Security Target

for

Tumbleweed MMS ™ and IME ™ Version 5.5.3

Release Date:	**June 1, 2005**
Version:	**4.5**
Status:	**Final**

Prepared By:

Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 Security Target Identification

ST Title: Security Target for Tumbleweed MMS ™ and IME ™ version 5.5.3

ST Version: 4.5

ST Date: June 1, 2005

TOE Identifier[1]: Tumbleweed MMS™ version 5.5.3 (Build 4039) and Tumbleweed IME ™ version 5.5.3 (Build 4018)

Assurance level: EAL 2 augmented with ACM_CAP.3: Authorisation Controls, ACM_SCP.1: TOE CM coverage, ADV_HLD.2: Security enforcing high-level design. (aka EAL 2+)

Author: Tumbleweed.

Common Criteria: Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999 (aligned with ISO/IEC 15408: 1999)

Interpretations: National and International interpretations are provided within section 9.3 of this Security Target

Keywords: Secure Messaging, Secure E-mail, MMS, IME, Messaging Management System (MMS), Integrated Messaging Exchange (IME), S/MIME

[1] Identification of the TOE for this evaluation remains as it is specified above. However, references in this document and other assurance documentation to Tumbleweed MMS ™ and IME ™ Version 5.5 also applies to Version 5.5.3..

1.2 Security Target Overview

Tumbleweed MMS ™ and IME ™ together provide a turnkey solution that allows companies to create a secure messaging and email solution; define email-filtering policies, archive messages that violate policies, monitor messaging traffic, and intelligently route sensitive messages through a secure channel.

In addition, Tumbleweed MMS and IME also include administrative tools for system management, policy management, and account management.

The Tumbleweed MMS and IME version 5.5 ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the Tumbleweed products meet in order to mitigate the defined threats:

- **TOE Description** – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- **TOE Security Environment** – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- **Security Objectives** – Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- **IT Security Requirements** – Presents the Security Functional Requirements (SFRs) met by the TOE and its environment. In addition, the Security Assurance Requirements (SARs) met by the TOE are presented.
- **TOE Summary Specification** – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- **Protection Profile Claims** – Presents the rationale concerning compliance of the ST with any protection profiles.
- **Rationale** – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- **References** – Presents a set of acronyms, vocabulary of terminology, and interpretations of requirements that apply to this ST.

1.3 CC Conformance Claims

This TOE is CC Version 2.1 Part 2 extended and CC Version 2.1 Part 3 conformant.

This ST claims assurance at EAL 2 (augmented with ACM_CAP.3: Authorisation Controls, ACM_SCP.1: TOE CM coverage, ADV_HLD.2: Security enforcing high-level design).

165 1.4 Documents Conventions

There are several font variations within this ST. The section below provides an explanation of the font conventions used to show operations, as defined in Common Criteria, performed on the requirements. When NIAP interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment: *<u>Requirement text will appear in Italics and underlined</u>*

Iteration: Typical CC requirement naming will be followed by a lower case letter for each new iteration. (Ex. FMT_MOF.1.1a)

Selection: **<u>Requirement text will appear in bold and underlined</u>**

Refinement: ***Requirement text will appear in bold italics***

2 TOE Description

This section describes the Target of Evaluation (TOE) in terms of the class of product, the provided security functionality, and the TOE boundaries.

2.1 Tumbleweed MMS and IME 5.5 Overview

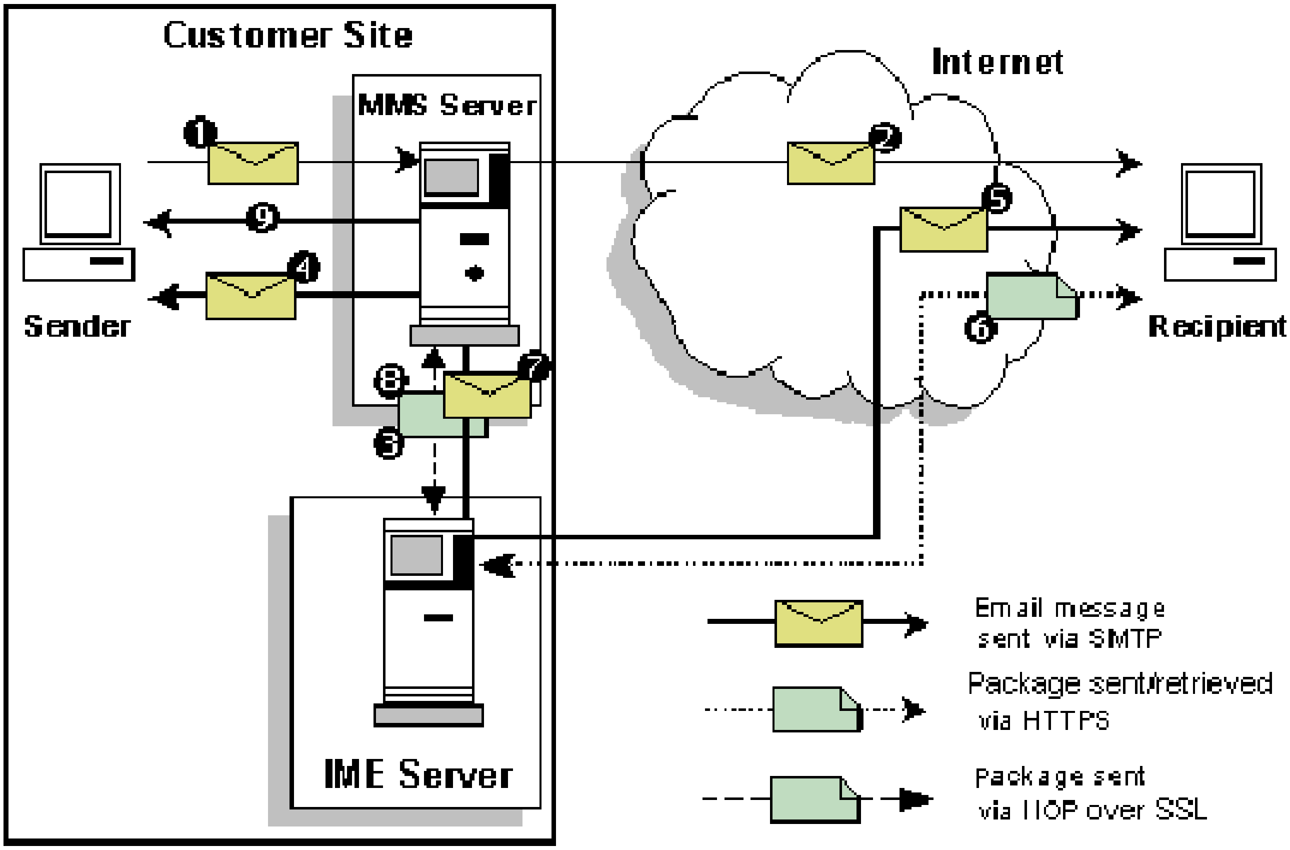
The Tumbleweed MMS and IME version 5.5 products consist of the two main components that comprise the TOE:

- The Tumbleweed MMS, also known as Messaging Management System (MMS), provides the enforcement of email-filtering policies for the use of corporate email systems. Such policies include those for mail filtering, included attachments, virus scanning, encryption filtering, signature filtering. Policies covering Secure Public Network handling, and headers removal are not included within this evaluation and are not claimed for this TOE.
- The Tumbleweed IME, also known as Integrated Messaging Exchange (IME), provides businesses with a secure interactive communications channel to reach their customers and partners.

In the context of Tumbleweed, encrypted messages and attachments are hereafter referred to as “IME packages” or “packages”. There are four different IME roles. The first role is an IME Administrator. The other three roles are collectively referred to as IME users, which includes the following roles.

- An IME Group Manager typically is a standard user, yet with the additional capability to add additional users to the group, as well as, remove members and change their password.
- The second user role is an IME Group Member, which is a member of an IME Group.
- The third IME user role is an IME Individual Account User, not a member of a group, but just an individual user account.

Figure 1: Message Flow Using MMS and IME Together


Customer Site
MMS Server
Internet
1
2
3
4
5
6
7
8
9
Sender
Recipient
IME Server
Email message sent via SMTP
Package sent/retrieved via HTTPS
Package sent via IIOP over SSL

1. A User sends an email message. Email messages destined for recipients outside the customer site are converted to SMTP format for transmission across the Internet. MMS routinely scans these email messages and enforces policies.

2. If an email message does not trigger a redirect policy, it is routed to the recipient using SMTP (unless other policies dictate special handling, for example, delivery using S/MIME).

3. If the email message triggers a redirection policy, MMS converts the message into an IME package and transmits it to the IME Server using the Tumbleweed Server API client. The package will be transmitted over SSL (Secure Socket Layer) between the MMS 5.5 and IME 5.5 servers

   Note: While this scenario shows policies redirecting outbound email to the IME secure server, policies can also be defined redirecting inbound email to the IME secure server.

4. Optionally, MMS returns a package description to notify the sender of the redirection. This notification takes the form of an email message and includes the IME package ID, service options, such as priority, and access information for the sender's IME account.

5. IME Server sends an SMTP message notifying recipient(s) of the IME package, including a URL with which the package can be retrieved. Or, if a recipient's Account Type specifies Secure Envelope ™ (SE) delivery, the recipient can open the encrypted message from within the email client, regardless of whether they are online or offline.

6. The Recipient retrieves the package using a Web browser. The recipient will be required to authenticate with the IME Server and use a secure (SSL) connection to access and retrieve the package.

7. IME Server optionally generates receipt confirmation messages to notify the sender when each recipient retrieves the package.

