operations – List Folder, Create top level folder, Create subfolder, Create item, Read item, Edit item, Delete item, Modify folder permissions].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1.a Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1.a The TSF shall enforce the [discretionary access control policy] to **mailbox and public folder** objects based on [

subject attribute – security ID of user or group

mailbox object attributes – Folder visible ACL, Create subfolders ACL, Folder Owner ACL, Create items ACL, Read items ACL, Edit items ACL, Delete items ACL

public folder object attributes – Folder visible ACL, Create top-level folders ACL; Create subfolders ACL, Folder Owner ACL, Create items ACL, Read items ACL, Edit items ACL, Delete items ACL].

FDP_ACF.1.2.a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

The operation is allowed,
if the operation is explicitly allowed and not explicitly denied by a security ID entry in the objects corresponding ACL; operations and corresponding ACLs are:

List folder – Folder visible ACL

Create top level folder – Create top level folder ACL

Create subfolder – Create subfolder ACL

Modify folder permissions – Folder Owner ACL

Create item – Create item ACL

Read item – Read item ACL

Edit item – Edit item ACL

Delete item – Delete item ACL].

FDP_ACF.1.3.a The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4.a The TSF shall explicitly deny access of subjects to objects based on the **following additional rules**: [none].

Dependencies: FDP_ACC1. Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACC.1.b Subset access control

Hierarchical to: No other components

FDP_ACC.1.1.b The TSF shall enforce the [distribution list restriction policy] on [

subjects – users sending e-mail

objects – distribution lists

operation – use, i.e. send messages to recipients in a distribution list].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1.b Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1.b The TSF shall enforce the [distribution list restriction policy] to **distribution list** objects based on [

subject attribute – sender ID (this is security ID of user or group if restricted access flag is set or FROM: field of the RFC821 payload envelope if the restricted access flag is cleared)

object attributes – restricted access flag, Access ACL].

FDP_ACF.1.2.b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

The operation is allowed, if

1) a) the restricted access flag is cleared
   or
   b) the restricted access flag is set and at the same time the subject
      is authenticated (i.e. the corresponding security ID is available),

and

2) a) no Access ACL is configured
   or
   b) the Access ACL is configured to contain only explicitly allowed sender IDs and the sender ID the accessing subject is listed in

the Access ACL

or

c) the Access ACL is configured to contain only explicitly denied sender IDs, and the sender ID of the accessing subject is not listed in the Access ACL].

FDP_ACF.1.3.b The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4.b The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [filtering policy] on [

subjects – external[11] SMTP server, the Exchange SMTP server

information – message

operations – message delivery].

Dependencies: FDP_IFF.1 Security attribute based access control

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [filtering policy] based on the following types of subject and information security attributes: [

subject attributes – IP address or domain of the external SMTP server, Accept Lists and Deny Lists of the Exchange SMTP server, security ID of user or group

information attributes – FROM: field of the RFC821 payload envelope, RCPT TO: field of the RFC821 payload envelope, Sender Filtering list, and Recipient Filtering list].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

The information flow is permitted, if

1) the IP address or domain of the external SMTP server is not on a Deny List

or

the IP address or domain of the external SMTP server is listed on

[11] An SMTP server outside the Exchange organization

a Deny List, but the IP address or domain of the external SMTP server is listed on an Accept List,

and

2) a) the sender listed in the FROM: field of the RFC821 message envelope is not on the Sender Filtering List,

and

b) the sending user is authenticated (i.e. a corresponding security ID

is available)

or

the recipient listed in the RCPT TO: field of the RFC821 message envelope is not on the Recipient Filtering List].

FDP_IFF.1.3 The TSF shall enforce [denial of information flow if the FROM: field of the RFC821 message envelope is blank].

FDP_IFF.1.4 The TSF shall provide the following **additional SFP capabilities:** [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules [none].

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

Application Note: The Accept and Deny Lists are either static lists maintained by the Exchange Administrator or are retrieved from an external DNS server (a so-called Block List Service provider) as configured by the Exchange Administrator.

5.1.2 Class FRU: Resource Utilization

FRU_RSA.1.a Maximum quotas

Hierarchical to: No other components

FRU_RSA.1.1.a The TSF shall enforce maximum quotas on the following resources: [mailbox size] that **an** *individual user* can use *simultaneously*.

Dependencies: No dependencies

FRU_RSA.1.b Maximum quotas

Hierarchical to: No other components

FRU_RSA.1.1.b The TSF shall enforce maximum quotas on the following resources: [public folder size] that *subjects* can use *simultaneously*.

Dependencies: No dependencies

5.1.3 Class FMT: Security Management

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

a) Management of security attributes for the discretionary access control according to FMT_MSA.1.a

b) Management of security attributes for the distribution list restriction according to FMT_MSA.1.b

c) Management of security attributes for the message and connection filtering according to FMT_MSA.1.c and FDP_IFF.1

d) Management of maximum values for quotas on mailbox and public folder sizes according to FRU_RSA.1, restricted to the Exchange Administrator

e) Disabling/enabling of enforcement of maximum quotas on mailbox and public folder sizes according to FMT_MOF.1

f) Disabling/enabling of filtering of messages with blank FROM: field according to FMT_MOF.1]

g) Disabling/enabling of connection/sender/recipient filtering according to FMT_MOF.1].

Dependencies: No Dependencies

FMT_SMR.1.a Security roles

Hierarchical to: No other components.

FMT_SMR.1.1.a The TSF shall maintain the role~~s~~ [Folder Owner].

FMT_SMR.1.2.a The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_MSA.1.a Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1.a The TSF shall enforce the [discretionary access control policy] to restrict the ability to *query and modify* the security attributes [as defined below] to [the Exchange Administrator and the Folder Owner].

Attribute	Exchange Administrator	Folder Owner
Create top level folders ACL	query and modify	none (N/A)

Attribute	Exchange Administrator	Folder Owner
(for public folders only)		
Create subfolders ACL	query and modify	query and modify
Folder Owner ACL	query and modify	query and modify
Folder visible ACL	query and modify	query and modify
Create items ACL	query and modify	query and modify
Read items ACL	query and modify	query and modify
Edit items ACL	query and modify	query and modify
Delete items ACL	query and modify	query and modify

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3.a Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1.a The TSF shall enforce the [discretionary access control policy] to provide [the following] default values for security attributes that are used to enforce the SFP.
for *mailboxes* default ACLs allow full access for the corresponding Folder Owner, and deny access for other users
for *public folders* default ACLs allow full access for the corresponding Folder Owner, allow to read and create items and subfolders for other users, and deny creation of top level folders for other users

FMT_MSA.3.2.a The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.b Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1.b The TSF shall enforce the [distribution list restriction policy] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2.b The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

Application Note: Here permissive means that there are no restrictions for distribution lists by default.

FMT_MSA.3.c Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1.c The TSF shall enforce the [filtering policy] to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2.c The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

Application Note: Here permissive means that Accept Lists, Deny Lists, Sender Filtering List and Recipient Filtering List are not configured by default.

5.2 TOE Security Assurance Requirements

Table 7 identifies the security assurance components drawn from CC Part 3. It is evaluation assurance level EAL4 augmented by ALC_FLR.3. The SARs are not iterated or refined from Part 3.

