Exchange Server 2007 Common Criteria Evaluation

Security Target

Exchange Server 2007 Team

Author: Amy Blumenfield

Version: 1.38
Date: 2009-09-28
File Name: MS_E12_ST_1.38.doc

Abstract

This document is the Security Target (ST) for Exchange Server 2007 Common Criteria Certification

Keywords

Common Criteria, Exchange, Security, Evaluation, Security Target

Revision History

Date	Version	Author	Edit
Oct-06	0.1	Microsoft Exchange Team	Initial Release for evaluators
Oct-17	0.2	Microsoft Exchange Team	First draft version for kick off meeting
Nov-28	0.3	Microsoft Exchange Team	Revised draft version for kick off meeting
Jan-4	0.4	Microsoft Exchange Team	Updated SF.CF and rationale
Jan-5	0.5	Microsoft Exchange Team	Version for next kick-off meeting
Jan -25	0.6	Microsoft Exchange Team	Incorporated feedback from kick-off meeting
Feb-1	0.7	Microsoft Exchange Team	Minor updates to SF.TC and related parts, minor editorial updates
Feb-14	0.8	Microsoft Exchange Team	Addressed comments from evaluation
Feb-22	0.9	Microsoft Exchange Team	Addressed comments from evaluation
June-6	1.0	Microsoft Exchange Team	General Update after development of FSP and HLD
Sep-07	1.1	Microsoft Exchange Team	General Update
Nov-27	1.2	Microsoft Exchange Team	General Update
Dec-4	1.21	Microsoft Exchange Team	Minor changes
Dec-11	1.22	Microsoft Exchange Team	Minor changes
Feb-07	1.23	Microsoft Exchange Team	Minor changes
Feb-26	1.24	Microsoft Exchange Team	Minor changes
Mar-16	1.25	Microsoft Exchange Team	Minor changes
Nov-19	1.26	Microsoft Exchange Team	SP2 added

Nov-19	1.27	Microsoft Exchange Team	FIA_AFL removed
Jan-15	1.28	Microsoft Exchange Team	SF.I&A restrictions, OR comments
Jan-22	1.29	Microsoft Exchange Team	SF.I&A changes
Jan-29	1.30	Microsoft Exchange Team	SF.I&A changes
Jan-29	1.31	Microsoft Exchange Team	Minor changes
Feb-03	1.32	Microsoft Exchange Team	Minor changes
Feb-04	1.33	Microsoft Exchange Team	Minor changes
April -04	1.34	Microsoft Exchange Team	Minor changes
May -19	1.35	Microsoft Exchange Team	Minor changes
Sep-09	1.36	Microsoft Exchange Team	Minor changes
Sep-10	1.37	Microsoft Exchange Team	Minor changes
Sep-28	1.38	Microsoft Exchange Team	Added references to guidance documents

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. A 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 2007 Common Criteria Evaluation Security Target
ST Version:	1.38
Date:	2009-09-28
Author:	Amy Blumenfield, Microsoft Corporation
TOE Identification:	Microsoft Exchange Server 2007 Enterprise Edition (English) and its related guidance documentation
TOE Version/Build:	08.02.0176.002[1]
TOE Platform:	Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English) including IIS 6.0 and Active Directory with patches as listed in the Exchange Server Guidance Addendum
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 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] This version includes SP2.

1.2 ST Overview

The TOE described in this Security Target is the Exchange Server 2007 Enterprise Edition, Service Pack SP2 (English) (hereinafter called Exchange (Exchange 2007) or TOE for simplicity), an e-mail and collaboration server that provides secure access to personal and shared data to a variety of clients using various protocols.

The security functionality of the TOE is based on the previous evaluation of Exchange 2003 but extends the previous evaluation by adding new Security Functions reflecting the further development of the product.

A summary of the TOE, its boundaries, the relationship to its client applications and its 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 extended - The functional requirements in this ST include functional components not defined in CC Part 2.
- The TOE is CC Part 3 conformant - The assurance requirements in this ST are based only upon assurance components in CC Part 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 2007 is an e-mail and collaboration server that provides secure access to personal and shared data to a variety of clients using various protocols.

The platform for the evaluated version of Exchange is Windows Server 2003 Enterprise Edition x64 Edition R2[2] plus SP 2 (English) operating system with patches as listed in the Exchange Server Guidance Addendum, which includes Internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

2.2 Physical Scope and Boundary of the TOE

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

Mailbox Server Role

The Mailbox server role hosts mailbox and public folder databases. The administrator manages e-mail Lifecycle folders and policies from a Mailbox server. The mailbox server role, in conjunction with the environment, provides access control for users, mail, fax, and voice messages.

Client Access Server Role

This is the server that hosts the client protocols. The Client Access Server also exposes a Web Services interface for application developers.

The Client Access server role accepts connections to the Exchange 2007 server from a variety of different clients. Please see chapter 2.3.2 for more details on client applications and protocols.

Unified Messaging Server Role

Unified Messaging combines voice messaging, fax, calendaring and e-mail, which are accessible from a telephone or a computer. Exchange Server 2007 Unified Messaging integrates Exchange Server with telephony networks and brings Unified Messaging features to the core of Exchange Server. Outlook Voice Access (OVA) is a feature of the Unified Messaging Role and lets users access their mailbox using telephone communication. OVA can optionally be secured by the Transport Layer Security Protocol (TLS).

Hub Transport Server Role

This is the mail routing server that routes mail within the Exchange organization. The Hub Transport server role handles all mail flow inside the organization, applies transport rules,

[2] Also simply referred to as “Windows” in the rest of the document

applies journaling policies, and delivers messages to the recipient's mailbox. Messages that are sent to the Internet are relayed by the Hub Transport server to the Edge Transport server role that is deployed in the perimeter network.

Edge Transport Server Role

This is the mail routing server that sits at the perimeter of the network topology and routes mail into and out of the Exchange organization. The Edge Transport server role handles the following scenarios:

Mail Flow

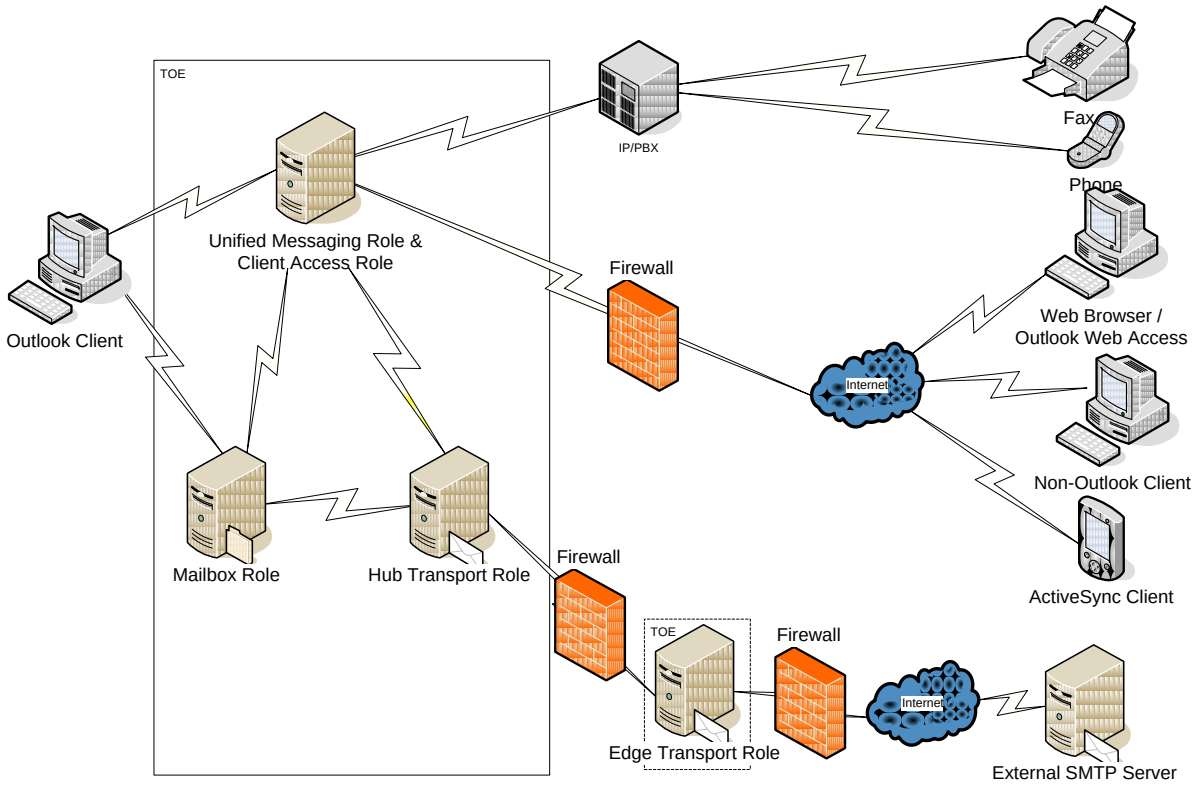
The Edge Transport server role accepts mail coming into the Exchange Server 2007 organization from the Internet and routes all outbound messages to the Internet.

Filtering

The Edge Transport server role helps protect the Exchange Server 2007 organization from spam by filtering inbound messages as they arrive and before they are delivered to the internal private network.

All roles, with the exception of the Edge Transport Server, can be installed on a single machine; however, for reasons of performance, in medium and large organization installations, these roles may be installed on more than one physical server. The TOE roles communicate in the same way, whether they are installed on one server or many servers. More information about the installation of the TOE will be provided in the related guidance documents.

Figure 1 – Exchange Server Installation



The following guidance documents and supportive information belong to the TOE:

- Exchange Server Help file (as of August 2009) [AGD]: This is the general guidance documentation of the TOE.
- Exchange Server Guidance Addendum [AGD_ADD]: The guidance addendum describes the specific aspects of the evaluated version. It extends the general guidance of the Exchange Server.

The website https://secure.tuvit.de/ provides both guidance documents and additional information about the TOE and its evaluated configuration. It shall be visited before using the TOE.

2.3 Logical Scope and Boundary of the TOE

The logical scope of the TOE can be defined by its Security Functions, the provided protocols, the excluded features and the functionality of the Operating System the TOE relies on.

2.3.1 Security Features

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.
- Message Filtering (**SF.MF**) – filters potential spam messages based on Administrator configured SMTP filters, including local and third party block/allow lists.
- Attachment Filtering (**SF.AF**) – provides a mechanism to filter potentially harmful attachments from external networks.
- Transport Filtering **(SF.TF)** – Allows the administrator to define mail policies to prevent specific internal and/or external users from emailing each other.
- Identification and Authentication **(SF.I&A)** – Provides an identification and authentication mechanism for the Outlook Voice Access functionality in cases where Outlook Voice Access is not secured by the use of the TLS protocol.
- Distribution Group Restriction (**SF.DGR**) – requires users sending mail to a distribution group to be successfully authenticated and to be authorized.
- Mailbox and public folder quota (**SF.QTA**) – allows Administrators to set quotas on the size of mailboxes and public folders.

2.3.2 Supported Protocols and clients

The TOE offers its services for users via a variety of protocols including:

- RPC for applications like Outlook 2007
- SMTP for generic clients and servers sending e-mail to the TOE
- HTTP for Web Browsers (using Outlook Web Access) and for Active Sync clients
- RPC tunneled over http
- Web Services Application Programming Interface (API) for In-house applications
- SIP/RTP for Outlook Voice Access (OVA).

Outlook Voice Access (OVA) can optionally be secured by enabling the TLS protocol with mutual authentication for SIP/RTP. In this case, the identification and authentication of OVA users is not done by the TOE but is the sole responsibility of the TLS authenticated application which is part of the IT environment.

Those protocols can be used to connect to the TOE by different clients. Clients can be 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 or Web Services to connect to the TOE.
- Outlook client:
  In contrast to the generic clients, an Outlook client uses RPC (or RPC over http) to connect to the TOE.