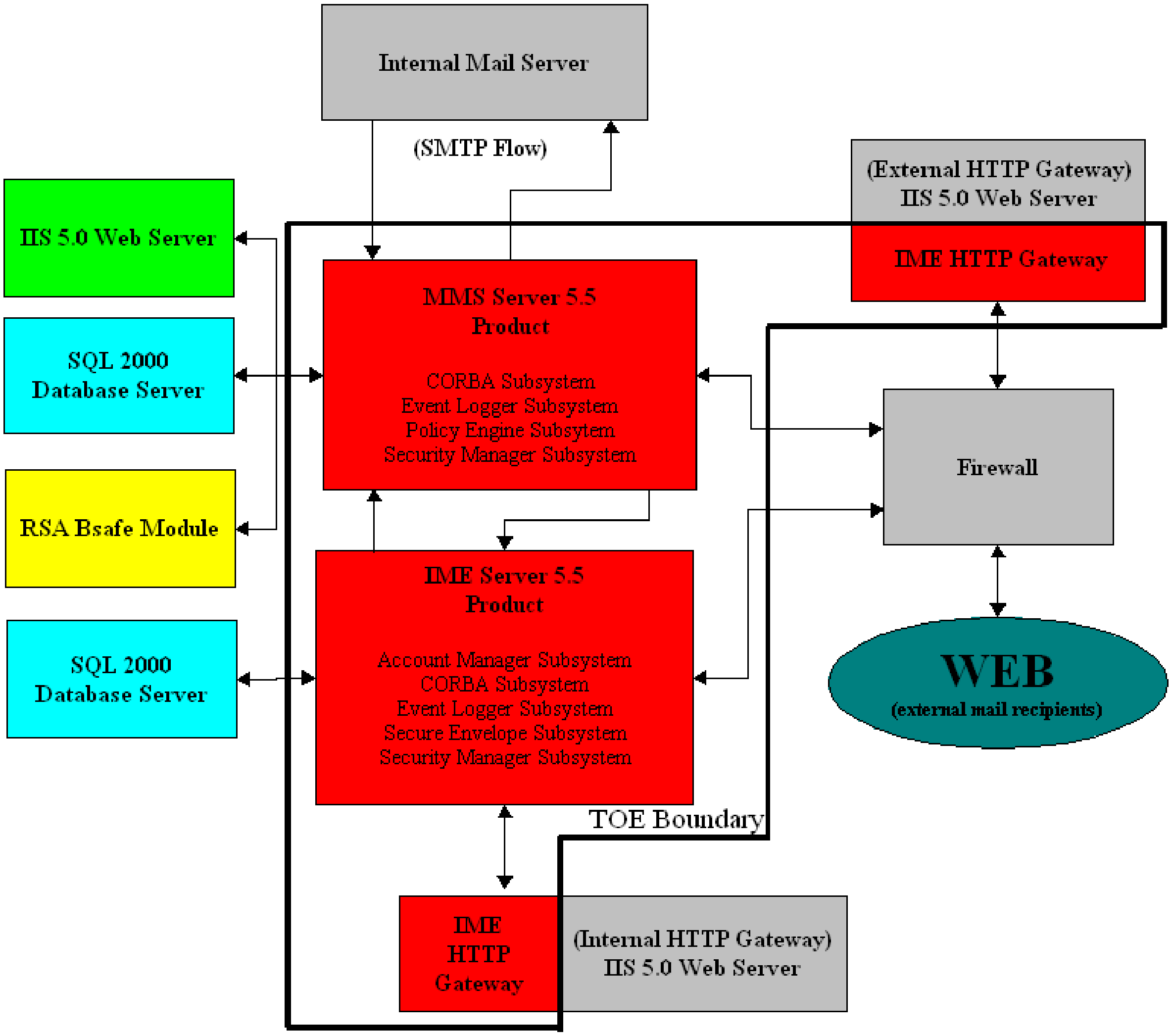
8. IME Server sends the reply to a message through Secure Response™ delivery to MMS using Internet Inter-ORB Protocol (IIOP) if the recipient's delivery method has Secure Response™ delivery selected.

9. MMS then sends the replied message to the sender (original sender of the message that was replied) using SMTP.

2.2 Logical Boundaries

230 This section describes the flow of information when a message is sent from an MMS system that uses Secure Redirect. Figure 1 above illustrates how mail is routed using the Secure Redirect service. Figure 1a illustrates the logical boundary of the TOE. TOE components are marked as red.

Figure 1a: Logical Boundary of the TOE



235

2.2.1 MMS Components

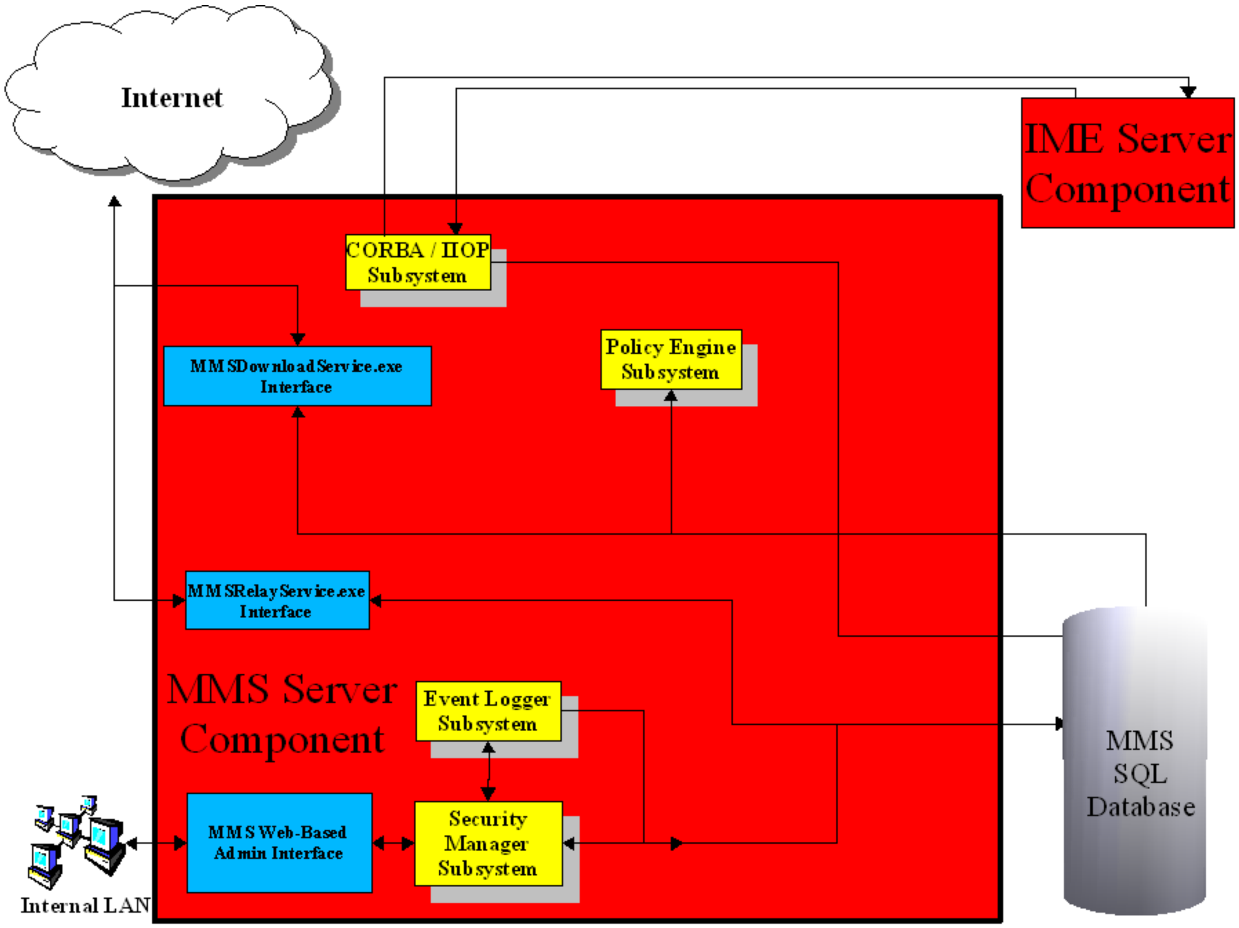
The MMS Server consists of the following components:

- MMS Web-based Administrative Interface;
- 240 CORBA;
- Event Logger;
- Policy Engine;
- Security Manager.

245 Figure 2 below shows the relation of how these MMS components work together to support the functionalities that MMS provides. MMS configuration data, policies, certificates, directory information, event log data, messages, archived messages and message meta-data are stored on the MMS SQL database.

Figure 2 also includes the two other external interfaces, the MMSDownloadService.exe and the 250 MMSRelayService.exe. These mediate access to the public internet and allow the MMS server to receive SMTP messages and to download new virus definitions.

Figure 2: MMS Components



255 *2.2.1.1 MMS Web-based Administrative Interface*

The Administrator Interface component of MMS provides an interface for remote administration of the MMS server. This interface is only accessible by individuals that possess MMS 1st level or 2nd level administration rights. The only subsystem which the MMS Web-based Administrative Interface directly interacts with is the security manager subsystem which acts as a
260 reference monitor mediating all requests for access to data or to other subsystems.

2.2.1.2 CORBA

The CORBA component of MMS provides a distributed object framework for the communication channel to an IME Server and, in the evaluated configuration, will be encrypted with OpenSSL. CORBA provides a communication path between the IME and the MMS servers. When a message is received by the CORBA subsystem, it is decrypted and stored in the MMS database.

2.2.1.3 Event Logger

The Event Logger component of MMS generates logs of system events for the MMS server. The events generated by the Event Logger can be viewed and sorted through the MMS Web-Based Administrator interface. The event logger monitors the security manager subsystem, when an auditable event occurs the event logger subsystem records it in the MMS database.

2.2.1.4 Policy Engine

When a new message is added to the MMS SQL 2000 database it is always passed to the Policy Engine for analysis. The MMS Policy Engine component of MMS uses the MMS Directory, a database within the MMS SQL 2000 database server, to determine which policies apply to each email message. The engine then evaluates each email message and checks against all the policies in succession. After this evaluation, the policy engine determines the disposition of the message and what action to take based on the action dictated by the most restrictive policy.

The policy engine always checks all of the policy categories, even if the email message is intercepted or blocked by the first policy category it encounters. Checking all the policy categories enables complete and detailed reporting on policy violations, without a noticeable effect on performance.

2.2.1.5 Security Manager

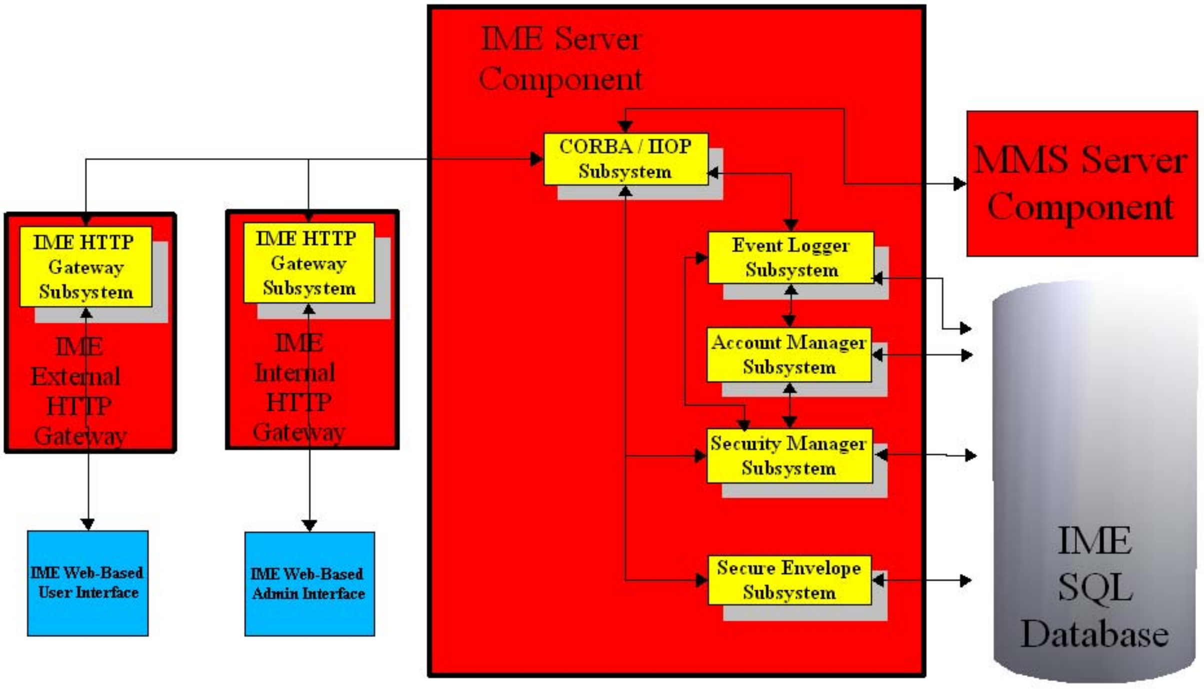
The Security Manager component of MMS provides a control of access permissions to MMS 1st level administrators and MMS 2nd level administrators and allows for the management of MMS configurations. The security manager subsystem acts as a reference monitor to the MMS web-Based Administrator Interface mediating all requests for access to data or to other subsystems.