Table 7 – TOE Security Assurance Requirements

SAR ID	SAR name	Dependencies
ACM_AUT.1	Partial CM automation	ACM_CAP.3
ACM_CAP.4	Generation support and acceptance procedures	ACM_SCP.1, ALC_DVS.1
ACM_SCP.2	Problem tracking CM coverage	ACM_CAP.3
ADO_DEL.2	Detection of modification	ACM_CAP.3
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.2	Fully defined external interfaces	ADV_RCR.1
ADV_HLD.2	Security enforcing high-level design	ADV_FSP.1, ADV_RCR.1
ADV_IMP.1	Subset of the implementation of the TSF	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_LLD.1	Descriptive low-level design	ADV_HLD.2, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None

SAR ID	SAR name	Dependencies
ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ALC_DVS.1	Identification of security measures	None
ALC_FLR.3	Systematic flaw remediation procedures	None
ALC_LCD.1	Developer defined life-cycle model	None
ALC_TAT.1	Well-defined development tools	ADV_IMP.1
ATE_COV.2	Analysis of coverage	ADV_FSP.1, ADV_FUN.1
ATE_DPT.1	Testing: high-level design	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing – sample	ADV_FSP.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.2	Validation of analysis	ADV_IGS.1, ADV_FSP.1, AGD_USR.1
AVA_SOF.1[12]	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.2	Independent vulnerability analysis	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_USR.1

[12] As the TOE has got no SOF-rateable security functions the vendor will not provide a SOF analysis and SOF evaluation will be limited to verification that there are really no permutational or probabilistic mechanisms in the TSF.

5.3 Security Requirements for the IT Environment

The environment satisfies the SFRs delineated in Table 8. The rest of this chapter contains a description of each component. The environment also has to fulfill all dependencies resulting from these requirements, but these will not be traced in this security target.

Table 8 - Security Requirements for the IT Environment

Class FDP: User Data Protection	
FDP_ACC.1.c	Subset access control
FDP_ACF.1.c	Security attribute based access control
Class FIA: Identification and authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_ATD.1	User attribute definition
Class FTP: Trusted path/channels	
FTP_TRP.1	Trusted path
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1.b	Management of security attributes
FMT_MSA.1.c	Management of security attributes
FMT_SMR.1.b	Security roles

5.3.1 Class FDP: User Data Protection

FDP_ACC.1.c Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1.c The **IT environment** shall enforce the [Windows discretionary access control policy] on [

subjects – processes acting on behalf of users

objects – NTFS files and/or NTFS directories (i.e. TOE executables, configuration files, message stores that store user mailboxes and public folders) and registry and Active Directory objects

operations – all operations among subjects and objects covered by Windows discretionary access control policy].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1.c Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1.c	The **IT environment** shall enforce the [Windows discretionary access control policy] to **NTFS files and/or NTFS directories (i.e. TOE executables, configuration files, message stores that store user mailboxes and public folders) and registry and Active Directory** objects based on [*subject attribute* – security ID of user or group *object attributes* – access control list].
FDP_ACF.1.2.c	The **IT environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [If the operation is explicitly allowed and not explicitly denied by an entry in the access list for the accessing subject, the accessing subject is able to perform the specified operation].
FDP_ACF.1.3.c	The **IT environment** shall explicitly authorize access of subjects to objects based on the following additional rules: [The operation is allowed, if the subject's security ID belongs to an authorized subject. The owner is always allowed to change permissions. The system administrator is always allowed take ownership.]
FDP_ACF.1.4.c	The **IT environment** shall explicitly deny access of subjects to objects based on the **following additional rules**: [none].
Dependencies:	FDP_ACC1. Subset access control FMT_MSA.3 Static attribute initialization

5.3.2 Class FIA: Identification and authentication

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication.
FIA_UAU.2.1	The **IT environment** shall require each user to be successfully authenticated before allowing any TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of Identification
Application Note:	To authenticate a user, the TOE passes the provided user credentials to the operating system, which authenticates the user against the Active Directory. The operating system then provides the result of the authentication procedure (authenticated or unauthenticated) to the TOE.

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The **IT environment** shall require each user to identify itself before allowing any TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Application Note:	To identify a user, the TOE passes the provided user credentials to the operating system, which identifies the user against the Active Directory. The operating system then provides the result of the identification procedure (identified or unidentified) to the TOE.

FIA_ATD.1 User attribute definition

Hierarchical to:	No other components
FIA_ATD.1.1	The **IT environment** shall maintain the following list of security attributes belonging to individual users: [security ID (user's identity) Group Memberships Mailbox Authentication Data Private Keys, and Privileges].
Dependencies:	No dependencies

5.3.3 Class FMT: Security Management

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to:	No other components
FMT_MOF.1.1	The **IT environment** shall restrict the ability to *disable* **and** *enable* the functions [a) Enforcement of maximum quotas on mailbox sizes and public folders according to FRU_RSA.1.a/b b) Filtering of messages with blank FROM: field according to FDP_IFF.1.3 c) Connection/sender/recipient filtering according to FDP_IFF.1] to [the Exchange Administrator].
Dependencies:	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of management functions

FMT_MSA.1.b Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1.b	The **IT environment** shall enforce the [distribution list restriction policy] to restrict the ability to *query and modify* the security attributes [Restricted access flag, Access ACL] to [the Exchange Administrator].
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.1.c Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1.c	The **IT environment** shall enforce the [filtering policy] to restrict the ability to *query and modify* the security attributes [Accept Lists, Deny Lists, Sender Filtering List and Recipient Filtering List] to [the Exchange Administrator].
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_SMR.1.b Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1.b	The **IT environment** shall maintain the role~~s~~ [Exchange Administrator].
FMT_SMR.1.2.b	The **IT environment** shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.3.4 Class FTP: Trusted path/channels

FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
FTP_TRP.1.1	The **IT environment** shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2	The **IT environment** shall permit *remote users* to initiate communication via the trusted path.
FTP_TRP.1.3	The **IT environment** shall require the use of the trusted path for [communication protection for SMTP, HTTP/HTTP-DAV and RPC connections].
Dependencies:	No dependencies
Application note:	TLS secured SMTP connections can be used to establish secured connections between SMTP servers during the mail delivery process. The RC4 protected RPC or SSL protected HTTP/HTTP-DAV connections are used to establish secured client connections.

5.4 Explicitly Stated Requirements for the TOE

This ST contains no explicitly stated requirements for the TOE.

5.5 Minimum Strength of Function (SOF) for the TOE

CC part 1, chapter C.2.6 a) b) and CC part 3, ASE_REQ.1.9C require a statement about the minimum strength level for the TOE security functions realized by probabilistic or permutational mechanisms. In this TOE there are no security functions realized by probabilistic or permutational mechanisms as all TSF are based on deterministic mechanisms:

- Security Management (**SF.SM**) – provides functionality for setting security parameters.
- Access Control (**SF.AC**) – grants/denies access based on comparison of object ACLs and user IDs.
- Connection Filtering (**SF.CF**) – filters connections by comparing domain names or IP addresses with configured lists.
- Message Filtering (**SF.MF**) – filters messages by comparing FROM: and RCPT TO: field of the message with configured lists.
- Distribution List Restriction (**SF.DLR**) – grants/denies access based on checking authentication status and authorization of a user.
- Mailbox and public folder quota (**SF.QTA**) – enforces quotas by comparing actual mailbox or public folder size with a configured value.

Accordingly there is not an SOF-claim for any SFR of the TOE in this ST.

6 TOE Summary Specification

This chapter presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation. The following table traces each IT security function to TOE security functional requirements.

6.1 TOE Security Functions

This chapter presents the security functions performed by the TOE to satisfy the identified SFRs in chapter 5.1.1. Traceability to SFRs is also provided. As stated in chapter 5.5 above, there are no security functions based on permutational or probabilistic mechanisms and therefore there are no SOF-claims.