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

The Unified Messaging server role in Exchange 2007 lets users access voice mail, e-mail, fax messages, and calendar information located in their Exchange 2007 mailbox from an e-mail client such as Microsoft Outlook or Outlook Web Access, from a mobile device that has Microsoft Exchange ActiveSync enabled, such as a Windows Mobile® powered smartphone or a personal digital assistant (PDA), or from a telephone.

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

The scope of the TOE ends at the interfaces where it provides its services and does not include any functionality of any client.

2.3.3 Excluded features

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

- IMAP4
- POP3

Further, all clients that can be used to connect to the TOE (see previous chapter) are not addressed during the evaluation.

For features of the TOE that rely on the use of external lists for filtering of email messages it should be noted that the way these external lists are compiled and transferred to the TOE are out of scope of the evaluation.

2.3.4 Important functionality of the environment

The following security functionality of the TOE environment is used by the TOE:

- **Identification and Authentication** – the TOE enforces the identification and authentication of users only in cases the users connect to OVA over a connection which is not TLS secured. All other I&A functionality that the TOE depends on (to implement its access control policy) is part of the IT environment:
    - The TOE relies on Active Directory authenticating users when they attempt to access the TOE via RPC (MAPI), HTTP (including HTTP-DAV and Web Services) or SMTP interfaces. After Windows performed the identification and authentication tasks, it provides information about the corresponding user ID and attributes to the TOE. On the basis of this information, the TOE decides whether access is granted or denied.
    - When users attempt to access the TOE via SIP/RTP over a mutually authenticated TLS connection the platform may authenticate the connecting application using the provided certificate. The trusted application (e.g., a PBX or an Office Communication Server) will identify and authenticate the users and provide the identity of the user to the TOE.
- **TOE Data Protection** – provided by Windows discretionary access control. During common operation it is necessary to restrict 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 access. 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 is needed to protect 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 an operating system level.
- **TOE Data Management** – for the TOE data that is stored using functionality of the Operating System, the Operating System provides adequate default values, management functionality and restricts the management functionality to certain roles.

3 TOE Security Environment

As an e-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 it) therefore may vary in their sensitivity, depending on the organization Exchange is used in. Therefore, it is impossible to determine the 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 the attack potential could range from low to high.

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 1 - Assumptions

Assumption	Description
A.COM_PROT	It is assumed that the communication channels between all server roles are appropriately secured against eavesdropping and manipulation by physical protection of the wire or by using encryption. Any internet connection to a server role is assumed to be appropriately secured by a firewall. Finally, it is assumed that the connection between the TOE and the user (connecting to the Unified Messaging role, the Mailbox Role, the Hub role, or the Client Access Server role) is appropriately secured by a physical protection of the wire or by using encryption to avoid eavesdropping or manipulation of the communication.
A.INSTALL	It is assumed that the TOE will be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.

Assumption	Description
A.PLATFORM	The platform upon which the TOE resides is Windows Server 2003 Enterprise Edition x64 Edition R2[3] plus SP 2 (English). The platform provides: • Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases (mailboxes and public folders) only to the authorized administrators. • Functionality for supporting and enforcing Identification and Authentication of users. It is assumed that the platform ensures the identification and authentication of users except for the case that they connect via a non TLS encrypted Outlook Voice Access connection. • Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict the access to TSF data where necessary. Beside the software necessary for the management and operation of the TOE (e.g. management tools) it is assumed that no untrusted software is installed on the machines the TOE is installed on. The administrator(s) ensure – during TOE installation and operation - that the platform the TOE is running on allows the secure operation of the TOE.
A.BLOCKLIST	Block/allow lists from third parties - which are used to evaluate email messages - have to be of sufficient quality and trustworthy. Therefore it is assumed that only third party block/allow lists from trustworthy sources will be used and that the download of these block/allow lists is appropriately secured with respect to the integrity and authenticity of the block/allow lists
A.NO_EVIL_ADM	There will be one or more competent administrator(s) assigned to manage the TOE, its platform and the security of the information both of them contain. The administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by

[3] It should be noted that Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English) has been evaluated according to Common Criteria (see [WIN_ST]) and the functionality that is required by this assumption was part of this evaluation. However, for the context of this evaluation there is no need to install and configure the Operating System exactly in its certified version as this would limit the operation of the TOE to an unacceptable extent.

Assumption	Description
	the administration documentation.
A.PHYS_PROTECT	The TOE and its platform will be located within facilities providing controlled access to prevent unauthorized physical access.

3.2 Threats

Table 2 identifies the threats to the TOE. 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 potential attackers of the TOE are considered to be users with public knowledge of how the TOE operates. The attackers have only network access to the TOE, not physical access (see A.PHYS_PROTECT).

Table 2 - Threats to the TOE

Threat	Description
T.UNAUTH_DAC[4]	An unauthenticated user may attempt to read, create, modify or delete information contained in private stores (i.e. mailboxes) or public stores (i.e., public folders)[5], which are managed by the TOE. An attacker may try to get access to mailboxes or public folders although he has no account information and is not authenticated.
T.AUTH_DAC[4]	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. For example: A user could use his account information to authenticate against Windows (the TOE relies on identification and authentication of the operating system). Once authenticated he could try to get unauthorized access to mailboxes belonging to other users of the TOE.
T.UNAUTHUSE[4]	An authenticated user may attempt to read, delete or modify information contained in a public folder (e.g. shared folders

[4] Exchange Server 2007 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.

[5] 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
	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 in this case the authenticated user tries to get unauthorized access to a public folder instead of a private store, although he is not a member of a group that is allowed to access the folder or is not authorized to use.
T.SPAM	An attacker could send Unsolicited Commercial email (UCE or spam) through the TOE, and have it 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. For example, this unwanted information may result in an attempt to obtain financial information from the end-user (a “phishing” attack)
T.DL_MISUSE	An unauthenticated user or an authenticated but unauthorized user may send messages that consume TOE resources by delivering inappropriate email, such as UCE to a distribution group[6]. A distribution group may be restricted in a way that only authenticated and authorized users shall be allowed to send messages to a distribution group. An attacker may attempt to send mail for such a distribution group although he is not allowed to deliver email to this distribution group.
T.OVERFLOW	An attacker may attempt a denial of service attack by attempting to overflow a server’s storage space by sending a large amount of mail to an individual’s mailbox or a mail-enabled public folder. Furthermore regular users that keep all of their received messages could 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. The consequences of the above threats would be a failure of the TOE to deliver mail to *other* users due to a lack of system resources (e.g. lack of hard disk space).

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

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 the TOE shall comply with.

Policy	Description
OSP.MAIL_FLOW	Administrators shall be able to control email flow within their organization. The administrator shall be able to prevent email flow between specific senders and recipients based on the flowing characteristics of an email: • Sender • Recipients • Subject • Classification • Header • Attachment Name • Attachment Size • Attachment MIME type • Importance • Keywords contained in the subject or body The Administrators should also be able to prevent specific attachments from being sent to, from or around the organization.

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.

Objectives are also used to ensure that assumptions and organizational security policies are met.

4.1 Security Objectives for the TOE

This chapter identifies and describes the security objectives of the TOE.

Table 3 - 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) based on the identity of the user. 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 and documents.
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 or hostname of the remote SMTP sender using accept and block/allow lists configurable by the administrator. The TOE shall further be able to calculate a reputation level for SMTP servers that expresses, how likely this server is used for SPAM. The TOE shall be able to block messages based on the sending server's reputation level.
O.RESTDIST	The TOE shall allow Administrators to restrict mail routing to distribution groups[7] by only allowing mail to be delivered to the distribution group from authenticated and authorized users. Also, Administrators can specify which users can or cannot send mail to specific distribution groups.
O.REDUCE_SPAM	The TOE shall allow Administrators to reduce unwanted or unsolicited mail (UCE or spam) by providing a filter mechanism based on the sender and receiver information of an email.

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

Objective	Description
O.MAIL_FLOW	The TOE shall allow Administrators to control email flow within their organization. The to TOE will provide the administrator with filters to prevent email flow between specific senders and receivers based on the flowing characteristics of an email: • Sender • Recipients • CC: • Subject • Classification • Header • Attachment Name • Attachment Size • Importance • Keywords contained in the subject or body Also, the TOE will allow Administrators to prevent specific types of attachments (characterized by the extension or the MIME type of the attachment) from being sent to, from or around the organization.
O.QUOTA	The TOE shall allow 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 Administrator, the delivery of further mails will be stopped and the user informed about the actual mailbox size. In this case, only the user whose mailbox has exceeded the quota is not able to receive mail. Other users are not affected and receive mail as usual. If a public folder reaches a size defined by the Administrator, new items cannot be created in this folder.
O.I&A	The TOE shall provide an identification and authentication mechanism for users using Outlook Voice Access in cases the access is not secured by TLS[8]. The resulting information about the identity of the user is then used by other policies of the TOE.

4.2 Security Objectives for the Environment

The security objectives for the TOE Environment are defined in Table 4.

[8] In case of a connection that is secured via a mutually authenticated TLS channel the environment will be responsible for the identification and authentication of the user

Table 4 - Security Objectives for the TOE Environment

Objective	Description
OE.COM_PROT (Non-IT)	The administrator of the TOE shall ensure that the communication channels between all server roles are appropriately secured against eavesdropping and manipulation by physical protection of the wire or by using encryption. Any internet connection to a server role shall be appropriately secured by a firewall. The administrator shall ensure that the connection between the TOE and the user is appropriately secured by a physical protection of the wire or by using encryption to avoid eavesdropping or manipulation of the communication.
OE.INSTALL (Non-IT)	The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures and only by trustworthy staff. The administrator must ensure that the TOE is delivered, installed, configured, managed and operated in a manner that is consistent with IT security. Beside the software necessary for the management and operation of the TOE (e.g. management tools) no untrusted software shall be installed on the machines the TOE is installed on. The administrator(s) shall ensure – during TOE installation and operation - that the platform the TOE is running on allows the secure operation of the TOE.

Objective	Description
OE.PLATFORM (IT)	The platform upon which the TOE resides shall be Windows Server 2003 Enterprise Edition x64 Edition R2 plus SP 2 (English). The platform provides: • Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases (mailboxes and public folders) only to the authorized administrators. • Functionality for supporting and enforcing Identification and Authentication of users. The platform shall ensure the identification and authentication of users except for the case that they connect via a non TLS encrypted Outlook Voice Access connection. • Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict access to TSF data where necessary.
OE.BLOCKLIST (Non-IT)	Block/allow lists from third parties - which are used to evaluate email messages - have to be of sufficient quality and trustworthy. Therefore, the administrator shall ensure that only third party block/allow lists from trustworthy sources will be used and that the download of these block/allow lists is appropriately secured with respect to the integrity and authenticity of the block/allow lists
OE.PHYSICAL (Non-IT)	The administrators shall ensure that those parts of the TOE and its platform that are critical to security policy are protected from any physical attack.

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 5. The rest of this chapter contains a description of each component.