2.2.2 IME Components

290 The IME product consists of the following components:

- Account Manager
- IME Web-Based Administrative Interfaces
- CORBA
- Event Logger
- 295 Secure Envelope
- Security Manager
- IME Web-Based User Interfaces
- IME HTTP Gateway

300 **Figure 3: IME Components**


IME Server Component
CORBA / IIOP Subsystem
Event Logger Subsystem
Account Manager Subsystem
Security Manager Subsystem
Secure Envelope Subsystem
MMS Server Component
IME SQL Database
IME HTTP Gateway Subsystem
IME External HTTP Gateway
IME HTTP Gateway Subsystem
IME Internal HTTP Gateway
IME Web-Based User Interface
IME Web-Based Admin Interface

2.2.2.1 Account Manager

The Account Manager component of IME manages the IME accounts, maintains account-related information, and validates each account every time the IME user or IME administrator authenticates to IME. The account manager is invoked by the security manager subsystem and interacts with the event logger subsystem to report auditable events.

2.2.2.2 IME Web-Based Administrative Interfaces

The Administrative Interface component of IME provides an interface for remote administration of the IME product. This interface is only accessible by individuals that possess IME administration rights. When an IME Administrator attempts authentication the Security Manager Subsystem is invoked so that the user ID and associated password provided may be verified to determine if the user is granted access. The user ID and password verification is provided by checking the supplied information against what is stored in the IME database. If the user ID and password matches a user ID and associated password within the IME database, then access is granted.

2.2.2.3 CORBA

The CORBA component of IME provides the distributed object framework that allows the IME Server components to communicate in addition to allowing communication from MMS.

The Naming Service of CORBA is the process that allows the components to find each other on the network. It keeps track of the component locations. The Naming Service acts like a White Pages directory to provide a reference that allows you to access a particular component. When the IME Server starts, the IME Server components can be accessed through the CORBA Naming Service.

The CORBA subsystem provides a communication path between the IME and the MMS servers. When a message is received by the CORBA subsystem, it is decrypted and sent to the IME database, via the event logger subsystem.

2.2.2.4 Event Logger

The Event Logger component of IME generates logs of system events for the IME product. The Event Logger can be viewed either through the IME Web-Based Administrator interface, or through the application log of the event viewer within the operating system. Auditable events may be passed to the event logger either from the MMS server, via the CORBA subsystem or from the IME account manager and security manager subsystems.

2.2.2.5 Secure Envelope

The Secure Envelope component of IME provides an alternative delivery method for a user to store an encrypted package locally on their personal computer without the need of retrieving the package from the IME product every time the package is accessed. Generally, when a package is sent using Secure Envelope, the package is encrypted on the IME product using either the package password provided by the sender or the account password of the recipient. Therefore once the recipient receives the package, they may authenticate and decrypt the package locally without the need of connecting to the IME product. The secure envelope subsystem is invoked from the IME Web-Based User interface but all requests are mediated by the security manager subsystem.

2.2.2.6 Security Manager

The Security Manager Subsystem performs the identification and authentication function and enforces the accesses users are granted based on their role. For example if an entity is identified as an IME user and attempts authentication via the IME Web-Based Admin Interface, the Security Manager Subsystem then denies the authentication request. Before accessing any IME data or resources users must be identified and authenticated by the Security manager. The security manager then creates a user session with access rights appropriate to the user's role.