6.1.1 Security Management (SF.SM)

Exchange Server 2003 provides for security management by (1) requiring administrator privileges for all server configuration and maintenance tasks and (2) defining multiple classes of user.

Exchange server management data and mail recipient data is stored in the Active Directory and access to read and modify those objects and attributes are controlled through AD-maintained access control lists.

The different types of users are domain users that have Exchange mailboxes, and Exchange Administrators responsible for running the Exchange servers.

Since Exchange 2003 is a directory-enabled application, an IT administrator can choose to delegate administrative tasks for specific servers and specific jobs to IT staff that have fewer privileges using role-based management. Recipient management tasks like creating mailboxes and setting storage quotas can also be delegated to administrators that have relatively few permissions.

Manual administration of the Exchange server and the topology is done through the Exchange System Manager tool. Managing mailbox recipients and distribution lists can be done either through the additional Exchange property pages or, when creating a new user or group, the Windows New User Wizard from the Active Directory Users and Computers management application.

SF.SM will provide in particular the following management functionality:

- Management of security attributes used in SF.AC, SF.DLR, SF.CF, SF.MF and SF.QTA; concerning SF.AC management capabilities for Exchange Administrator and Folder Owner are as follows:

Security Attribute of SF.AC	**Exchange Administrator**	**Folder Owner**
Create top level folders ACL (for public folders only)	query and modify	none (N/A)
Create subfolders ACL	query and modify	query and modify
Folder Owner ACL	query and modify	query and modify

Security Attribute of SF.AC	Exchange Administrator	Folder Owner
Folder visible ACL	query and modify	query and modify
Create items ACL	query and modify	query and modify
Read items ACL	query and modify	query and modify
Edit items ACL	query and modify	query and modify
Delete items ACL	query and modify	query and modify

- Disabling/enabling of SF.QTA, disabling/enabling of SF.CF, disabling/enabling of SF.MF and disabling/enabling of filtering of messages with blank FROM: field (i.e. a part of SF.MF)
- Creation/deletion of distribution lists used in SF.DLR; for new distribution lists restricted access flag is not set and Access ACL is empty

After installation of the TOE Accept and Deny Lists used for SF.CF and Sender and Recipient Filtering Lists used for SF.MF are empty.

Functional Requirements Satisfied: FMT_MSA.1.a, FMT_MSA.3.b/c, FMT_SMF.1, FMT_SMR.1.a

Note:

1. The administrator has to enable SF.QTA, SF.CF and SF.MF according to A.INSTALL.

2. Remark about default values for security attributes: default security attributes applied to newly created mailboxes or top level public folders are hardcoded within Exchange and cannot be changed. There are no default security attributes for subfolders, as during creation of a subfolder this one will inherit the security attributes of its corresponding parent folder.

6.1.2 Access Control (SF.AC)

SF.AC controls access of users to the two types of Exchange Server 2003 data stores: mailboxes – also known as a private store – that are specific to an individual mailbox-enabled user and public folders for shared folders and documents.

SF.AC utilizes access control lists (ACLs), implemented as NT security descriptors, on public folders and mailboxes (private folders) using Microsoft Windows permissions to control access along with permissions that are specific to Exchange. However, when communicating with MAPI-based client applications, such as Microsoft Outlook, Exchange 2003 converts the permissions to MAPI permissions when displaying them to the user. If the user modifies the permissions, Exchange converts them back to Windows permissions to save them.

Mailbox access: By default, the owner of the mailbox can read, write, or create new items or folders in the mailbox – other users have no access. The mailbox owner can grant permissions to either the entire mailbox or folders within a mailbox or messages within a folder to other users, including permissions to not only open the mailbox but to both send and receive mail as if they were the mailbox owner. SF.AC uses the following set of ACLs for controlling operations to mailboxes:

- Create items ACL (for control of create item operation)

- Read items ACL (for control of read item operation)
- Create subfolders ACL (for control of create subfolder operation)
- Folder Owner ACL (for control of modify folder permissions operation)
- Folder visible ACL (for control of list folder operation)
- Edit items ACL (for control of edit item operation)
- Delete items ACL (for control of delete item operation)

Public folder access: By default authenticated domain users have a restricted set of permissions on public folders: they can read and create items and subfolders but can not create new top level public folders – the Folder Owner has full access. The Folder Owner can grant permissions to other users. SF.AC uses the following set of ACLs for controlling access to public folders:

- Create top level folders ACL (for control of create top level folder operation)
- Create items ACL (for control of create item operation)
- Read items ACL (for control of read item operation)
- Create subfolders ACL (for control of create subfolder operation)
- Folder Owner ACL (for control of modify folder permissions operation)
- Folder visible ACL (for control of list folder operation)
- Edit items ACL (for control of edit item operation)
- Delete items ACL (for control of delete item operation)

SF.AC allows access to a mailbox or public folder object if the requested operation is explicitly allowed and not explicitly denied by an entry in the corresponding ACL.

Functional Requirements Satisfied: FDP_ACC.1.a, FDP_ACF.1.a, FMT_MSA.3.a, FMT_SMR.1.a

6.1.3 Connection Filtering (SF.CF)

SF.CF will reject SMTP connections based on domain or IP address of the connecting external SMTP server[13].

To do so, SF.CF uses Accept Lists and Deny Lists, which may contain IP addresses, IP address ranges, or domains.

If an SMTP connection is established, SF.CF performs in the following order, according to the IP address of the external SMTP server:

1. If the IP address is specified in an Accept List, SF.CF will allow the connection, regardless of any Deny List settings.
2. If the IP address is specified in a Deny List, SF.CF will block the connection.

[13] An external SMTP server is an SMTP server outside the Exchange organization.

The Accept and Deny Lists are either static lists maintained by the Exchange Administrator or are retrieved from a Block List Service provider as configured by the Exchange Administrator.

SF.CF can be enabled/disabled by the Exchange Administrator (via SF.SM).

Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1

6.1.4 Message filtering (SF.MF)

SF.MF will reject messages based on the FROM: and RCPT TO: SMTP commands and the security ID of the sending user, by using a Sender Filtering List and a Recipient Filtering List configurable by the administrator (via SF.SM).

If the sender given in the FROM: field is specified in the Sender Filtering list, SF.MF will reject the message.

If a recipient given in the RCPT TO: field is specified in the Recipient Filtering list and the sending user is not authenticated (i.e. no corresponding security ID is available), SF.MF will reject delivery of the message to this recipient.

Optionally SF.MF will also reject any message with a blank FROM: field (this is configurable by Exchange Administrator via SF.SM).

SF.MF can be enabled/disabled by the Exchange Administrator (via SF.SM).

Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1

6.1.5 Distribution List Restriction (SF.DLR)

SF.DLR restricts usage of distribution lists by three security attributes connected to distribution lists: restricted access flag, Access ACL and sender ID (the latter is the security ID of user or group if restricted access flag is set or the FROM: field of the RFC821 payload envelope if the restricted access flag is cleared).

SF.DLR will block a message sent to a distribution list, if

1. the restricted access flag is set, but the sending user is not authenticated (i.e. no corresponding security ID is available),

or

2. the Access ACL is configured to contain only explicitly allowed senders, but the sender is not listed in the Access ACL,

or

3. the Access ACL is configured to contain only explicitly denied senders, and the sender is listed in the Access ACL.