Table 5 - TOE Security Functional Requirements

Class FDP: User Data Protection	
FDP_ACC.1/Folder	Subset access control
FDP_ACC.1/Group	Subset access control
FDP_ACF.1/Folder	Security attribute based access control
FDP_ACF.1/Group	Security attribute based access control
FDP_IFC.1/Connect	Subset information flow control
FDP_IFC.1/SRL	Subset information flow control
FDP_IFC.1/Message	Subset information flow control
FDP_IFC.1/AttachmentFilter	Subset information flow control
FDP_IFC.1/Transport	Subset information flow control
FDP_IFF.1/Connect	Simple security attributes
FDP_IFF.1/SRL	Simple security attributes
FDP_IFF.1/Message	Simple security attributes
FDP_IFF.1/AttachmentFilter	Simple security attributes
FDP_IFF.1/Transport	Simple security attributes
Class FIA: Identification and Authentication	
FIA_SOS.1	Verification of secrets
FIA_UAU.8(EXP)	User subset authentication before any action
FIA_UID.3(EXP)	User subset identification before any action

FIA_USB.1	User-subject binding
Class FRU: Resource Allocation	
FRU_RSA.1/Mail	Maximum quotas
FRU_RSA.1/Public	Maximum quotas
Class FMT: Security Management	
FMT_SMF.1	Specification of management functions
FMT_MSA.1/Folder	Management of Security Attributes
FMT_MSA.3/Folder	Static attribute initialization
FMT_MSA.3/Group	Static attribute initialization
FMT_MSA.3/Connect	Static attribute initialization
FMT_MSA.3/SRL	Static attribute initialization
FMT_MSA.3/Message	Static attribute initialization
FMT_MSA.3/AttachmentFilter	Static attribute initialization
FMT_MSA.3/Transport	Static attribute initialization

5.1.1 Class FDP: User Data Protection

FDP_ACC.1/Folder Subset access control

FDP_ACC.1.1/Folder The TSF shall enforce the [Discretionary Access Control SFP] on [

subjects – processes acting on behalf of users

objects – mailbox and public folder items[9] and (sub)folders

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

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

[9] Mailbox and public folder items include all objects that are stored in a mailbox or public folder (e.g. emails, contacts or certificates)

FDP_ACF.1/Folder	**Security attribute based access control**
FDP_ACF.1.1/Folder	The TSF shall enforce the [Discretionary Access Control SFP] to objects based on the following: [Object Attributes - Access Control Lists that exist for every folder, Owner of the folder subject attribute –ID[10] of the user and its corresponding groups].
FDP_ACF.1.2/Folder	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 an entry in the ACL of the folder that the object resides in].
FDP_ACF.1.3/Folder	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].
FDP_ACF.1.4/Folder	The TSF shall explicitly deny access of subjects to objects based on the **following additional rules**: [none].

[10] The ID of the current user is provided by the Windows Operating System or by the authentication policy as expressed in FIA_UAU.8.(EXP) (only when the user is connected via non-TLS secured Outlook Voice Access).

FDP_ACC.1/Group **Subset access control**

FDP_ACC.1.1/Group The TSF shall enforce the [Distribution Group Restriction SFP] on [

subjects – users sending e-mail

objects – distribution groups

operation – use, i.e. send messages to a distribution group].

FDP_ACF.1/Group **Security attribute based access control**

FDP_ACF.1.1/Group The TSF shall enforce the [Distribution Group Restriction SFP] to objects based on the following: [

subject attribute – ID of the user and its corresponding group, FROM: field of the RFC 2821 payload envelope

object attributes (distribution groups) – restricted access flag, Access Control Lists (each distribution group has one ACL to allow users and one to deny users)].

FDP_ACF.1.2/Group 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 ID is available),

and

2) a) no Access Control List is configured
   or
   b) the Access ACL that is configured to contain only explicitly allowed IDs contains the ID of the sending user
   or
   c) the Access ACL that is configured to contain only explicitly denied IDs, does not contain the ID of the sending user].

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

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

Application Note: It should be noted that the ACLs for this Security Function can only contain the IDs of local users (i.e. users in the Active Directory). If an email is sent to a distribution group by an unauthenticated user, the sending user has no ID and the checks in 2b) and 2c) of FDP_ACF.1.2/Group will lead to the result that the user is not contained in the ACL.

FDP_IFC.1/Connect Subset information flow control

FDP_IFC.1.1/Connect The TSF shall enforce the [Connection Filtering SFP] on [

Subjects – External SMTP Servers, Edge Transport Server Role

Information – email messages

Operations – email transfer].

FDP_IFF.1/Connect Simple security attributes

FDP_IFF.1.1/Connect The TSF shall enforce the [Connection Filtering SFP] based on the following types of subject and information security attributes: [

subject attributes – IP address of the external SMTP server, allow/block lists of the Edge Transport Server Role, list of exceptional recipients of the Edge Transport Server Role

information attributes – recipients of the e-mail].

FDP_IFF.1.2/Connect The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [none]

FDP_IFF.1.3/Connect The TSF shall enforce the **additional ordered rules:** [

1. If the IP address of the sending external SMTP server is listed on a local allow list, the message will be accepted
2. If the IP address of the sending external SMTP server is listed on a local block list, the message will be rejected
3. If the IP address of the sending external SMTP server is listed on a remote allow list, the message will be accepted
4. If one of the recipients of the e-mail is on the local list of exceptional recipients the message will be accepted
5. If the IP address of the sending external SMTP server is listed on a remote block list, the message will be rejected
6. Else the message will be accepted].

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

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

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

Application Note: This functionality utilizes the following kinds of allow and block lists:

1. Local allow and block lists maintained by Administrators
2. Remote allow and block lists retrieved from external service providers (so called “block list service providers”)
3. A local list of exceptional recipients.

The remote lists are not considered to be Security Attributes in the context of this policy as they are not stored locally (The necessary characteristics of those block/allow lists are ensured via A.BLOCKLIST).

FDP_IFC.1/SRL	**Subset information flow control**
FDP_IFC.1.1/SRL	The TSF shall enforce the [Sender Reputation SFP] on [subjects: External SMTP Servers, Edge Transport Server Role information: email Messages Operations: Mail Transfer].
FDP_IFF.1/SRL	**Simple security attributes**
FDP_IFF.1.1/SRL	The TSF shall enforce the [Sender Reputation SFP] based on the following types of subject and information security attributes:[subject attributes - Sender Reputation Level (SRL) of the external SMTP server (calculated by the TOE), SRL Threshold and the local list of SRL values from the Edge Transport Server Role information attributes: None].
FDP_IFF.1.2/SRL	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [none].

FDP_IFF.1.3/SRL The TSF shall enforce the **additional rules:** [

- If the local list of SRL values contains an entry for the external SMTP server with a SRL value greater than or equal to the SRL threshold or

- The SRL value (calculated by the TOE) for the external SMTP server is greater than or equals the SRL Threshold

the server will be added to the local block list of FDP_IFF.1/Connect for an Authorized Administrator configurable period of time].

FDP_IFF.1.4/SRL The TSF shall provide the following **additional SFP capabilities:** [

Calculation of the SRL after an e-mail message has been received from an external SMTP server[11]].

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

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

FDP_IFC.1/Message Subset information flow control

FDP_IFC.1.1/Message The TSF shall enforce the [Message Filtering SFP] on [

subjects: External SMTP Servers, Edge Transport Server Role

information: email messages

Operations: email transfer].

FDP_IFF.1/Message Simple security attributes

FDP_IFF.1.1/Message The TSF shall enforce the [Message Filtering SFP] based on the following types of subject and information security attributes: [

subject attributes – sender and recipient filtering lists from the Edge Transport Server Role, local address book[12] from the Edge Transport Server Role

information attributes – MAIL FROM: field of the RFC 2821 envelope, RFC 2822 header, RCPT TO: field of the RFC 2821 envelope].

[11] Please note that the SRL is only calculated after at least 20 messages have been received from a server.

[12] The local address book is a list of local SMTP addresses.

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

The e-mail will be accepted unless:

a) the sender listed in the MAIL FROM: field of the (RFC 2821) message envelope is on the sender filtering list or

b) the sender in the FROM header of the message (RFC 2822) is on the sender filtering list or

c) the MAIL FROM: field of the RFC 2821 message envelope is blank[13] and the FROM header of the message (RFC 2822) does not contain a valid e-mail address[14] or

d) the recipient listed in the RCPT TO: field of the RFC 2821 message envelope is on the recipient filtering list or

e) the recipient does not exist in the local address book].

FDP_IFF.1.3/Message The TSF shall enforce the **additional rules**: [none].

FDP_IFF.1.4/Message The TSF shall provide the following **additional SFP capabilities:** [The TOE shall be able to evaluate the SPF record of the domain of the sender and stamp the result on the message].

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

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

[13] As this field can never be completely empty, the term “blank” refers to a so called null address which is a MAIL FROM field that contains the characters "<>"

[14] A valid email address in this context means a string in the structure of [recipient]@[domain].[top level domain]

FDP_IFC.1/AttachmentFilter Subset information flow control

FDP_IFC.1.1/ AttachmentFilter The TSF shall enforce the [Attachment SFP] on [

subjects: External SMTP Servers, Edge Transport Server Role

information: email messages

Operations: email transfer].

FDP_IFF.1/AttachmentFilter Simple security attributes

FDP_IFF.1.1/AttachmentFilter The TSF shall enforce the [Attachment SFP] based on the following types of subject and information security attributes: [

subject attributes - Attachment Policy of the Edge Transport Server Role

information attributes - MIME Type and extension of the attachment].

FDP_IFF.1.2/AttachmentFilter 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 not explicitly prohibited by the Attachment policy]

FDP_IFF.1.3/ AttachmentFilter The TSF shall enforce the **additional rule:** [

Attachments will be stripped or emails containing attachments will be blocked in accordance with the Attachment policy].

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

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

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

Application Note: The attachment policy as defined in FDP_IFF.1/AttachmentFilter comprises a set of ordered rules that are defined by the administrator of the TOE. These rules are evaluated in order to determine how an e-mail attachment shall be handled. The MIME type and Attachment extension information attributes are used by these rules to define whether a rule shall be applied to an attachment. Each rule is comprised of:

A) A set of criteria that defines the attachments to which the rule shall apply (based on MIME type and Attachment extension).
B) A set of exceptions to which the rule shall not be applied.

C) An action to perform when an attachment meets the rule criteria.

FDP_IFC.1/Transport	**Subset information flow control**
FDP_IFC.1.1/Transport	The TSF shall enforce the [Hub Transport SFP] on [subjects: Hub Transport Server Role information: email messages Operations: email transfer].
FDP_IFF.1/Transport	**Simple security attributes**
FDP_IFF.1.1/Transport	The TSF shall enforce the [Hub Transport SFP] based on the following types of subject and information security attributes: [subject attributes – Hub Transport Policy of the Hub Transport Server Role Information attributes – • Sender • Recipients • CC: • Subject • Classification • Header • Attachment Name • Attachment Size • Attachment extension • Importance • Key words in Subject or email body].
FDP_IFF.1.2/Transport	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [none].
FDP_IFF.1.3/Transport	The TSF shall enforce the **following additional rule:** [For each email the Hub Transport policy shall be evaluated and each rule that fits to the email shall be applied].
FDP_IFF.1.4/Transport	The TSF shall provide the following **additional SFP capabilities:** [none].
FDP_IFF.1.5/Transport	The TSF shall explicitly authorize an information flow based on the following rules: [none].
FDP_IFF.1.6/Transport	The TSF shall explicitly deny an information flow based on the following rules: [none].

Application Note: The Hub transport policy as defined in FDP_IFF.1/Transport comprises a set of ordered rules that are defined by the administrator of the TOE. The rules are evaluated in order to determine how an e-mail message shall be handled. Each rule is comprised of:

A) A set of criteria that define the mails to which the rule shall be applied (based on the information attributes).
B) A set of exceptions to which the rule shall not be applied.
C) An action to perform when a mail meets the rule criteria.

5.1.2 Class FIA: Identification and Authentication

FIA_SOS.1 **Verification of secrets**

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [Outlook Voice Access PIN quality metrics as defined by the administrator including an Outlook Voice Access PIN of at least 8 digits].

Application Note: The Outlook Voice Access PINs are the only secrets maintained by the TOE in the context of this requirement.