2.2.2.7 IME Web-Based User Interfaces

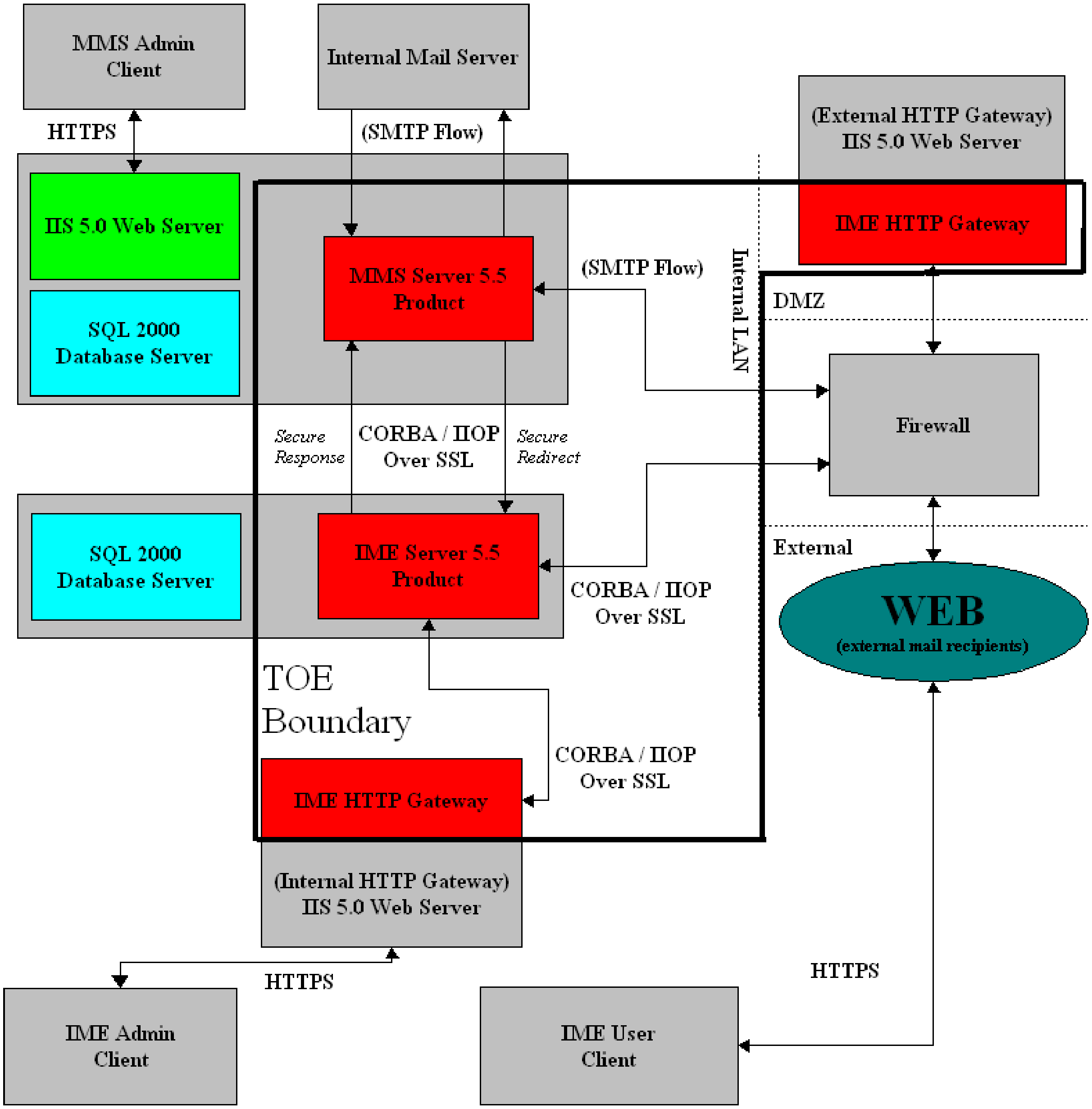
The User Interface component of IME provides individuals possessing a user account, an interface for remote accessibility of the IME product for their specified account. Within this interface, an IME Group Member, IME Group Manager and IME Individual Account User can retrieve messages, send messages, access their address book, and change their passwords. When an IME user attempts authentication the Security Manager Subsystem is invoked so that the user ID and associated password provided may be verified to determine if the user is granted access. The user ID and password verification is provided by checking the supplied information against what is stored in the IME database. If the user ID and password matches a user ID and associated password within the IME database, then access is granted.

2.2.2.8 IME HTTP Gateway

The IME HTTP Gateway acts as a broker between HTTP client requests and the IME back-end API. The HTTP gateway assists the Security Manager in enforcing the identification and authentication function. Following the establishment of a session the HTTP gateway creates a token associated with the identity of the authenticated user. This token is passed with each request for access to TOE functionality and TOE or user data. The Security Manager can use this token to ensure that the user session is not hijacked.

2.3 Physical Boundaries

Figure 4: TOE Boundaries



The TOE is defined to be the Tumbleweed MMS and IME version 5.5 products. The diagram shown above in Figure 4 represents the physical boundaries of the TOE. Each grayed area within the figure represents a physical machine, showing the physical layout and relationships with the TOE and non-TOE components.

The TOE is intended to operate in a protected environment. This means that all components should be behind a suitably configured firewall, with the external HTTP gateway on the firewall DMZ. A DMZ is a screened subnet between a company's private network and the outside public network used to allow external users access to an organizations public data, like web pages, while protecting the firm's private network. The Security Target and supporting documents only make specific claims about the firewall and network architecture, not about the specifics of the firewall and its rulebase. Indeed the TOE imposes no special configuration rules on the firewall than would be needed for any system using mail and internet i.e. access on at least port 23 for SMTP, port 80 for HTTP and port 443 for HTTPS.

The MMS server consists of the MMS version 5.5 product, a SQL 2000 database server, and an IIS 5.0 Web Server running on Windows 2000 Server. The IME server consists of the IME version 5.5 product with a SQL 2000 database server running on Windows 2000 Server. The two IIS 5.0 web servers communicating with the IME server run on separate machines with Windows 2000 Server.

The first web server is identified as the external HTTP gateway and is recommended to be within a DMZ environment so that a complete separation, as well as, use of the CORBA / IIOP over SSL communication channel is provided to allow a secure communication between the external HTTP gateway and IME. The second web server is located internally within the network infrastructure and is referred to as the internal HTTP gateway.