Functional Requirements Satisfied: FDP_ACC.1.b, FDP_ACF.1.b

6.1.6 Mailbox and public folder quota (SF.QTA)

SF.QTA allows the Exchange Administrator to set three levels of quotas for size restrictions on a mailbox. When a mailbox reaches the *warning quota*, SF.QTA sends a message notifying the owner that they are nearing their quota. When the mailbox reaches the *send quota*, SF.QTA will refuse to accept messages sent by the mailbox owner. When the mailbox reaches the *send-and-receive quota*, SF.QTA will refuse to accept new messages sent to the mailbox owner in addition to messages sent by the mailbox owner.

SF.QTA allows the Exchange Administrator to set quotas for size restrictions on a public folder. When a public folder reaches this quota, SF.QTA prevents creation of new items in this folder.

SF.QTA can be enabled/disabled by the Exchange Administrator (via SF.SM).

Functional Requirements Satisfied: FRU_RSA.1.a/b

6.2 Assurance Measures

For the evaluation of the TOE the assurance requirements according to CC EAL4 augmented with ALC_FLR.3 apply. This chapter identifies the assurance measures that are or will be applied by Microsoft in the course of the evaluation to satisfy the CC EAL4 augmented assurance requirements. The corresponding assurance measures are listed in Table 9 below (N.B. Some of the documentation listed therein is not prepared yet, therefore currently corresponding document titles and versions are not available).

Table 9 - Assurance Measures

SAR(s)	Assurance Measure(s)
ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	Usage of a CM system, Provision of CM system documentation
ADO_DEL.2	Application of secure delivery procedures, Provision of delivery documentation
ADO_IGS.1	Provision of installation, generation and startup documentation (either as part of administrator guidance documentation or as a separate document)
ADV_FSP.2	Provision of functional specification documentation
ADV_HLD.2	Provision of high-level design documentation
ADV_IMP.1	Provision of a subset of the implementation of the TOE
ADV_LLD.1	Provision of low-level design documentation
ADV_RCR.1	Provision of representation of correspondence documentation
ADV_SPM.1	Provision of an informal security policy model documentation
AGD_ADM.1 AGD_USR.1	Provision of user/administrator guidance documentation
ALC_DVS.1	Application of development security measures, Provision of development security documentation

SAR(s)	Assurance Measure(s)
ALC_FLR.3	Application of flaw remediation security measures, Provision of flaw remediation documentation
ALC_LCD.1	Provision of life-cycle model documentation
ALC_TAT.1	Usage of well-defined development tools, Provision of tool and techniques documentation
ATE_COV.2 ATE_DPT.1 ATE_FUN.1	Performance of testing of the TSF, Provision of test documentation
ATE_IND.2	Provision of the TOE and its platform, Provision of test tools, scripts, etc., Support of the evaluator to prepare/perform independent evaluator tests
AVA_MSU.2	Performance of a misuse analysis, Provision of misuse analysis documentation, Support of the evaluator to prepare/perform penetration testing
AVA_SOF.1	(The vendor will not provide an SOF analysis for this TOE, as no security function is realized by probabilistic or permutational mechanisms.)
AVA_VLA.2	Performance of a vulnerability analysis, Provision of security analysis documentation

7 Protection Profile (PP) Claims

This TOE does not claim conformance to any PP.

8 Rationale

This chapter demonstrates the completeness and consistency of this ST by providing justification for the following:

Traceability The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

- security objectives to threats encountered
- environmental objectives to assumptions met
- SFRs to objectives met

Assurance Level A justification is provided for selecting an EAL4 level of assurance for this ST.

SOF A rationale is provided why the SOF claim is not part of this ST.

Dependencies A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This chapter demonstrates that all security objectives for the TOE and its environment are traced back to aspects of the identified threats to be countered and/or aspects of the defined assumptions. Furthermore this chapter demonstrates that all threats and assumptions are covered by the security objectives of the TOE and its environment.

Table 10 - Security Objectives Rationale for the TOE

Objective	Threat(s)	Rationale
O.DAC	T.UNAUTH_DAC, T.AUTH_DAC, T.UNAUTHUSE	• O.DAC (discretionary access control concerning mailboxes and public folders) directly traces back to the threats T.UNAUTH_DAC, T.AUTH_DAC, T.UNAUTHUSE about unauthorized access to mailboxes and public folders. • T.UNAUTH_DAC, T.AUTH_DAC, T.UNAUTHUSE deal with adversaries trying to access information contained in mailboxes or public folders for which they are not authorized. O.DAC counters these threats by providing discretionary access on these objects.
O.CONBLK	T.SPAM	• O.CONBLK (blocking of SMTP connections from IP numbers known to be origin of UCE) directly traces back to

Objective	Threat(s)	Rationale
		T.SPAM. • Blocking connections from known SMTP hosts helps reduce the amount of UCE because the TOE is able to filter SMTP connections. Therefore T.SPAM is partly countered by O.CONBLK (the other aspect of T.SPAM about known senders of UCE is countered by O.FILTER_EMAIL, see below).
O.RESTDIST	T.DL_MISUSE	• O.RESTDIST (access control for distribution lists) directly traces back to T.DL_MISUSE. • T.DL_MISUSE defines misuse of distribution lists as a threat. O.RESTDIST counters this threat by allowing the Exchange administrator to restrict the use of distribution lists to only those users that have been authenticated and – optionally – which are explicitly authorized to use a distribution list.
O.FILTER_EMAIL	T.SPAM	• O.FILTER_EMAIL (sender/recipient filtering) directly traces back to T.SPAM. • Blocking messages with known UCE sender addresses helps reduce the amount of UCE because the TOE is able to filter the messages. Therefore T.SPAM is partly countered by O.FILTER_EMAIL (the other aspect of T.SPAM about known IP addresses of UCE origin is countered by O.CONBLK, see above).
O.QUOTA	T.OVERFLOW	• O.QUOTA (limitation of mailbox and public folder sizes) directly traces back to T.OVERFLOW. • T.OVERFLOW is countered by O.QUOTA as the Exchange administrator can limit the size of mailboxes and public folders. Doing so, O.QUOTA limits the amount of resources necessary to support the mailbox and public folder, respectively.

Table 11 - Security Objectives Rationale for the Environment

Objective	Assumption(s)	Rationale
OE.I&A	A.I&A	OE.I&A is a re-statement of A.I&A, requiring that the TOE platform provides means to identify and authenticate users and to provide corresponding user ID and attributes to Exchange.
OE.DAC	A.ACCESS_CONTROL	OE.DAC is a re-statement A.ACCESS_CONTROL, protecting TOE's executables, libraries or data files from unauthorized access and modification.
OE.COM_PROT	A.COM_PROT	OE.COM_PROT is a re-statement of A.COM_PROT, requiring that the TOE platform provides means to protect communications between the TOE and remote trusted IT products (clients or SMTP servers).
OE.PLATFORM_ SUPPORT	A.CORRECT_HW	OE.PLATFORM_SUPPORT is a re-statement of A.CORRECT_HW, ensuring that the underlying hardware/firmware work correctly as expected.
OE.PHYSICAL	A.PHYS_PROTECT	OE.PHYSICAL is a re-statement of A.PHYS_PROTECT, protecting the system the TOE is running on from unauthorized modification or tampering.
OE.INSTALL	A.NO_EVIL_ADM, A.INSTALL, A.MANAGE	OE.INSTALL is a combined re-statement of A.INSTALL, A.MANAGE and A.NO_EVIL_ADMIN, ensuring that the TOE and its platform is installed, configured, and managed in the certified configuration by competent and trustworthy individuals.