FIA_UAU.8(EXP) **User subset authentication before any action**

FIA_UAU.8(EXP).1 The TSF shall require each user connecting via [non TLS-secured Outlook Voice Access] to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.3(EXP) **User subset identification before any action**

FIA_UID.3(EXP).1 The TSF shall require each user connecting via [non TLS-secured Outlook Voice Access] to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 **User-subject binding**

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [

- ID (user's identity)
- Group Memberships].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

5.1.3 Class FRU: Resource Utilization

FRU_RSA.1/Mail **Maximum quotas**

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

FRU_RSA.1/Public Maximum quotas

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

5.1.4 Class FMT: Security Management

FMT_MSA.1/Folder Management of security attributes

FMT_MSA.1.1/Folder The TSF shall enforce the [Discretionary Access Control SFP] to restrict the ability to *query, modify* the security attributes [Access Control Lists of folder, Owner of the folder] to [Authorized Administrator and the owner of the folder].

Application Note: While the management of attributes of security policies and their default values is usually done by the Operating System (see chapter 5.3.3) the TOE controls the ability to query and modify the Access Control Lists of folders.

FMT_MSA.3/Folder Static attribute initialization

FMT_MSA.3.1/Folder The TSF shall enforce the [Discretionary Access Control SFP] 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,
- for *public folders,* default ACLs allow full access for the corresponding Folder Owner, allow other users to read and create items and subfolders.]

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

FMT_MSA.3/Group	**Static attribute initialization**
FMT_MSA.3.1/Group	The TSF shall enforce the [Distribution Group Restriction SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Group	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.
Application Note:	Here “permissive” means that no Access Control Lists are specified and the restricted access flag is set.

FMT_MSA.3/Connect	**Static attribute initialization**
FMT_MSA.3.1/Connect	The TSF shall enforce the [Connection Filtering SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Connect	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/SRL	**Static attribute initialization**
FMT_MSA.3.1/SRL	The TSF shall enforce the [Sender Reputation SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/SRL	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.
Application Note:	Here “permissive” means an SRL threshold of “7”.

FMT_MSA.3/Message	**Static attribute initialization**
FMT_MSA.3.1/Message	The TSF shall enforce the [Message Filtering SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Message	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/AttachmentFilter	**Static attribute initialization**
FMT_MSA.3.1/AttachmentFilter	The TSF shall enforce the [Attachment SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AttachmentFilter	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Transport	**Static attribute initialization**
FMT_MSA.3.1/Transport	The TSF shall enforce the [Hub Transport SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Transport	The TSF shall allow ~~the~~ [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: In the context of this ST, the functionality required by FMT_MSA.3.2/x shall be seen in the way that the TOE does not provide any functionality to change the default values rather than restricting the access to such functionality.

FMT_SMF.1	**Specification of management functions**
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 SFP (FDP_ACC.1/Folder)

b) Management of security attributes for the Distribution Group Restriction SFP (FDP_ACC.1/Group)

c) Management of security attributes for the Message Filtering SFP (FDP_IFF.1/Message)

d) Management of security attributes for the Connection Filtering SFP(FDP_IFF.1/Connect)

e) Management of security attributes for the Sender Reputation SFP (FDP_IFF.1/SRL)

f) Management of security attributes for the Attachment SFP (FDP_IFF.1/AttachmentFilter)

g) Management of security attributes for the Hub Transport SFP (FDP_IFF.1/Transport)

h) Management of maximum values for quotas on mailbox and public folder sizes (FRU_RSA.1/Mail and FRU_RSA.1/Public).

i) Management of attributes for authentication via Outlook Voice Access (FIA_UAU.8(EXP))

j) Management of quality metric for user PINs (FIA_SOS.1)].

5.2 TOE Security Assurance Requirements

Table 6 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 6 – TOE Security Assurance Requirements

SAR ID	SAR name
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_FLR.3	Systematic flaw remediation procedures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

5.3 Security Requirements for the IT Environment

The environment satisfies the SFRs delineated in Table 7. 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 7 - Security Requirements for the IT Environment

Class FDP: User Data Protection	
FDP_ACC.1/ENV	Subset access control
FDP_ACF.1/ENV	Security attribute based access control
Class FIA: Identification and authentication	
FIA_UAU.8(EXP)/ENV	User subset authentication before any action
FIA_UID.3(EXP)/ENV	User subset identification before any action
FIA_ATD.1	User attribute definition
Class FMT: Security Management	
FMT_MSA.1/Group	Management of security attributes
FMT_MSA.1/Connect	Management of security attributes
FMT_MSA.1/SRL	Management of security attributes
FMT_MSA.1/Message	Management of security attributes
FMT_MSA.1/AttachmentFilter	Management of security attributes
FMT_MSA.1/Transport	Management of security attributes
FMT_SMR.1	Security roles

5.3.1 Class FDP: User Data Protection

FDP_ACC.1/ENV Subset access control

FDP_ACC.1.1/ENV 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].

FDP_ACF.1/ENV Security attribute based access control

FDP_ACF.1.1/ENV 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, ADAM and Active Directory** objects based on [

subject attribute –security ID of the user and its corresponding group IDs

object attributes – Access Control List].

FDP_ACF.1.2/ENV 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 Control List for the accessing subject, the accessing subject is able to perform the specified operation].

FDP_ACF.1.3/ENV 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 ID belongs to an authorized subject.

The owner is always allowed to change permissions.

Authorized Administrators are always allowed to take ownership.]

FDP_ACF.1.4/ENV The **IT environment** shall explicitly deny access of subjects to objects based on the **following additional rules**: [none].

5.3.2 Class FIA: Identification and authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The **IT environment** shall maintain the following list of security attributes belonging to individual users: [

SID (user's identity)

Group Memberships

Authentication Data

Privileges,

Mailbox number (If OVA is enabled for user)].

Application Note: The secret for OVA is part of the authentication data and stored in the environment but maintained by the TOE.

FIA_UAU.8(EXP)/ENV User subset authentication before any action

FIA_UAU.8(EXP).1/ENV The **IT environment** shall require each user connecting via [RPC, SMTP, HTTP, RPC over HTTP, Web Services, TLS-secured OVA] to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.3(EXP)/ENV User subset identification before any action

FIA_UID.3(EXP).1/ENV The **IT environment** shall require each user connecting via [RPC, SMTP, HTTP, RPC over HTTP, Web Services, TLS-secured OVA] to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.3.3 Class FMT: Security Management

FMT_MSA.1/Group Management of security attributes

FMT_MSA.1.1/Group The **IT environment** shall enforce the [Distribution Group Restriction SFP] to restrict the ability to *query, modify* the security attributes [Restricted access flag, Access Control Lists] to [Authorized Administrator].

FMT_MSA.1/Connect	**Management of security attributes**
FMT_MSA.1.1/Connect	The **IT environment** shall enforce the [Connection Filtering SFP] to restrict the ability to *query, modify* the security attributes [allow lists, block lists and list of exceptional recipients of the Edge Transport Server Role] to [Authorized Administrator].
FMT_MSA.1/SRL	**Management of security attributes**
FMT_MSA.1.1/SRL	The **IT environment** shall enforce the [Sender Reputation SFP] to restrict the ability to *query, modify* the security attributes [SRL Threshold Configuration, local list of SRL values, time to add server to local block list] to [Authorized Administrator].
FMT_MSA.1/Message	**Management of security attributes**
FMT_MSA.1.1/Message	The **IT environment** shall enforce the [Message Filtering SFP] to restrict the ability to *query, modify* the security attributes [sender and recipient filtering lists, local address book] to [Authorized Administrators].
FMT_MSA.1/AttachmentFilter	**Management of security attributes**
FMT_MSA.1.1/AttachmentFilter	The **IT environment** shall enforce the [Attachment SFP] to restrict the ability to *query, modify* the security attributes [Attachment Policy] to [Authorized Administrator].
FMT_MSA.1/Transport	**Management of security attributes**
FMT_MSA.1.1/Transport	The **IT environment** shall enforce the [Hub Transport SFP] to restrict the ability to *query, modify* the security attributes [Hub transport policy] to [Authorized Administrators].
FMT_SMR.1	**Security roles**
FMT_SMR.1.1	The **IT environment** shall maintain the roles [Exchange Organization Administrators, Exchange Recipient Administrators, Exchange View-Only Administrators, ExchangeLegacyInterop group, Windows Users].
FMT_SMR.1.2	The **IT environment** shall be able to associate users with roles.
Application Note:	In the context of this ST, the term Authorized Administrator refers to a group of users which comprise the predefined Exchange and Windows administrators. This includes any user

who is allowed to perform a management operation because permission has been granted to him by assigning him to a role with administrator permissions or by granting him the ability to perform an administrative operation explicitly. In this context, all roles that are listed in FMT_SMR.1 represent the group of Authorized Administrators.

5.4 Minimum Strength of Function (SOF) for the TOE

There is only one SFR in the chapter 5.1 for which a SOF-claim is applicable: FIA_UAU.8(EXP). The SOF level for this SFR is defined to be **SOF-medium**.

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.

6.1 TOE Security Functions

This chapter presents the security functions performed by the TOE to satisfy the identified SFRs in chapter 5. Traceability to SFRs is also provided. As stated in chapter 5.4 above, the SOF claim for the TOE is **SOF-Medium**.

The only Security Functions with a SOF-Claim is SF.I&A. The other functions are not based on probabilistic or permutational mechanisms.

6.1.1 Security Management (SF.SM)

Exchange Server 2007 provides management of the TOE through the Exchange Management Shell. The Exchange Management Shell is a task-based command line shell and scripting language for system administration. It exposes all administration functionality necessary for the administering the TOE.

Exchange server security management configuration data and mail recipient data is stored in the Active Directory or the local file system. Ability to read and modify those objects and attributes is controlled through Access Control Lists.

As the Edge Transport Server Role has no direct access to the Active Directory, the Hub Server maintains the required configurations (block lists etc) from the Active Directory to the Active Directory Application Mode (ADAM) service running on the Edge Transport Server Role.

The different types of users/roles exposed to the TOE are domain users that have Exchange mailboxes as well as the following Exchange specific Windows groups:

- ExchangeLegacyInterop group (This group exists for interoperability with Exchange 2003 servers within the same forest),
- Exchange Organization Administrators (Users in this group have permission to read and modify all Exchange configuration data),
- Exchange Recipient Administrators (Users in this group can manage Exchange user attributes in Active Directory and perform select mailbox operations) and
- Exchange View-Only Administrators (Users in this group have permission to read all Exchange configuration information but cannot modify this information).

Exchange 2007 is a directory-enabled application, and as such, an Authorized Administrator (e.g. the Exchange Organization Administrator that has an administrative role in the environment) can choose to delegate administrative tasks for specific servers and specific jobs to IT staff using role-based management. For example, recipient management tasks like creating mailboxes and setting storage quotas can be delegated to administrators without permitting those administrators access to other administration tasks and information.

SF.SM will specifically provide the following management functionality for the other Security Functions:

6.1.1.1 Security Management for Access Control

The TOE will provide functionality to manage the Access Control Lists of folders (within mailboxes and Public Folders). This functionality allows Authorized Administrators to grant or revoke permissions to other users.

6.1.1.2 Security Management for Connection Filtering

The TOE will provide functionality to

- Manage local allow and block lists,
- manage the list of exceptional recipients,
- manage the use of remote block and allow lists,
- manage the use of the list of local SRL values,
- configure SRL threshold settings and the period of time for which servers exceeding the threshold will be added to the block list.

6.1.1.3 Security Management for Message Filtering

The TOE will provide functionality to manage sender and recipient filtering lists.

6.1.1.4 Security Management for Attachment Filtering

The TOE will provide functionality to manage the Attachment Filtering Policy. This functionality will allow Authorized Administrators to add or delete rules to the Attachment Filtering Policy.

6.1.1.5 Security Management for Transport Filtering

The TOE will provide functionality to manage the Hub Transport Policy. This functionality will allow Authorized Administrators to add or delete rules to the Hub Transport Policy.