The TOE environment consists of web/messenger clients, IME administration client, MMS administration client, three web servers, two database servers, the underlying operating systems and supported hardware for both MMS and IME, and optionally an internal mail server. The web/messenger clients provide a web-based interface for IME users to access the IME server over the internet. To access the IME server as an IME user, an IME web client must connect to the external HTTP gateway. The IME administration client provides a web-based interface for IME administrators to access and administrate the IME server. To access the IME server for administration, an IME administrator client may only connect through the internal HTTP gateway. This disallows administration of the IME server from the internet. The MMS administration client provides a web-based interface for MMS administrators to access and administrate the MMS server. The web servers provide the capability for IME users, IME administrators, and MMS administrators to access the MMS and IME servers via HTTP/HTTPS. The database server for the IME server provides storage of configuration data, and user data. The database server for the MMS server provides storage of configuration data, virus definitions, queued packages, and archived packages.

In cases where an internal mail server is provided, the MMS server relays messages to this server after checking its configured policies to make sure that the messages do not violate any policy or require to be redirected to IME. In cases where an internal mail server is not provided, MMS server checks incoming messages for configured policies to make sure that the messages do not violate any policy and then redirect the messages to IME.

A typical case of information flow internally into the MMS and IME messaging and email solution would be the following:

> An SMTP message is directed from the internet to the domain in which MMS is hosting. The organization’s firewall directs the incoming SMTP message to the MMS server. The MMS server checks the message in accordance with the policies it has defined. If a message triggers a policy, the policy will enforce the actions specified for that policy. Depending on the action specified, MMS may drop the delivery, return the message back to the sender, quarantine the delivery, detain the delivery, defer the delivery, deliver normally, or redirect to the IME server. In the event the message is redirected to the IME server, the message is encrypted and sent through the CORBA / IIOP over SSL communication channel. Once IME receives this new message, it sends a notification to the IME user’s email account to notify the user of a new IME delivery. Depending on the security provided for the IME message, the notification sent to the user may include a personalized URL to receive the message, a URL to login to IME via an IME account, a URL to login to IME via a package password via an IME account, a URL to login to IME via a package password, or the actual message encrypted within an attachment, also known as Secure Envelope.

The following hardware components are not considered part of the TOE, yet the TOE requires at a minimum two Intel Pentium computers consisting of the following:

- Processor equivalent to Pentium III, 700 MHz or higher recommended.
- RAM – 512 MB minimum (1 GB or more recommended).
- Hard Drive Space – 300 MB minimum (for IME Server installation)
  20 GB (for MMS installation).
- TCP/IP networking adapter.

The following software components are required for TOE operation but are not considered to be part of the TOE:

- MMS and IME Database Server (SQL 2000 with SP3, installed locally on each server)
- Web Server (IIS 5.0) - *required to be installed on MMS for remote administration, and additionally installed separately from IME; IME requires two web servers which include internal and external HTTP gateways*
- Web Client/Messenger Client (JavaScript or ActiveX capable)
- Operating system (Windows 2000 Server with SP3)

3 TOE Security Environment

The TOE environment is both a physically and a logically secure environment that can operate in a mode capable of protecting the transmitted or stored information at the highest classification level of messages in this environment. Additionally, the MMS and IME will coexist with other network devices not covered by this security target (e.g. firewall), to provide for data transmission to lower classification systems. Physical, personnel, and administrative non-technical security is provided by a local support environment and procedures that protect all clients and servers by limiting access to MMS, IME, and messages to authorized IME users. The TOE environment shall implement the Information Assurance (IA) Defense in Depth strategy. The risk level of the environment is considered to be low.

- The TOE environment shall ensure network services provide appropriate confidentiality and defenses against denial of service attacks.

- The TOE environment shall defend the perimeter of information environments (e.g., firewalls, intrusion detection, and uniform policy on protocols allowed across perimeter boundaries).

- The TOE environment shall make appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, and directories).

3.1 Assumptions

A.Admin

It is assumed that one or more authorized administrators are assigned who are competent to manage the SQL 2000 Database Servers for MMS and IME, the Internal and External HTTP Gateways, the IIS 5.0 web server for MMS, and the Windows 2000 operating systems of MMS and IME, who are competent to manage the security of the information these systems contain, and who can be trusted not to deliberately abuse their privileges so as to undermine security.

A.Locate

The processing resources of the TOE are assumed to be located within controlled access facilities which will restrict unauthorized physical access.

A.Message_Secure

The IME user will select the proper security protections for messages (e.g. encrypt, plaintext).

A.Timestamp

A reliable source of time is provided by the Windows 2000 operating system for MMS, IME, and the two HTTP Gateways communicating with IME.

A.User_Auth_Credentials

The user will not disclose their password.

3.2 Threats

3.2.1 Threats against the TOE

T.Admin_Err_Commit: Administrative errors of commission

An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

T.Admin_Err_Omit: Administrative errors of omission

The MMS 1st level administrator, MMS 2nd level administrator, or IME administrator fails to perform some function essential to security.

T.Admin_Hostile_Modify: Hostile administrator modification of user or system data

An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

T.Admin_UserPriv: Administrator violates user privacy policy

An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator which has full access privileges gains knowledge of privacy-related information such as the identity of an IME user.

T.Audit_Exhaustion: Hacker fills the MMS audit log

A hacker might exhaust the storage capacity of the audit trail of the MMS sever in order to prevent the auditing of unauthorized access.