8.2 Security Requirements Rationale

This chapter provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 TOE SFR Rationale

This chapter provides evidence demonstration that the security objectives of the TOE are satisfied by the corresponding security requirements and vice versa. The following tables provide the security requirements to security objective mapping and a rationale to justify the mapping.

Table 12 – Mapping of TOE SFRs to Objectives

	O.DAC	O.RESTDIST	O.CONBLK	O.FILTER_EMAIL	O.QUOTA
FDP_ACC.1.a	X				
FDP_ACC.1.b		X			
FDP_ACF.1.a	X				
FDP_ACF.1.b		X			
FDP_IFC.1			X	X	
FDP_IFF.1			X	X	
FRU_RSA.1.a/b					X
FMT_MSA.1.a	X				
FMT_MSA.3.a	X				
FMT_MSA.3.b		X			
FMT_MSA.3.c			X	X	
FMT_SMF.1	X	X	X	X	X
FMT_SMR.1.a	X				

Table 13 – TOE SFRs to Objectives Rationale

SFR	Objective(s)	Rationale
FDP_ACC.1.a / FDP_ACF.1.a	O.DAC	To protect mailboxes and public folders and their contents from unauthorized access, including modification and deletion of messages, FDP_ACC.1.a and FDP_ACF.1.a provide discretionary access controls based on user identity. These requirements directly support O.DAC.

SFR	Objective(s)	Rationale
FDP_ACC.1.b / FDP_ACF.1.b	O.RESTDIST	To meet the objective O.RESTDIST, FDP_ACC.1.b and FDP_ACF.1.b allow the Exchange administrator to put discretionary access controls on distribution lists. One way method employed by senders of UCE requires the sender to guess at the names of potential distribution lists. A design meeting these SFRs will allow the Exchange administrator to protect distribution lists so that only authenticated users and/or explicitly allowed senders can send to distribution lists.
FDP_IFC.1 / FDP_IFF.1	O.CONBLK O.FILTER_EMAIL	To help meet the objective O.CONBLK, FDP_IFC.1 and FDP_IFF.1 provide blocking of SMTP connections based on the IP address or domain of the sending SMTP server. To help meet the objective O.FILTER_EMAIL, FDP_IFC.1 and FDP_IFF.1 provide filtering of SMTP messages based on the FROM: field and the RCPT TO: of the RFC821 envelope and the security ID of the sender (if authenticated).
FMT_MSA.1.a	O.DAC	FMT_MSA.1.a supports the management of security attributes used to make access decisions, Indirectly supporting O.DAC by allowing folder/item owner and Exchange Administrator to make changes to the corresponding security attributes.
FMT_MSA.3.a	O.DAC	FMT_MSA.3.a supports the management of security attributes used to make access decisions by providing permissive default values for security attributes concerning object owner and restrictive default values for security attributes concerning other users, as needed for O.DAC.
FMT_MSA.3.b	O.RESTDIST	FMT_MSA.3.b supports the management of security attributes used to make access decisions by providing permissive default values for security attributes needed for O.RESTDIST.
FMT_MSA.3.c	O.CONBLK O.FILTER_EMAIL	FMT_MSA.3.c supports the management of security attributes used to make access decisions by providing permissive default values for security attributes needed for O.CONBLK and O.FILTER_EMAIL.
FMT_SMF.1	O.DAC O.CONBLK O.RESTDIST O.FILTER_EMAIL O.QUOTA	FMT_SMF.1 specifies the security functions managed by the Exchange administrator (the TOE has only one top-level administrative security function SF.SM). FMT_SMF.1 indirectly supports O.DAC, O.CONBLK, O.RESTDIST, O.FILTER_EMAIL and O.QUOTA.
FMT_SMR.1.a	O.DAC	FMT_SMR.1.a maintains owner information for mailboxes and public folders, indirectly supporting O.DAC.

SFR	Objective(s)	Rationale
FRU_RSA.1.a/b	O.QUOTA	To help reduce the amount of storage consumed by UCE, the Exchange administrator can place quotas on the amount of storage for mailboxes and public folders. This SFR directly meets O.QUOTA.

Summarized, all TOE SFRs trace back to TOE security objectives.

Table 14 – TOE Objectives to SFRs Rationale

Objective	SFR(s)	Rationale
O.DAC	FDP_ACC.1.a FDP_ACF.1.a FMT_MSA.1.a FMT_MSA.3.a FMT_SMF.1 FMT_SMR.1.a	Discretionary access control for mailboxes and public folders is directly supported by access control components FDP_ACC.1.a and FDP_ACF.1.a. Indirect support is provided by the corresponding components from the FMT class, to enable management of the security attributes used by discretionary access control and to restrict this management to the Exchange Administrator and the folder owner, respectively.
O.RESTDIST	FDP_ACC.1.b FDP_ACF.1.b FMT_MSA.3.b FMT_SMF.1	Distribution list restriction is directly supported by access control components FDP_ACC.1.b and FDP_ACF.1.b. Indirect support is provided by the corresponding components from the FMT class, to enable management of the security attributes used for distribution list restriction.
O.CONBLK	FDP_IFC.1 FDP_IFF.1 FMT_MSA.3.c FMT_SMF.1	Objective O.CONBLK is primarily met by FDP_IFC.1 and FDP_IFF.1, which provide blocking of SMTP connections based filtering of SMTP messages based on the FROM: field and the RCPT TO: of the RFC821 envelope and the security ID of the sender (if authenticated). Indirect support is provided by the corresponding components from the FMT class, to enable management of connection blocking and corresponding security attributes.
O.FILTER_EMAIL	FDP_IFC.1 FDP_IFF.1 FMT_MSA.3.c FMT_SMF.1	Objective O.FILTER_EMAIL is primarily met by FDP_IFC.1 and FDP_IFF.1, which provide filtering of SMTP messages based on the FROM: field and the RCPT TO: of the RFC821 envelope and the security ID of the sender (if authenticated). Indirect support is provided by the corresponding components from the FMT class, to enable management of message filtering and corresponding security attributes.
O.QUOTA	FRU_RSA.1.a/b	O.QUOTA is directly supported by FRU_RSA.1 requiring quota functionality concerning mailbox and public folder sizes.

Summarized, all TOE security objectives are covered by the TOE SFRs.

8.2.2 Environment SFR Rationale

This chapter provides evidence demonstration that the IT security objectives of the environment are satisfied by the corresponding security requirements and vice versa. The following tables provide the IT security requirements to security objective mapping and a rationale to justify the mapping (non-IT security objectives, i.e. objectives related to personnel or procedural issues are not included in this rationale, as these do not trace to security functional requirements).

Table 15 – Mapping of Environment SFRs to IT Objectives

	OE.I&A	OE.DAC	OE.COM_PROT
FDP_ACC.1.c		X	
FDP_ACF.1.c		X	
FIA_UAU.2	X		
FIA_UID.2	X		
FIA_ATD.1	X		
FMT_MOF.1		X	
FMT_MSA.1.b/c		X	
FMT_SMR.1.b	X		
FTP_TRP.1			X

Table 16 – Environment SFRs to IT Objectives Rationale

SFR	Objective(s)	Rationale
FDP_ACC.1.c / FDP_ACF.1.c	OE.DAC	FDP_ACC.1.c and FDP_ACF.1.c directly support OE.DAC, as they define requirements about access control for NTFS files and folders and registry and Active directory objects (to protect the TOE and its data).
FIA_UAU.2 / FIA_UID.2	OE.I&A	FIA_UAU.2 and FIA_UID.2 directly support OE.I&A, as they define requirements about identification and authentication of users (the resulting authentication state is then utilized by the TOE).
FIA_ATD.1	OE.I&A	FIA_ATD.1 directly supports OE_I&A, as it defines requirements about user attributes to be provided by the IT environment (which are then utilized by the TOE).