6.1.1.6 Security Management for Identification and Authentication

The TOE will provide functionality to manage the attributes of users for Outlook Voice Access. Specifically this will allow Authorized Administrators to manage the quality metric for Outlook Voice Access PINs.

6.1.1.7 Security Management for Distribution Group Restriction

The TOE will provide functionality to

- Create and delete distribution groups
- Modify the restricted access flag for a distribution group
- Modify the Access Control Lists for a distribution group

6.1.1.8 Security Management for Mailbox and Public Folder Quota

The TOE will provide functionality to change the quota settings for public folders and mailboxes.

Note: Default security attributes applied to newly created mailboxes or top level public folders are predefined and cannot be changed. There are no default security attributes for subfolders. During creation of a subfolder, it inherits the security attributes of its parent folder.

Functional Requirements Satisfied: FMT_SMF.1

6.1.2 Access Control (SF.AC)

SF.AC controls access of users (via client software) to the two types of Exchange Server 2007 data stores: mailboxes – also known as private stores – that are associated with an individual mailbox-enabled user and public folders that store shared folders and documents. This access control function covers all items that are stored in mailboxes and public folders, including e-mails, contact data, calendar data, complete folders and certificates.

SF.AC utilizes Access Control Lists (ACLs) on folders stored in public folders and mailboxes (private folders)) to control access along with Windows permissions that are specific to Exchange. All folders in mailboxes and public folders have Access Control Lists that define the level of access for all objects stored in that folder. However, when communicating with MAPI-based client applications such as Microsoft Outlook, Exchange 2007 converts the ACL permissions to MAPI permissions when transmitting the permissions to Outlook. If the user modifies the ACL permissions, Exchange converts them back to Windows permissions prior to saving them.

Mailbox access: By default, the mailbox owner can read, write, or create new items or folders in their own mailbox – other users have no access. The mailbox owner can grant other users access to the entire mailbox, folders within the mailbox or messages within a folder. These users' rights in the mailbox may include permissions to to send and receive mail as if they were the mailbox owner.

The following user relevant permissions on a mailbox are maintained by access control:

- FullAccess (Provides full access to all items in the mailbox)
- SendAs (Allows a user to send messages that appear as if they were coming from the mailbox owner)
- ExternalAccount (Allows a user to associate an external account with the mailbox)
- DeleteItem (Allows a user to delete items in the mailbox)
- ReadPermission (Allows a user to read permissions in the mailbox)
- ChangePermission (Allows a user to change permissions of items)
- ChangeOwner (Allows a user to change the mailbox owner)

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 only the Folder Owner has full access. The Folder Owner can grant permissions to other users. The following permissions on public folders are maintained by the access control function:

- ReadItems (Allows a user to read items in the public folder)
- CreateItems (Allows a user to create items in the public folder)
- EditOwnedItems (Allows a user to edit items they own in the public folder)
- DeleteOwnedItems (Allows a user to delete items they own in the public folder)
- EditAllItems (Allows a user to edit all items in the public folder)
- DeleteAllItems (Allows a user to delete any item in the public folder)
- CreateSubfolders (Allows a user to create subfolders in the public folder)

- FolderOwner (Makes a user the owner of a public folder. The user then has the ability to view and move the public folder. The user cannot read items, edit items, delete items, or create items in the public folder.)
- FolderContact (Makes a user the contact for a public folder)
- FolderVisible (Allows users to view the public folder)

The Access Control Lists for both public folders and mailboxes are stored in database files. This Security Function also limits the ability to query and modify the Access Control Lists to authorized administrators and the mailbox or public folder owners.

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 (i.e. the ACL of the folder that the object resides in).

Functional Requirements Satisfied: FDP_ACC.1/Folder, FDP_ACF.1/Folder, FMT_MSA.1/Folder, FMT_MSA.3/Folder

6.1.3 Connection Filtering (SF.CF)

SF.CF will reject SMTP connections based on IP address of the connecting external SMTP server[15]. To do so, SF.CF references allow lists, block lists and a list of exceptional recipients. These lists which may contain IP addresses or IP address ranges. The TOE references local and remote allow and block lists. Local lists are defined by an Authorized Administrator while remote allow and block lists are retrieved from external service providers (so called block list service providers).

When an SMTP connection is established, SF.CF enforces the following ordered rules, according to the IP address of the external SMTP server:

1. If the IP address of the sending SMTP server is listed on a local allow list, the message will be accepted;
2. If the IP address of the sending SMTP server is listed on a local block list, the message will be rejected;
3. If the IP address of the sending SMTP server is listed on a remote allow list, the message will be accepted;
4. If one of the recipients of the e-mail is on the local list of exception recipients, the message will be accepted;
5. If the IP address of the sending SMTP server is listed on a remote block list, the message will be rejected;
6. Else the message will be accepted.

By default, the local allow and block lists that are used in this Security Function are empty.

The TOE also calculates the Sender Reputation Level (SRL) of a remote SMTP server after at least 20 mails have been received from this server. This SRL is a numeric value between 0 and 9 that serves as an indicator of how likely the sending server is a spammer.

[15] An external SMTP server is an SMTP server logically outside the Exchange organization that connects to an Edge Server.

Further, the environment of the TOE maintains a local list of SRL values for known SMTP servers. This list is updated on a regular basis.

If the local SRL for a sending SMTP server or the calculated SRL has reached or exceeded an administrator configurable value (the SRL Threshold which is 7 by default), the SMTP server will be added to the local block list for an administrator defined period of time.

Functional Requirements Satisfied: FDP_IFC.1/Connect, FDP_IFC.1/SRL, FDP_IFF.1/Connect, FDP_IFF.1/SRL , FMT_MSA.3/SRL, FMT_MSA.3/Connect

6.1.4 Message filtering (SF.MF)

SF.MF allows the administrators to configure the TOE to reduce spam received by an organization.

Message Filter:

The Message Filter will accept or reject messages based on the rules of the following policies. By default, messages will be accepted by this policy.

Messages will be rejected if:

- the sender listed in the MAIL FROM: field of the RFC 2821 message envelope is on the sender filtering list or
- the sender in the FROM header of the message (RFC 2822) is on the sender filtering list or
- the MAIL FROM: field of the RFC 2821 message envelope is blank[16] and the FROM header of the message (RFC 2822) does not contain a valid email address
- the recipient listed in the RCPT TO: field of the RFC 2821 message envelope is on the recipient filtering list or
- the recipient does not exist in the local address book

Finally, the TOE evaluates the SPF record for the sending domain and stamps the result on the message. This SPF record is published by domain servers in addition to their standard DNS information and identifies the machines that are allowed to send emails on behalf of the domain. In this way, the SPF record can help to identify forged addresses.

By default, the sender and recipient filtering list for this Security Function are empty.

Functional Requirements Satisfied: FDP_IFC.1/Message, FDP_IFF.1/Message, FMT_MSA.3/Message

[16] As this field can never be completely empty the term blank refers to a so called null address which is a MAIL FROM field that contains only the characters "<>"

6.1.5 Attachment Filtering (SF.AF)

The TOE applies an attachment filter to incoming mail based on the e-mail attachments.

The TOE provides the administrator the ability to specify that messages that contain a specified attachment or attachment type be subject to a predefined action. The Administrator can choose to block the whole message while optionally advising the sender that the message was not delivered, or remove the attachment and deliver the message. This policy is defined by the administrator based on the Attachment MIME Type or the Attachment extension.

The default policy is to remove all attachments of the following MIME types and extensions:

MIME Type: application/x-msdownload, message/partial, text/scriptlet, application/prg, application/msaccess, text/javascript, application/x-javascript, application/javascript, x-internet-signup, application/hta

Extensions: *.xnk, *.wsh, *.wsf, *.wsc, *.vbs, *.vbe, *.vb, *.url, *.shs, *.shb, *.sct, *.scr, *.scf, *.reg, *.prg, *.prf, *.pif, *.pcd, *.ops, *.mst, *.msp, *.msi, *.psc2, *.psc1, *.ps2xml, *.ps2, *.ps11xml, *.ps11, *.ps1xml, *.ps1, *.msc, *.mdz, *.mdw, *.mdt, *.mde, *.mdb, *.mda, *.lnk, *.ksh, *.jse, *.js, *.isp, *.ins, *.inf, *.hta, *.hlp, *.fxp, *.exe, *.csh, *.crt, *.cpl, *.com, *.cmd, *.chm, *.bat, *.bas, *.asx, *.app, *.adp, *.ade,

Functional Requirements Satisfied: FDP_IFC.1/AttachmentFilter, FDP_IFF.1/AttachmentFilter, FMT_MSA.3/AttachmentFilter

6.1.6 Transport Filtering (SF.TF)

The TOE allows an administrator to configure a set of ordered rules that can be applied to all messages passing through the Hub Transport server role. The Hub server will evaluate all the rules in order and execute any rules that apply. By default, no rules exist for this policy initially.

The administrator can define rules for messages based on the following attributes of an email:

- Sender
- Recipients
- CC:
- Subject
- Classification
- Header
- Attachment Name
- Attachment Size
- Attachment extension
- Importance
- Key words in Subject or email body

Functional Requirements Satisfied: FDP_IFC.1/Transport, FDP_IFF.1/Transport, FMT_MSA.3/Transport

6.1.7 Identification and Authentication (SF.I&A)

The TOE will identify and authenticate all users connecting via non-TLS secured Outlook Voice Access.

The identity of the user in the context of this Security Function is represented by the user's mailbox number or a telephone number that is transmitted from the PBX to the TOE (caller ID). When a user initiates a phonecall to OVA, the TOE references the associated Caller Id that is transmitted from the PBX as an additional mechanism to identify the user. If the Caller Id matches a user, the user does not have to enter their mailbox number, but still must enter their PIN prior to gaining access to any TOE resources[17]. If the Caller ID is not transmitted or the transmitted number has not been assigned to a mailbox, the user is asked to enter their mailbox number. After this identification, the user is asked to enter their PIN for authentication. After successful authentication, the TOE associates the calling user with their corresponding Windows user account and the corresponding roles.

Please note that if the PBX establishes a connection over mutually authenticated TLS the authentication is not enforced as the environment is responsible for user authentication in this case.

Further, the TOE will ensure that PINs generated by administrators, the user or the TOE itself meet a quality metric as defined by the administrator based on:

- The number of digits of the PIN
- The history of the last PINs
- Common patterns

[17] Please note that the caller ID and the mailbox number are only mechanisms for the TOE to map the calling user to their corresponding ID.

The TOE specifically ensures that a PIN has at least a length of 8 digits.

After the user has been successfully authenticated, the user's identity is used to control the user's access to data to ensure that one user can not access other user's data via this interface.

Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.8(EXP), FIA_UID.3(EXP), FIA_USB.1.

6.1.8 Distribution Group Restriction (SF.DGR)

SF.DGR restricts usage of distribution groups by the following security attributes: restricted access flag, the send ACL for the distribution group, the sender's ID (the latter is the ID of user or its associated groups).

SF.DGR will block a message sent to a distribution group, if

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

For newly created distribution groups, the restricted access flag is set and no Access Control Lists are specified.

Functional Requirements Satisfied: FDP_ACC.1/Group, FDP_ACF.1/Group, FMT_MSA.3/Group

6.1.9 Mailbox and public folder quota (SF.QTA)

SF.QTA allows the Administrator to set three size restriction quota levels 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 save messages sent by the mailbox owner. When the mailbox reaches the *send-and-receive quota*, SF.QTA will refuse to accept new messages or to messages sent by the mailbox owner.

NDRs (Non Delivery Reports) and voice messages that are generated by the TOE will be accepted after a mailbox has reached the send-and-receive quota. However, once the send-and-receive quota is exceeded by more than 10%, those types of messages will also be blocked.