SFR	Objective(s)	Rationale
FMT_MOF.1	OE.DAC	FMT_MOF.1 restricts enabling/disabling of some TOE functionality, i.e. modification of the corresponding configuration settings, to the Exchange Administrator. Therefore it directly supports OE.DAC, which shall prevent - among others – unauthorized access to TSF data.
FMT_MSA.1.b/c	OE.DAC	FMT_MSA.1.b/c restrict setting of some security attributes, i.e. modification of the corresponding configuration settings, to the Exchange Administrator. Therefore they directly support OE.DAC, which shall prevent – among others – unauthorized access to TSF data.
FMT_SMR.1.b	OE.I&A	FMT_SMR.1.b maintains the Exchange Administrator role, directly supporting OE.I&A, which shall maintain user IDs and corresponding attributes.
FTP_TRP.1	OE.COM_PROT	FTP_TRP.1 directly supports OE_COM_PROT, as it defines requirements about usage of a secure communication path for SMTP, HTTP/HTTP/DAV and RPC access (to protect communication data from disclosure or modification).

Summarized, all environment SFRs trace back to environment IT security objectives.

Table 17 – Environment IT Objectives to SFRs Rationale

Objective	SFR(s)	Rationale
OE.I&A	FIA_UAU.2 FIA_UID.2 FIA_ATD.1 FMT_SMR.1.b	OE.I&A is covered by FIA_UAU.2, FIA_UID.2, FIA_ATD.1 and FMT_SMR.1.b, as these define requirements about the necessary identification and authentication of users and about the necessary provision of user attributes (which are used by the TOE)
OE.DAC	FDP_ACC.1.c FDP_ACF.1.c FMT_MOF.1 FMT_MSA.1.b/c	OE.DAC is covered by FDP_ACC.1.c and FDP_ACF.1.c, as these define the necessary requirements about access control for NTFS files and folders and Active directory objects (to protect the TOE and its data). Furthermore the FMT requirements define, for which TSF data the IT environment has to restrict modification to the Exchange Administrator.
OE.COM_PROT	FTP_TRP.1	OE.I&A is covered by FTP_TRP.1, as this defines the necessary requirements about provision of secure communication between the TOE and remote trusted IT products (to protect communication data from disclosure or modification).

Summarized, all environment IT security objectives are covered by the environment SFRs.

8.2.3 TOE SAR Rationale

This ST has been developed for a TOE in a physically secure environment. The TOE will be exposed to a low level of risk environment because the TOE sits protected space where it is under almost constant supervision. Agents cannot physically access the TOE and have no means of tampering with the TOE. However, the TOE does expose a network interface and implements Internet standards for the exchange of messages and could be the target of an attack to gain access to a protected network.

But as stated in chapter 3, the TOE is intended to be used in cases where a low attack potential due to asset value, environmental protection, and resulting attacker motivation and capabilities are given.

Therefore Evaluation Assurance Level 4 is appropriate, as it contains AVA_VLA.2 component, which shall provide confidence that the TOE is resistant against attackers possessing a low attack potential (by low-level design and implementation evaluation and independent developer and evaluator vulnerability analyses).

The augmentation by ALC_FLR.3 has been chosen to ensure that security of the TOE is maintained after evaluation/certification is finished.

8.2.4 TOE SFR and SAR Dependencies Rationale

The following table is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied.

The dependencies of the SFRs have been satisfied within the TOE SFRs, with the following exceptions:

- The dependency FIA_UID.1 is fulfilled by the IT environment (in form of hierarchical component FIA_UID.2). The TOE is integrated with the host operating system and relies upon the operating system to perform identification and authentication of users.
- The dependency FMT_SMR.1 is partly fulfilled by the IT environment (in form of FMT_SMR.1.b). The role Exchange Administrator is maintained by the Active Directory (in terms of membership to a dedicated user group).
- As SFRs FMT_MSA.3.b and FMT_MSA.3.c do not require a specific user role nor refer to one, their dependencies FMT_SMR.1 are not applicable here.

Table 18 - SFR Dependencies Status

SFR ID	SFR Name	Dependency (as actually included in this ST)	Satisfied
FDP_ACC.1.a	Subset access control	FDP_ACF.1.a	Yes, by TOE
FDP_ACC.1.b	Subset access control	FDP_ACF.1.b	Yes, by TOE
FDP_ACF.1.a	Security attribute based access control	FDP_ACC.1.a, FMT_MSA.3.a	Yes, by TOE
FDP_ACF.1.b	Security attribute based access control	FDP_ACC.1.b, FMT_MSA.3.b	Yes, by TOE

SFR ID	SFR Name	Dependency (as actually included in this ST)	Satisfied
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Yes, by TOE
FDP_IFF.1	Simple security attributes	FDP_IFC.1, FMT_MSA.3.c	Yes, by TOE
FRU_RSA.1.a	Maximum quotas	None	n/a
FRU_RSA.1.b	Maximum quotas	None	n/a
FMT_MSA.1.a	Management of security attributes	FMT_ACC.1.a, FMT_SMF.1, FMT_SMR.1.a/b	Yes, by TOE and IT environment
FMT_MSA.3.a	Static attribute initialization	FMT_MSA.1.a, FMT_SMR.1.a	Yes, by TOE
FMT_MSA.3.b	Static attribute initialization	FMT_MSA.1.b (A dependent FMT_SMR.1 requirement is not needed here, as FMT_MSA.3.b does not require or refer to a security role.)	Yes, by TOE
FMT_MSA.3.c	Static attribute initialization	FMT_MSA.1.c (A dependent FMT_SMR.1 requirement is not needed here, as FMT_MSA.3.b does not require or refer to a security role.)	Yes, by TOE
FMT_SMF.1	Specification of management functions	None	n/a
FMT_SMR.1.a	Security roles	FIA_UID.2	Yes, by IT environment.

SAR dependencies identified in the CC have been met by this ST as

- within each EAL (here EAL4 has been chosen) all dependencies are met by definition of the EALs, and
- the only augmentation requirement ALC_FLR.3 has no dependencies.

Dependencies of the SFRs for the IT environment haven't been regarded.

8.2.5 Explicitly Stated Requirements Rationale

This ST contains no explicitly stated requirements.

8.2.6 Explicitly Stated Requirements Dependencies Rationale

This ST contains no explicitly stated requirements.

8.2.7 TOE SOF Claim Rationale

This ST does not include a SOF claim for the TOE. As explained in chapter 5.5, the TOE only contains security functions which are realized by deterministic mechanisms (mainly comparisons of security attributes with configured values or lists).

8.2.8 Internal Consistency and Mutually Supportive Rationale

The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

The choice of security requirements is justified as shown in chapters 8.2.1, 8.2.2 and 8.2.3. The choice of SFRs and SARs is based on the assumptions about, the threats to and the objectives for the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

The security functions of the TOE satisfy the SFRs as shown in Table 20. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 18 and described in chapter 8.2.4.

The SARs are appropriate for the assurance level of EAL4 and are satisfied by the TOE as shown in Table 9. EAL4 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

The SFRs and SARs presented in chapter 5 and justified in chapters 8.2.1, 8.2.2 and 8.2.3 are internally consistent. There is no conflict between security functions, as described in chapter 2 and chapter 6, and the SARs to prevent satisfaction of all SFRs.