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

Functional Requirements Satisfied: FRU_RSA.1/Mail, FRU_RSA.1/Public

6.2 Assurance Measures

For the evaluation of the TOE, the assurance requirements according to CC EAL4 augmented by 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 8 below (N.B. Some of the documentation listed therein is not prepared yet, therefore currently corresponding document titles and versions are not available).

Table 8 - 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
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	Performance of SOF analysis,
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 PPs.

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 for the TOE is SOF-medium.

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

8.1 TOE Security Objectives Rationale

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

Table 9 - Security Objectives Rationale for the TOE

Threat	Objectives	Rationale
T.UNAUTH_DAC	O.DAC O.I&A OE.PLATFORM	• O.DAC (discretionary access control concerning mailboxes and public folders) directly counters T.UNAUTH_DAC. • T.UNAUTH_DAC deals with adversaries trying to access information contained in mailboxes to which they are not authorized. O.DAC counters this threat by providing discretionary access on these objects. • O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. • OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted

Threat	Objectives	Rationale
		Outlook Voice Access connection. • The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user for access control.
T.AUTH_DAC	O.DAC O.I&A OE.PLATFORM	• O.DAC (discretionary access control concerning mailboxes and public folders) directly counters T.AUTH_DAC of unauthorized access to mailboxes. • T.AUTH_DAC deals with adversaries trying to access information contained in mailboxes to which they are not authorized. O.DAC counters these threats by providing discretionary access on these objects. • O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. • OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection. • The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user for access control.
T.UNAUTHUSE	O.DAC O.I&A OE.PLATFORM	• O.DAC (discretionary access control concerning mailboxes and public folders) counters the threat T.UNAUTHUSE of unauthorized access to public folders. • T.UNAUTHUSE deals with adversaries trying to access information contained in mailboxes or public folders to which they are not authorized. O.DAC counters this threat by providing discretionary access on these objects. • O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non

Threat	Objectives	Rationale
		TLS-secured OVA. • OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection.
T.SPAM	O.CONBLK	• O.CONBLK (blocking of SMTP connections from IP addresses of suspected spammers) directly traces back to T.SPAM. • Blocking connections from suspected UCE 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.REDUCE_SPAM, see below).
	O.REDUCE_SPAM	• Blocking messages with suspected 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.REDUCE_SPAM (the other aspect of T.SPAM about known IP addresses of UCE origin is countered by O.CONBLK. See above).
T.DL_MISUSE	O.RESTDIST O.I&A OE.PLATFORM	• O.RESTDIST (access control for distribution groups) directly addresses T.DL_MISUSE. • T.DL_MISUSE defines misuse of distribution groups as a threat. O.RESTDIST counters this threat by allowing the administrator to restrict the use of a distribution group to only those users that have been authenticated and/or – optionally – identify users who are explicitly authorized to use a distribution group. • O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. • OE.PLATFORM provides the

Threat	Objectives	Rationale
		mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection. • The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user to enforce the policy as defined in O.RESTDIST.
T.OVERFLOW	O.QUOTA	• O.QUOTA (limitation of mailbox and public folder sizes) directly traces back to T.OVERFLOW. • T.OVERFLOW is countered by O.QUOTA as the administrator can limit the size of mailboxes and public folders. By doing so, O.QUOTA limits the amount of resources necessary to support the mailbox and public folder, respectively.
OSP.MAIL_FLOW	O.MAIL_FLOW	The OSP.MAIL_FLOW is directly and completely addressed by the Security Objective O.MAIL_FLOW. The OSP as well as the Objective define that an administrator shall be able to control email flow within their organization and use the same set of email characteristics for this functionality

8.2 Environmental Security Objectives Rationale

This chapter demonstrates that all assumptions are covered by the security objectives of the environment and shows how the objectives for the environment can be traced back to assumptions.

Table 10 - Security Objectives Rationale for the Environment

Assumption	Objectives	Rationale
A.COM_PROT	OE.COM_PROT	OE.COM_PROT is a re-statement of A.COM_PROT requiring protection by of the communication.
A.INSTALL	OE.INSTALL	A.INSTALL is restated in (the first paragraph of) OE.INSTALL.
A.PLATFORM	OE.PLATFORM OE.INSTALL	OE.PLATFORM is a re-statement of the IT aspects of A.PLATFORM requiring a certain Operation System include a specific functionality to support the operation of the TOE. The Non-IT aspects of A.PLATFORM are restated in OE.INSTALL.
A.BLOCKLIST	OE.BLOCKLIST	OE.BLOCKLIST is a re-statement of A.BLOCKLIST.
A.NO_EVIL_ADMIN	OE.INSTALL	The aspects of A.NO_EVIL_ADMIN are implicitly contained in OE.INSTALL
A.PHYS_PROTECT	OE.PHYSICAL	OE.PHYSICAL is a re-statement of A.PHYS_PROTECT, protecting the system the TOE is running on from unauthorized modification or tampering.

8.3 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).

8.3.1 TOE SFR Rationale

Table 11 – TOE Objectives to SFRs Rationale

Objective	SFR(s)	Rationale
O.DAC	FDP_ACC.1/Folder FDP_ACF.1/Folder FMT_MSA.1/Folder FMT_MSA.3/Folder FMT_SMF.1	Discretionary access control for user access to mailboxes and public folders is directly supported by access control components FDP_ACC.1/Folder and FDP_ACF.1/Folder. FMT_MSA.1/Folder ensures that access control is also provided for the attributes that are utilized for this policy. FMT_MSA.3/Folder ensures that appropriate default values are used for all attributes of this policy. Eventually, FMT_SMF.1 ensures that the TOE provides management functionality to query and modify the attributes of the access control policy.
O.CONBLK	FDP_IFC.1/Connect FDP_IFF.1/Connect FDP_IFC.1/SRL FDP_IFF.1/SRL FMT_MSA.3/Connect FMT_MSA.3/SRL FMT_SMF.1	O.CONBLK is represented by the SFRs FDP_IFC.1/Connect and FDP_IFF.1/Connect, which build an information flow policy for connection blocking based on allow and block lists and FDP_IFC.1/SRL and FDP_IFF.1/SRL, which build an information flow policy based on the “Sender Reputation Level” that determines the likelihood of a sender being a spammer. Support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3/Connect resp. FMT_MSA.3/SRL to ensure appropriate default values for the policies.
O.RESTDIST	FDP_ACC.1/Group FDP_ACF.1/Group FMT_MSA.3/Group FMT_SMF.1	O.RESTDIST is represented by the SFRs FDP_ACC.1/Group and FDP_ACF.1/Group , which form an access control policy for distribution groups to restrict the ability of users to send emails to Distribution Groups. FMT_MSA.3/Group ensures that appropriate default values are used for all attributes of this policy. Eventually, FMT_SMF.1 ensures that the TOE provides management functionality to query and modify the attributes of the policy.

Objective	SFR(s)	Rationale
O.REDUCE_SPAM	FDP_IFC.1/Message FDP_IFF.1/Message FMT_MSA.3/Message FMT_SMF.1	O.REDUCE_SPAM is represented by the SFRs FDP_IFC.1/Message and FDP_IFF.1/Message, which form an information flow policy to filter e-mail based on the RCPT TO: and MAILFROM fields of the RFC 2821 envelope and the RFC 2822 header of the email. Indirect support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3/Message to ensure that appropriate default values are provided.
O.MAIL_FLOW	FDP_IFC.1/AttachmentFilter FDP_IFF.1/AttachmentFilter FDP_IFC.1/Transport FDP_IFF.1/Transport FMT_MSA.3/AttachmentFilter FMT_MSA.3/Transport FMT_SMF.1	O.MAIL_FLOW is represented by a combination of two information flow policies. FDP_IFC.1/AttachmentFilter and FDP_IFF.1/ AttachmentFilter allow e-mail attachment filtering already on the Edge Transport Server Role of the TOE while FPP_IFC.1/Transport and FDP_IFF.1/Transport allow the administrator to specify rules for e-mail transport on the hub server role based on characteristics of the e-mail. Support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3/AttachmentFilter resp. FMT_MSA.3/Transport to ensure that appropriate default values are provided.
O.QUOTA	FRU_RSA.1/Mail FRU_RSA.1/Public FMT_SMF.1	O.QUOTA is represented by a combination of FRU_RSA.1/Mail, which specifies the quota for mailboxes and FRU_RSA.1/Public, which specifies the quota for public folders. Indirect support is provided by FMT_SMF.1 components from the FMT class, to enable management of the security attributes used by this policy.

Objective	SFR(s)	Rationale
O.I&A	FIA_UAU.8(EXP) FIA_UID.3(EXP) FIA_USB.1 FIA_SOS.1 FMT_SMF.1	O.I&A requires the identification and authentication of users that connect to the TOE via a non TLS OVA session (for the rest of the cases the environment is responsible for identification and authentication). This identification and authentication mechanism for non TLS-secured Outlook Voice Access is defined in FIA_UID.3(EXP) and FIA_UAU.8(EXP). FIA_USB.1 defines the security attributes for subjects that are used to bind subjects to their users. Finally, FIA_SOS.1 ensures that the PINs for Outlook Voice Access follow a quality metric to reduce the likelihood that an attacker can guess the PIN of a user. Indirect support is provided by FMT_SMF.1 components from the FMT class to enable management of the security attributes used by this policy.

As can be seen by the above rationale, all TOE security objectives are covered by the TOE SFRs.

8.3.2 Environment SFR Rationale

Table 12 – Environment IT Objectives to SFRs Rationale

Objective	SFR(s)	Rationale
OE.PLATFORM	FIA_UAU.8(EXP)/ENV FIA_UID.3(EXP)/ENV FIA_ATD.1 FDP_ACC.1/ENV FDP_ACF.1/ENV FMT_MSA.1/Group FMT_MSA.1/Connect FMT_MSA.1/SRL FMT_MSA.1/Message FMT_MSA.1/AttachmentFilter FMT_MSA.1/Transport FMT_SMR.1	The IT aspects of OE.PLATFORM require the underlying Operating System to provide functionality to support the operation of the TOE. • Access Control for access of users to files in the Windows files system is defined by FDP_ACC.1/ENV and FDP_ACF.1/ENV. • Functionality for enforcing and supporting Identification and Authentication of users is defined by FIA_UAU.8(EXP)/ENV, FIA_UID.3(EXP)/ENV. FIA_ATD.1. The identification and authentication mechanism for protocols that are part of the TOE (except non TLS-encrypted Outlook Voice Access) is defined in FIA_UID.3(EXP)/ENV and FIA_UAU.8(EXP)/ENV. FIA_ATD.1 defines the user attributes that have to be maintained for users in the environment. • Methods to store and manage TSF data for the TOE are defined by the following management requirements: o FMT_MSA.1/Group o FMT_MSA.1/Connect o FMT_MSA.1/SRL o FMT_MSA.1/Message o FMT_MSA.1/AttachmentFilter o FMT_MSA.1/Transport o FMT_SMR.1

The environmental objectives OE.COM_PROT, OE.INSTALL, OE.BLOCKLIST and OE.PHYSICAL do not contain any direct IT aspects and as such are not mapped to SFRs of the environment.

8.3.3 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 environmental risk because the TOE is in a protected space where it is under supervision. Agents cannot physically access the TOE and have no means of physically 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.

As stated in Chapter 3, the TOE is intended to be used in cases where there is a low attack potential due to asset value, environmental protection, and resulting attacker motivation and capabilities.

Therefore, Evaluation Assurance Level 4 is appropriate, as it contains the 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.

The explicit requirements that are used in this Security Target (see chapter 9.1) have been developed in close dependence on existing criteria in part II of Common Criteria. As such no specific assurance requirements are considered being necessary in order to support those explicit requirements. Instead the aforementioned assurance level is considered being sufficient to support the evaluation of those explicit requirements.

8.3.4 TOE SFR and SAR Dependencies Rationale

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

Table 13 - SFR Dependencies Status

SFR ID	Dependency	Satisfied by the use of
FDP_ACC.1/Folder	FDP_ACF.1	FDP_ACF.1/Folder
FDP_ACC.1/Group	FDP_ACF.1	FDP_ACF.1/Group
FDP_ACF.1/Folder	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Folder and FMT_MSA.3/Folder
FDP_ACF.1/Group	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Group and FMT_MSA.3/Group
FDP_IFC.1/Connect	FDP_IFF.1	FDP_IFF.1/Connect
FDP_IFC.1/SRL	FDP_IFF.1	FDP_IFF.1/SRL
FDP_IFC.1/Message	FDP_IFF.1	FDP_IFF.1/Message
FDP_IFC.1/AttachmentFilter	FDP_IFF.1	FDP_IFF.1/AttachmentFilter
FDP_IFC.1/Transport	FDP_IFF.1	FDP_IFF.1/Transport
FDP_IFF.1/Connect	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Connect and FMT_MSA.3/Connect
FDP_IFF.1/SRL	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/SRL and FMT_MSA.3/SRL
FDP_IFF.1/Message	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Message and FMT_MSA.3/Message
FDP_IFF.1/AttachmentFilter	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/AttachmentFilter and FMT_MSA.3/AttachmentFilter
FDP_IFF.1/Transport	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Transport and FMT_MSA.3/Transport
FIA_SOS.1	-	
FIA_UAU.8(EXP)	FIA_UID.3(EXP)	FIA_UID.3(EXP)
FIA_UID.3(EXP)	-	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1 (in the environment)
FRU_RSA.1/Mail	-	
FRU_RSA.1/Public	-	
FMT_MSA.1/Folder	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Folder, FMT_SMF.1 and FMT_SMR.1 (in the environment)
FMT_MSA.3/Folder	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Folder and FMT_SMR.1 (FMT_SMR.1 in the environment)
FMT_MSA.3/Group	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Group and FMT_SMR.1 (both in the environment)
FMT_MSA.3/Connect	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Connect and FMT_SMR.1 (both in the environment)
FMT_MSA.3/SRL	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/SRL and FMT_SMR.1(both in the environment)
FMT_MSA.3/Message	FMT_MSA.1	FMT_MSA.1/Message and

SFR ID	Dependency	Satisfied by the use of
	FMT_SMR.1	FMT_SMR.1(both in the environment)
FMT_MSA.3/AttachmentFilter	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/AttachmentFilter and FMT_SMR.1(both in the environment)
FMT_MSA.3/Transport	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Transport and FMT_SMR.1(both in the environment)
FMT_SMF.1	-	

The following table is a cross-reference of the functional components of the IT environment, their related dependencies and how the dependency was satisfied. Therefore, only first level dependencies are considered.

Table 14 - SFR Dependencies Status for the environment

SFR ID	Dependency	Satisfied by the use of
FDP_ACC.1/ENV	FDP_ACF.1	FDP_ACF.1/ENV
FDP_ACF.1/ENV	FDP_ACF.1/ENV is used to fulfill the dependency of FDP_ACC.1. As only dependencies of the first level are considered for the environment these dependencies have not been considered.	
FIA_UAU.8(EXP)/ENV	FIA_UID.3(EXP)	FIA_UID.3(EXP)/ENV
FIA_UID.3(EXP)/ENV	-	-
FIA_ATD.1	-	-
FMT_MSA.1/Group	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1/Group FMT_SMF.1 and FMT_SMR.1
FMT_MSA.1/Connect	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_IFC.1/Connect, FMT_SMF.1 and FMT_SMR.1
FMT_MSA.1/SRL	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_IFC.1/SRL , FMT_SMF.1 and FMT_SMR.1
FMT_MSA.1/Message	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_IFC.1/Message, FMT_SMF.1 and FMT_SMR.1
FMT_MSA.1/AttachmentFilter	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1	FDP_IFC.1/AttachmentFilter , FMT_SMF.1 and FMT_SMR.1

SFR ID	Dependency	Satisfied by the use of
	FMT_SMR.1	
FMT_MSA.1/Transport	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_IFC.1/Transport, FMT_SMF.1 and FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.3(EXP) FIA_UID.3(EXP)/ENV The dependency to FIA_UID.1 is fulfilled by the use of two instances of FIA_UID.3(EXP) (one for the TOE and one for the environment). The combination of these two SFRs ensures that eventually each user is identified before any other actions are allowed on behalf of that user. As such this combination is equivalent to the use of FIA_UID.2. As FIA_UID.2 is hierarchical to FIA_UID.1 the dependency is considered being fulfilled.

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

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

8.3.5 TOE SOF Claim Rationale

The SOF-claim for the TOE is **SOF-medium**.

Based on the definition of the attack potential in Chapter 3, it would have been sufficient to claim it to be SOF-basic as the attacker has only a low attack potential. Additionally, the definitions of SFRs in Chapter 5.1 and the definition of the Security Objectives do not contain any explicit requirement regarding the SOF claim.

However, the ST authors consider that the functions implemented in the TOE are more robust than SOF-Basic. For this reason the author specified the strength of this function to be SOF-medium.

8.3.6 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 8.3.1, 8.3.2 and 8.3.3. 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 the security objectives for the TOE environment.

The security functions of the TOE satisfy the SFRs as shown in Table 15. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 13.

The SARs are appropriate for the assurance level of EAL4 and are satisfied by the TOE as shown in Table 8. 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 8.3.1, 8.3.2 and 8.3.3 are internally consistent. There is no conflict between security functions as described in Chapter 2 and 6 and the SARs to prevent satisfaction of all SFRs.

8.3.7 Extended Functional Requirements Rationale

Chapter 9.1 defines the extended functional components FIA_UAU.8(EXP) (User subset authentication before any action) and FIA_UID.3(EXP) (User subset identification before any action) of the existing functional class FIA (Identification and Authentication).

These components were defined because part II of [CC] does not contain any SFRs which allow specifying a specific *subset* of users that require identification and authentication before any action. As the TOE described in this ST only provides identification and authentication before any action for users connecting via non TLS-secured Outlook Voice Access it was necessary to define these explicit functional requirements. All existing components from class FIA in part II of [CC] cover *each* user and it is not allowed to refine such a component in a way that restricts the group of users that need to be identified and authenticated by the TOE (as a TOE meeting the refined SFR would not automatically also meet the original SFR).

8.4 TOE Summary Specification Rationale

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

8.4.1 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 an explanation of the mapping.

Table 15 – TOE SFRs to Security Functions Rationale

SFR	Security Function(s)	Rationale
FDP_ACC.1/Folder, FDP_ACF.1/Folder	SF.AC	SF.AC fully implements the access policy for the public folders, and mailboxes as required by

SFR	Security Function(s)	Rationale
		FDP_ACC.1/Folder and FDP_ACF.1/Folder. This access control policy covers all objects in mailboxes and public folders. It works based on Access Control Lists that define a relationship between users (or groups), an operation and an object. The access control policy will allow access to an object only if the operation is allowed and not denied for the requesting user in the Access Control List.
FDP_ACC.1/Group, FDP_ACF.1/Group	SF.DGR	SF.DGR fully implements the defined access policy for distribution groups. This access control policy restricts the ability of users to send emails to distribution groups based on Access Control Lists containing allow and deny entries and a restricted access flag that allows only emails by authenticated users.
FDP_IFC.1/Connect FDP_IFF.1/Connect	SF.CF	SF.CF fully implements the required information flow policy for controlling connections to the TOE based on the IP address of the remote SMTP server. It ensures that local and remote allow and block lists as well as a local list of recipient exceptions are utilized to block (with respect to allow) incoming SMTP connections.
FDP_IFC.1/SRL FDP_IFF.1/SRL	SF.CF	SF.CF fully implements the required information flow policy for controlling connections to the TOE based on the Sender Reputation Level. This Security Function ensures that the TOE calculates a Sender Reputation Level for sending SMTP servers (that expresses how likely the sending SMTP server is a spammer) and adds sending SMTP servers that meet or exceed a defined threshold to the local block list for connection filtering.
FDP_IFC.1/Message FDP_IFF.1/Message	SF.MF	SF.MF fully implements the defined information flow policy for delivering messages based on the sender and receiver information contained in the message and the SPF record. It blocks messages based on certain attributes of the e-mail (e.g. the MAIL FROM field) and defines that the TOE is able to evaluate the SPF record of the sending SMTP server and stamps the result of this check to the message.

SFR	Security Function(s)	Rationale
FDP_IFC.1/AttachmentFilter FDP_IFF.1/AttachmentFilter	SF.AF	SF.AF fully implements the defined information flow policy for evaluating messages based on the message attachments. It describes that the TOE will check a set of administrator defined rules for each email. The rules contain criteria based on the MIME type and the attachment's extension. If the criteria of a rule match an attachment, the TOE applies the action of the rule to the message.
FDP_IFC.1/Transport FDP_IFF.1/Transport	SF.TF	SF.TF fully implements the defined information flow policy for delivering messages based on message attributes as defined by the administrator. It describes that the TOE will check a set of administrator defined rules for each e-mail. The rules contain criteria based on the characteristics of the e-mail. If the criteria of a rule meet an e-mail, the TOE applies the action of the rule to the message.
FIA_SOS.1	SF.I&A	SF.I&A fully implements this SFR by ensuring that each OVA user PIN meets a quality metric as defined by the administrator including a minimum length of 8 digits.
FIA_UAU.8(EXP)	SF.I&A	SF.I&A fully implements this SFR by ensuring that each user connecting via non TLS-secured Outlook Voice Access has to be successfully authenticated before allowing any other actions on behalf of that user.
FIA_UID.3(EXP)	SF.I&A	SF.I&A fully implements this SFR by ensuring that each user connecting via non TLS-secured Outlook Voice Access has to be successfully identified before allowing any other actions on behalf of that user.
FIA_USB.1	SF.I&A	SF.I&A fully implements this SFR by ensuring that the TOE is able to maintain the ID of a user for subjects acting on behalf of that user.
FRU_RSA.1/Mail	SF.QTA	FRU_RSA.1/Mail is directly instantiated by SF.QTA as this Security Function defines the quota regulations that apply to mailboxes.
FRU_RSA.1/Public	SF.QTA	FRU_RSA.1/Public is directly instantiated by SF.QTA as this Security Function defines the quota regulations that apply to public folders.

SFR	Security Function(s)	Rationale
FMT_MSA.1/Folder	SF.AC	FMT_MSA.1/Folder specifies that only authorized administrators are allowed to query and modify the Access Control Lists that are associated with a mailbox or public folder. The Security Function SF.AC implements this requirement by controlling access to the Access Control Lists in the same way as access to any object under access control.
FMT_MSA.3/Folder	SF.AC	The default values for the access control policy are defined as part of the Security Function SF.AC
FMT_MSA.3/Group	SF.DGR	The default values for newly created Distribution Groups (restricted access flag is set and Access Control Lists are empty) are defined as part of SF.DGR.
FMT_MSA.3/Connect	SF.CF	The default values for Connection Filtering (empty allow and block lists) are defined as part of SF.CF.
FMT_MSA.3/SRL	SF.CF	The default values for SRL functionality is defined as part of SF.CF.
FMT_MSA.3/Message	SF.MF	The default values (accept all messages per default) for message filtering are defined as part of SF.MF.
FMT_MSA.3/AttachmentFilter	SF.AF	The default values for attachment filtering (block attachments of a certain MIME type or extension) are defined as part of SF.AF.
FMT_MSA.3/Transport	SF.TF	The default values for transport filtering (no rule) are defined as part of SF.TF.
FMT_SMF.1	SF.SM	a) SF.SM describes that the TOE will provide management functions for access control functionality (i.e. for granting and revoking permissions) b) SF.SM provides the management functions for Distribution Groups c) SF.SM provides the configuration of block lists as required by the Message Filtering SFP and provides the configuration of Sender and Recipient filtering d) SF.SM provides the configuration of block and allow lists and block list providers as required by the Connection Filtering SFP e) SF.SM provides the configuration of SRL tolerance and when to add server to block list

SFR	Security Function(s)	Rationale
		f) SF.SM provides the configuration of attachment blocking/stripping policies as required for the Attachment Filtering SFP g) SF.SM provides the configuration of internal transport policies as required for the Hub Transport SFP h) SF.SM allows management of maximum values for quotas on mailbox and public folder sizes i) SF.SM provides the functionality to configure access to users for Outlook Voice Access including the quality settings on users' Outlook Voice Access PINs. As all aspects of the SFR are implemented in the SFs, the SFR as a whole is implemented in the SFs.