8.3 TOE Summary Specification Rationale

This chapter demonstrates that the TSFs and Assurance Measures meet the SFRs.

8.3.1 Security Functions Rationale

The specified TSFs work together to satisfy the TOE SFRs. The following tables provide a mapping between TOE SFRs and security functions and a rationale to justify the mapping.

Table 19 – Mapping of TOE SFRs to Security Functions

	SF.SM	SF.AC	SF.DLR	SF.CF	SF.MF	SF.QTA
FDP_ACC.1.a		X				
FDP_ACC.1.b			X			

	SF.SM	SF.AC	SF.DLR	SF.CF	SF.MF	SF.QTA
FDP_ACF.1.a		X				
FDP_ACF.1.b			X			
FDP_IFC.1				X	X	
FDP_IFF.1				X	X	
FRU_RSA.1.a/b						X
FMT_MSA.1.a	X					
FMT_MSA.3.a		X				
FMT_MSA.3.b	X					
FMT_MSA.3.c	X					
FMT_SMF.1	X					
FMT_SMR.1.a	X	X				

Table 20 – TOE SFRs to Security Functions Rationale

SFR	Security Function(s)	Rationale
FDP_ACC.1.a / FDP_ACF.1.a	SF.AC	FDP_ACC.1.a and FDP_ACF.1.a are directly instantiated by SF.AC as access rules about mailbox and public folders are reflected one to one in requirements and security function.
FDP_ACC.1.b / FDP_ACF.1.b	SF.DLR	FDP_ACC.1.b and FDP_ACF.1.b are directly instantiated by SF.DLR as access rules about distribution list access are reflected one to one in requirements and security function.
FDP_IFC.1 / FDP_IFF.1	SF.CF SF.MF	FDP_IFC.1 and FDP_IFF.1 requirements define two different information flow control aspects: control of external SMTP connections based on IP address or domain and control of message delivery based on sender/recipient information. Each of these aspects are directly instantiated by SF.CF and SF.MF, respectively, as information flow rules are reflected one to one in requirements and corresponding security function for both aspects.
FMT_MSA.1.a	SF.SM	FMT_MSA.1.a requires management of security attributes for mailbox and public folders access, as instantiated by SF.SM.

SFR	Security Function(s)	Rationale
FMT_MSA.3.a	SF.AC	FMT_MSA.3.a requires for mailbox access permissive default values for security attributes concerning object owner and restrictive default values for security attributes concerning other users, as instantiated by SF.AC. FMT_MSA.3.a requires for public folder access specific default values for security attributes, as instantiated by SF.AC.
FMT_MSA.3.b	SF.SM	FMT_MSA.3.b requires for distribution list access permissive default values for security attributes, as instantiated by SF.SM (on creation of a new distribution list corresponding restricted access flag is not set and Access ACL is empty).
FMT_MSA.3.c	SF.SM	FMT_MSA.3.c requires for connection filtering permissive default values for security attributes, as instantiated by SF.SM (initial Accept and Deny lists are empty). FMT_MSA.3.c requires for message filtering permissive default values for security attributes, as instantiated by SF.SM (initial Sender and Recipient Filtering Lists are empty).
FMT_SMF.1	SF.SM	FMT_SMF.1 is directly instantiated by SF.SM which comprises all management functions (except provision of default permissions for SF.AC).
FMT_SMR.1.a	SF.SM SF.AC	The requirement FMT_SMR.1.a (to maintain the role Folder Owner) is instantiated by SF.SM and SF.AC, which are able to distinguish the folder owner from other accessing users.
FRU_RSA.1.a/b	SF.QTA	FRU_RSA.1 is directly instantiated by SF.QTA.

Summarized, all TOE SFRs are covered by the TOE security functions.

Table 21 – Security Functions to TOE SFRs Rationale

Security Function	SFR(s)	Rationale
SF.SM	FMT_MSA.1.a FMT_MSA.3.b/c FMT_SMF.1 FMT_SMR.1.a	Security function SF.SM directly instantiates all security management requirements for the TOE (i.e. it contains management functionality concerning all other security functions) except FMT_MSA.3.a (which is instantiated by SF.AC). SF.SM is in particular also instantiating FMT_MSA.3.b and FMT_MSA.3.c requirements, as via the corresponding security functions SF.DLR and SF.CF/SF.MF no new controlled objects can be created (e.g. SF.DLR instantiates the access control for distribution lists, but creation of new distribution lists with permissive default security attributes is up to SF.SM).
SF.AC	FDP_ACC.1.a FDP_ACF.1.a FMT_MSA.3.a FMT_SMR.1.a	Security function SF.AC is directly instantiating the requirements FDP_ACC.1.a and FDP_ACF.1.a. As SF.AC allows creation of new controlled objects, FMT_MSA.3.a (Static attribute initialization) is also instantiated by SF.AC. Furthermore SF:AC is able to distinguish the Folder Owner from other accessing users, therefore implementing FMT_SMR.1.a. (Other security management concerning SF.AC is performed by SF.SM.)
SF.DLR	FDP_ACC.1.b FDP_ACF.1.b	Security function SF.DLR is directly instantiating the requirements FDP_ACC.1.b and FDP_ACF.1.b. (Security management concerning SF.DLR is performed by SF.SM.)
SF.CF	FDP_IFC.1 FDP_IFF.1	Security function SF.CF is instantiating the part of requirements FDP_IFC.1 and FDP_IFF.1, which is related to blocking of external SMTP connections based on sender IP address or domain. (Security management concerning SF.CF is performed by SF.SM.)
SF.MF	FDP_IFC.1 FDP_IFF.1	Security function SF.MF is instantiating the part of requirements FDP_IFC.1 and FDP_IFF.1, which is related to filtering of messages according to sender and recipient information. (Security management concerning SF.MF is performed by SF.SM.)
SF.QTA	FRU_RSA.1.a/b	Security function SF.QTA is directly instantiating the requirements FRU_RSA.1.a/b. (Security management concerning SF.QTA is performed by SF.SM.)

Summarized, all TOE security functions trace back to TOE SFRs.

8.3.2 Assurance Measures Rationale

Chapter 6.2 of this document identifies the Assurance Measures implemented by Microsoft Corporation to satisfy the assurance requirements of EAL4, augmented with ALC_FLR.3 as delineated in the table in Annex B of the CC, Part 3. Table 9 - Assurance Measures clearly shows that for each assurance requirement dedicated documentation will be provided and/or appropriate action will be taken (e.g. performance of testing). The listed assurance measures are in principle suitable to meet the assurance requirements – if they actually are will be determined when these will be evaluated.

9 Appendix

9.1 References

The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032, Incorporated with interpretations as of 2003-12-31.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033, Incorporated with interpretations as of 2003-12-31.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0, Incorporated with interpretations as of 2003-12-31.

Furthermore all Final Interpretations (FI) about CC and CEM dated after 2003-12-31 have been regarded.

9.2 Conventions, Glossary, and Abbreviations

This chapter identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

9.2.1 Conventions

This chapter describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

The CC allows several operations to be performed on security functional components; *assignment, refinement*, *selection,* and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment value(s)] indicates an assignment.

The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. In this ST refinements have been exclusively used to increase readability and understandability of security requirements, not to limit the set of acceptable implementations by specifying additional technical detail.

The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

Iterated functional components are given unique identifiers by appending to the component/element name from CC an additional period and a letter, i.e., FDP_ACC.1.a for an iterated component and FDP_ACC.1.1.a for an iterated element.

Plain *italicized text* is used to emphasize text.

9.2.2 Glossary

Access Control List	(ACL) A list of security protections that applies to an object. (An object can be a file, process, event, or anything else having a security descriptor.) An entry in an access control list (ACL) is an access control entry (ACE). There are two types of access control list, discretionary and system.
Active Directory	Active Directory is a directory service. It supports a single unified view of objects on a network and allows locating and managing resources faster and easier.
Administrator	Either an Exchange administrator or a Windows administrator.
Authentication	Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks, authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. Logically, authentication precedes authorization (although they may often seem to be combined).
Authenticated user	A user, who has provided valid credentials and thus, for whom the authentication could be carried out successfully.
Authentication data	Information used to verify the claimed identity of a user.
Authorization	Authorization is the process of giving someone permission to do or permission to have something. In multi-user computer systems, an administrator defines which users are allowed access a system and what privileges of use (such as access to which file directories, applications, and so forth). Assuming that someone has logged in to a computer operating

	system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by an administrator and the actual checking of the permission values that have been set up when a user is getting access. Logically, authorization is preceded by authentication.
Authorized user	A user who may, in accordance with the TOE Security Policy (TSP[14]), perform an operation.
Block List Service provider	A service provider that provides a blocklisting service, based on DNSBL-Lists (see Blocklisting)
Blocklisting	Blocklisting is a variation on filtering whereby a mail server refuses to accept any email from machines that have a reputation for producing a disproportionate amount of spam. The main tool for blocklisting are so-called DNSBL Lists. These are publicly available lists of IP addresses that can be queried using a DNS lookup. There are a wide variety of DNSBL lists listing IP addresses according to various criteria; an individual site will have to choose the services to use based upon their own requirements.
Credentials	An authentication method used to validate client-to-server and server-to-server communication. Credentials include a user name and a password that is used to validate requests from client computers or from other computers in an array or chain.
Common Information Model	The Common Information Model (CIM) is an extensible, object-oriented data model that contains information about different parts of an enterprise. Through Windows Management Instrumentation (WMI), a developer can use the CIM to create classes that represent hard drives, applications, network routers, or even user-defined technologies such as a networked air conditioner.
Discretionary Access Control List	(DACL) An access control list that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.
Event Sink	A function that handles events. The code, which contains event handlers for one or more controls, is an event sink.
Exchange administrator	An authorized user, who installs, configures and operates Exchange 2003.
External IT entity	Any email client or SMTP server.
Human User	Any person who interacts with the TOE.
Identification	Identification, according to a current compilation of information security terms, is "the process that enables recognition of a user described to an automated data processing system. This is generally by the use of unique machine-readable names" [Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)].
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Mail-enabled	A public folder may be mail-enabled, i.e. an email address is assigned to the public folder and sending a message to this address results in posting of a message in the public folder.

[14] TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE

Microsoft Management Console (MMC)	MMC centralizes and unifies the experience of anyone configuring or monitoring computers and applications. MMC is a user interface shell (the console), application programming interfaces (APIs) for ISVs to use the MMC shell, and a, and a set of programming guidelines. MMC is a tool host—it provides no management functionality of its own. The MMC console itself is a Windows-based multiple document interface (MDI) application. MMC itself provides no management behavior, but instead provides a common environment for the (MMC) snap-ins, which provide the actual management functionality.
MMC Snap-In	Application-specific software that makes up the smallest unit of MMC extension. One snap-in represents one unit of management behavior. The MMC provides only a common environment. The specific management functionality for different applications is implemented in MMC Snap-Ins. These Snap-Ins are opened within the MMC which provides a user interface shell for the snap-ins.
Object	An entity within the TOE Security Function (TSF[15]) Scope of Control (TSC[16]) that contains or receives information and upon which subjects perform operations.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secure Sockets Layer (SSL)	A protocol that supplies secure data communication through data encryption and decryption. SSL enables communications privacy over networks.
Security context	The security attributes or rules that are currently in effect. A security context is an opaque data structure that contains security data relevant to a connection, such as a session key or an indication of the duration of the session.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.
Security Identifier	(SID) A data structure of variable length that identifies user, group, and computer accounts. Every account in a Windows Active Directory forest is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.
Service Pack	A collection of product enhancements and bug fixes for a specific Microsoft product.
Snap-In	See MMC Snap-In
Subject	An entity within the TSC that causes operations to be performed.
System administrator	An authorized user who manages the Windows 2003 operating system, which is used as a platform for the Exchange 2003 product.
TLS	Transport Layer Security: TLS is based on the SSL 3.0 Protocol Specification; see Secure Sockets Layer
User	Any entity (human user or external IT entity) outside the TOE, that interacts with the TOE.
Windows	The WMI infrastructure is a Microsoft Windows operating system

As defined in the CC, Part 1, version 2.1:

[15] TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

[16] TSC -The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

Management Instrumentation	component that moves and stores information about objects to be managed. The WMI infrastructure is made of two components: the Windows Management service, and the WMI repository. The Windows Management service acts as an intermediary between the providers, management applications, and the WMI repository, placing information from a provider into the WMI repository. The Windows Management service also accesses the WMI repository in response to queries and instructions from management applications. Finally, the Windows Management service can pass information directly between a provider and a management application. In contrast, the WMI repository acts as a storage area for information passed in by the various providers.
WMI-Provider	A Windows Management Instrumentation (WMI) provider is an intermediary between WMI and the object to be managed. A provider can be preinstalled with a managed object, or a developer can create a custom provider to use with a specific technology.

9.2.3 Abbreviations

The following abbreviations are used in this Security Target:

Abbreviation	Definition
AC	Access Control
ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CF	Connection Filtering
CM	Configuration Management
COM_PROT	Communication Protection
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DLL	Dynamic Linked Library
DLR	Distribution List Restriction
EAL	Evaluation Assurance Level
ESM	Exchange System Manager
FDP	User Data Protection CC Class
FI	Final Interpretation
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of Security Functions
FSP	Functional Specification
HLD	High Level Design

Abbreviation	Definition
HTTP-DAV	Hypertext Transfer Protocol Distributed Authoring and Versioning
I&A	Identification & Authentication
IIS	Internet Information Server
IMAP4	Interactive Mail Access Protocol Version 4 (see RFC1730)
ISO	International Standards Organization
ISO 15408	Common Criteria 2.1 ISO Standard
ISV	Independent Software Vendor
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAPI	Message Application Programming Interface
MF	Message Filtering
MIME	Multipurpose Internet Mail Extensions
MMC	Microsoft Management Console
MOF	Management of Functions
MSDN	Microsoft Developer Network
MTD	Management of TSF Data
OLE	Object linking and embedding
OMA	Outlook Mobile Access
OSI	Open Systems Interconnection Reference Model
OSP	Organizational Security Policy
OWA	Outlook Web Access
PC	Personal Computer
PDA	Personal Digital Assistant
POP3	Post Office Protocol Version 3 (see RFC1725)
PP	Protection Profile
QTA	Quota
RPC	Remote Procedure Call
RTM	Release to Market
SA	Exchange System Attendant
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SMTP	Simple Mail Transport Protocol
SOF	Strength of Function
SSL	Secure Socket Layer

Abbreviation	Definition
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UIA	User Identification
WebDAV	Web Distributed Authoring and Versioning
WMI	Windows Management Instrumentation