In summary, all TOE SFRs are covered by the TOE security functions.

8.4.2 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 8 - Assurance Measures clearly shows that for each assurance requirement, dedicated documentation will be provided and/or appropriate action will be taken (e.g. testing). The listed assurance measures are in principle suitable to meet the assurance requirements.

9 Appendix

9.1 Definition of Extended Functional Requirements

This chapter defines the extended functional components FIA_UAU.8(EXP) (User subset authentication before any action) and FIA_UID.3(EXP) (User subset identification before any action) of the existing functional class FIA (Identification and Authentication).

9.1.1 Definition of FIA_UAU.8(EXP)

The family FIA_UAU is extended by the new component FIA_UAU.8(EXP) as follows:

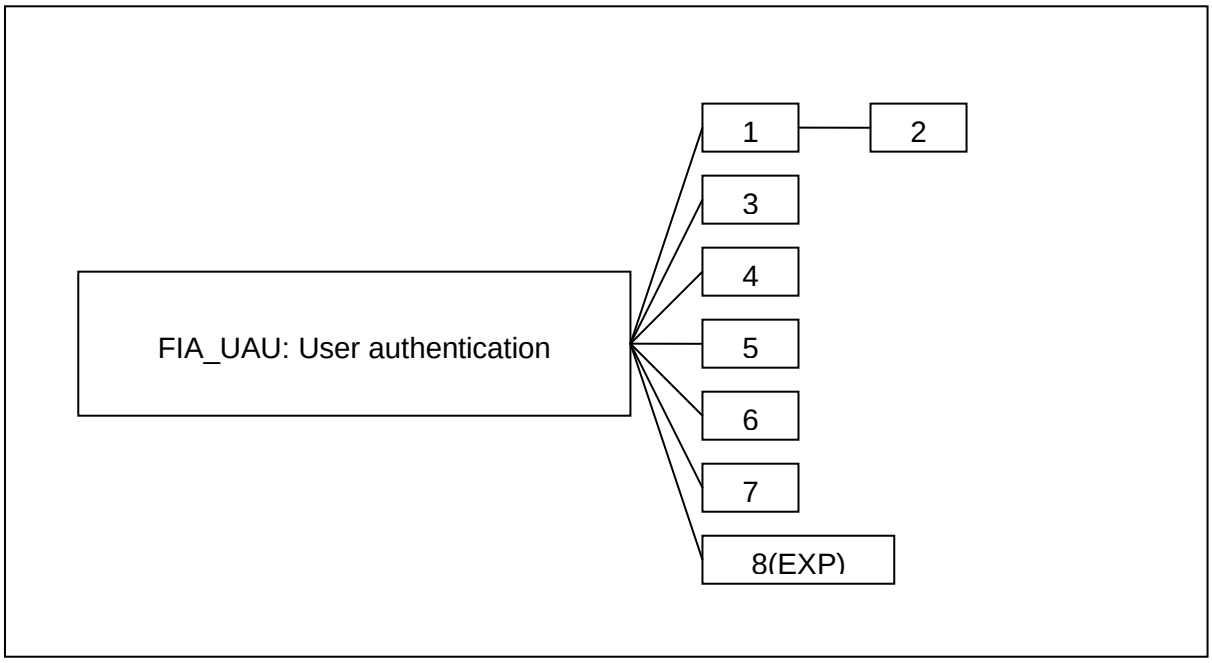


Figure 2 - Component levelling of FIA_UAU.8(EXP)

FIA_UAU.8(EXP) User subset authentication before any action, requires that a subset of users are authenticated before any action will be allowed by the TSF.

Management: FIA_UAU.8(EXP)

The following actions could be considered for the management functions in FMT:

a) management of the authentication data by an administrator;

b) management of the authentication data by the user associated with this data.

Audit: FIA_UAU.8(EXP)

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the authentication mechanism;

b) Basic: All use of the authentication mechanism.

FIA_UAU.8(EXP) User subset authentication before any action

Hierarchical to: No other components
Dependencies: FIA_UID.3(EXP) User subset identification before any action

FIA_UAU.8(EXP).1 The TSF shall require all users connecting via [assignment: *list of connection methods*] to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

9.1.2 Definition of FIA_UID.3(EXP)

The family FIA_UID is extended by the new component FIA_UID.3(EXP) as follows:

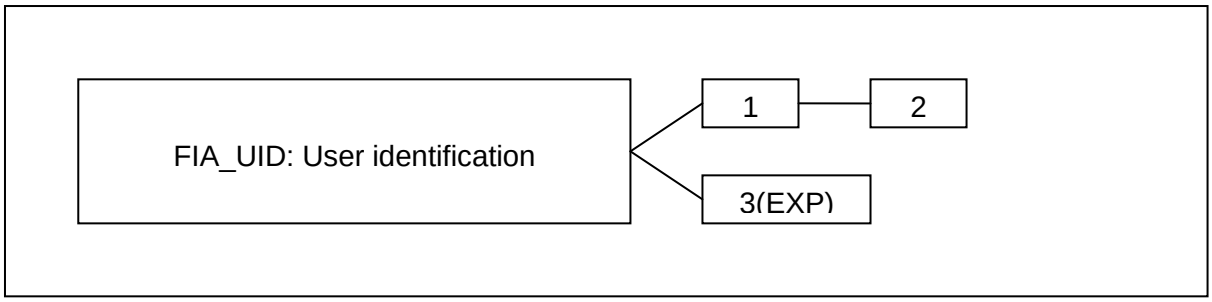


Figure 3 - Component levelling of FIA_UID.3(EXP)

FIA_UID.3(EXP) User subset identification before any action, requires that a subset of users identify themselves before any action will be allowed by the TSF.

Management: FIA_UID.3(EXP)

The following actions could be considered for the management functions in FMT:

a) the management of the user identities.

Audit: FIA_UID.3(EXP)

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;
b) Basic: All use of the user identification mechanism, including the user identity provided.

FIA_UID.3(EXP) User subset identification before any action

Hierarchical to: No other components
Dependencies: No dependencies.

FIA_UID.3(EXP).1 The TSF shall require a user connecting via [assignment: *list of connection methods*] to identify itself before allowing any other TSF-mediated actions on behalf of that user.

9.2 References

[AGD]	Microsoft Exchange Server 2007 Help (August 2009)
[AGD_ADD]	Exchange Server 2007 Common Criteria Evaluation, Guidance Addendum, Installation and Startup, version 1.10, date 2009-09-28
[CC]	Common Criteria for Information Technology Security Evaluation – Part 1-3 model, dated August 2005, version 2.3, CCIMB-08-001-3
[RFC 2821]	Simple Mail Transfer Protocol, http://www.ietf.org/rfc/rfc2821.txt
[RFC 2822]	Internet Message Format, http://www.ietf.org/rfc/rfc2822.txt
[RFC 1730]	Internet Message Access Protocol - Version 4, http://www.ietf.org/rfc/rfc1730.txt
[RFC 1725]	Post Office Protocol - Version 3, http://www.ietf.org/rfc/rfc1725.txt

9.3 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.

9.3.1 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 identifier, e.g. FDP_IFC.1/SRL.

Plain *italicized text* is used to emphasize text.

9.3.2 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.
(Authorized) Administrator	This term refers to a group of users which comprise the predefined Exchange and Windows administrators and any user who is allowed to perform a management operation because the permission has been granted to him by assigning him to a role with administrator permissions or by granting him the possibility to perform an administrative operation explicitly.
Authenticated user	A user, who has provided valid credentials and thus, for whom the authentication could be carried out successfully.
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).
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[18]), 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.
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.
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.
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.
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.
Mailbox number	A number that can be assigned to the mailbox of a user. This number allows the user to use their mailbox via the Outlook Voice Access functionality without having to provide their user name. Exchange internally maps the mailbox number to the corresponding user identity.
MAPI	Messaging Application Programming Interface, framework for

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

	development of messaging applications.
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[19]) Scope of Control (TSC[20]) that contains or receives information and upon which subjects perform operations.
Perimeter Network	Demilitarized zone (DMZ), network area that sits between an organization's internal network and an external network, usually the Internet.
PBX	A Private Branch eXchange (PBX) is a telephone exchange that serves a particular business or office.
Public Folder	Public folders, introduced in the first version of Microsoft Exchange, are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders are hierarchically organized, stored in dedicated databases, and can be replicated between Exchange servers. The term public folder is distinct of the term “folder” that refers to a directory that exists within a Public Folder or a Mailbox and hosts the mailbox or Public Folder items (e.g. emails)
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
RPC	Remote Procedure Calls are a mechanism for inter process communication
RTP	RTP is a thin protocol that supports real-time applications containing continuous media such as the following: • Audio • Timing reconstruction • Loss detection • Security • Content identification

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

[19] 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.

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

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.
Sender Policy Framework	Domain administrators publish sender policy framework (SPF) records on their DNS servers. SPF records identify authorized outbound e-mail servers. If an SPF record is configured on the sender's DNS server, the Edge Transport can parse the SPF record and determine whether the IP address from which the message was received is authorized to send e-mail on behalf of the domain that is specified in the message.
Service Pack	A collection of product enhancements and bug fixes for a specific Microsoft product.
SIP	Session Initiation Protocol used for setting up and tearing down voice and video calls over the Internet. It is transport-independent and can be used with UDP, TCP, TLS or other connections.
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 operating system, which is used as a platform for the Exchange 2007 product.
TCP	Transmission Control Protocol: TCP provides a reliable and ordered delivery of a stream of bytes.
TLS	Transport Layer Security: TLS is based on the SSL 3.0 Protocol Specification; see Secure Sockets Layer
UDP	User Datagram Protocol: UDP is a lightweight protocol to deliver data packages over a network.
User	Any entity (human user or external IT entity) outside the TOE, that interacts with the TOE.
Windows Management Instrumentation	The WMI infrastructure is a Microsoft Windows operating system 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.

9.3.3 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
DGR	Distribution Group Restriction
EAL	Evaluation Assurance Level
EMC	Exchange Management Console
EMS	Exchange Management Shell
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
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

Abbreviation	Definition
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
NDR	Non Delivery Report
NTFS	New Technology File System
OLE	Object linking and embedding
OMA	Outlook Mobile Access
OSI	Open Systems Interconnection Reference Model
OSP	Organizational Security Policy
OVA	Outlook Voice Access
OWA	Outlook Web Access
PC	Personal Computer
PDA	Personal Digital Assistant
POP3	Post Office Protocol Version 3 (see RFC1725)
PP	Protection Profile
QTA	Quota
RC4	Ron’s Code 4
RPC	Remote Procedure Call
RTM	Release to Market
S/MIME	Secure / MIME
SA	Exchange System Attendant
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SM	Security Management
SMR	Security Management Roles
SMTP	Simple Mail Transport Protocol
SOF	Strength of Function
SPF	Sender Policy Framework

Abbreviation	Definition
SRL	Sender Reputation Level
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UCE	Unsolicited Commercial email
UDP	User Datagram Protocol
UIA	User Identification
WebDAV	Web Distributed Authoring and Versioning
WMI	Windows Management Instrumentation