T.Brute_Force: Brute force attack on passwords

A hacker repeatedly attempts password authentication on known IME User accounts to gain unauthorized access of those accounts.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications

A hacker obtains IME user data by eavesdropping on communications lines.

T.Hack_Masq: Hacker masquerading as a legitimate user or as a system process

A hacker masquerades as an authorized user or system process to perform operations that will be attributed to the authorized user or a system process.

T.Hack_Msg_Data: Message content modification

A hacker modifies information within a message and thereby deceiving the intended recipient.

T.New_Virus: Newly discovered virus

An attacker sends a message with a newly discovered virus that is undetected by virus scanners that have not been updated.

T.Repudiate_Receive: Recipient denies receiving information

The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

T.Repudiate_Send: Sender denies sending information

The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

T.User_Abuse_Conf: Hostile user acts cause confidentiality breaches

An IME user gains unauthorized access to read, modify or remove IME Packages sent or received by another IME User.

T.User_Conf: Unauthorised access to message

An unauthorised user of low attack potential gains access to a message sent to an individual without an IME account.

T.User_Misuse_Avl_Resc: User's misuse causes denial of service

A user's unauthorized use of resources causes an undue burden on an affected resource.

T.User_Modify: User abuses authorization to modify data

A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.

3.2.2 Threats against the TOE Environment

TE.Audit_Data_Integrity: A user modifies audit records

A user modifies audit records stored in the environment in an attempt to cover up actions that were previously performed.

TE.Audit_Exhastion: Hacker fills the IME audit log

A hacker might exhaust the storage capacity of the audit trail of the IME sever in order to prevent the auditing of unauthorized access.

3.3 Organizational Security Policies (OSPs)

540 **P.Message_Archive: Archival of messages triggered by policy violations**

All messages detected to violate a policy shall be archived for review by a local administrator of the MMS Server's operating system.

P.Policy_Engine: Policy Engine

All messages shall be subject to review by the policies defined within the policy engine.

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 TOE Environment.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives satisfied by the TOE. The TOE accomplishes the security objectives delineated within this section.

O.AC_Admin_Limit: Limitation of administrative access control

The TOE shall design administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions.

O.Admin_Guidance: Administrator guidance documentation

The TOE shall deter administrator errors by providing adequate administrator guidance.

O.Archive_Messages: Archiving of Messages

The TOE shall archive all messages that violate any of the MMS defined policies, so that they may be viewed at the local administrator's convenience.

O.Audit_Gen: Generate Audit Data

The IME server shall generate audit data. The date and time of the event, type of event, source of event, user identity (if applicable), and a description of the event will be recorded.

O.Audit_Clear: Clearing old audit records

The MMS server shall remove audit records if they are older than 30 days or if the audit trail exceeds 10048KB.

O.Audit_Review

The TOE shall provide the capability for authorized administrators to review the audit trail in a suitable format.

O.Authentication: Restrict actions before authentication

The TOE shall require that an IME user, IME administrator, MMS 1st level administrator, or MMS 2nd level administrator present a valid user identity / password before being allowed any other direct access to the TOE.

O.Auth_Failure: Authentication failure

The IME server shall provide the ability to temporarily disable IME users' and administrators' accounts based on a defined number of authentication failures to the specified account.

O.Data_Exchange_Conf: Enforce data exchange confidentiality

The TOE shall provide the ability to protect IME data confidentiality during the transmission between TOE components.

O.MsgMod_ID: Identify message modification in messages sent or received remotely or locally

The TOE initiates a check which recognizes changes to signed messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages. This check is performed by the RSA Crypto-C module in the environment and the TOE is notified in the case of modification.

O.NonRepudiate_Recd: Non-repudiation for received information

The TOE shall provide evidence to prevent IME users from avoiding accountability of received messages.

O.NonRepudiate_Sent: Non-repudiation for sent information

The TOE initiates a verification of the digital signatures provided in messages sent to MMS for the validity of the signatures. This is performed by the RSA Crypto-C module in the environment and the TOE is notified if the signature is invalid. Based on the validity of the digital signature, the sender cannot repudiate the information sent.

O.Pass_Auth: Password-based authentication

The IME server shall provide a mechanism to verify the strength of IME user-generated secrets for the password-based authentication of IME Users.

O.Pol_Eng: Policy Engine

The TOE shall enforce all messages to be reviewed by all of the MMS configured policies and apply appropriate actions to any messages in violation in accordance with the specified configured policy.

O.Protect_Accounts: Protecting Accounts

During the logon process the TOE will not give any feedback which will aid an attacker to gain unauthorized access to a user or administrator account.

O.SE_Auth: Secure Envelope Authentication

The TOE shall produce Secure Envelope packages on behalf of IME users.

O.Security_Attr_Mgt: Manage security attributes

The TOE shall provide restricted management mechanisms for the initialization of and configuration of values for, and allowable operations on, security attributes.

O.Security_Func_Mgt: Manage behavior of security functions

The TOE shall provide restricted management mechanisms for security mechanisms.

O.Security_Roles: Security roles

The TOE shall maintain security-relevant roles for the IME Server and the association of individuals with those roles.

O.Session_Termination: System terminates session for inactivity

The TOE shall terminate a session after a given interval of inactivity.

O.Trusted_Path: Trusted communications path

The TOE shall provide a communication channel capable of protecting confidentiality and of providing reliable entity authentication of the endpoints of the communication path.

O.User_Attributes: Maintain user attributes

The TOE shall maintain a set of security attributes (which includes user identity, password and group membership) associated with individual users in addition to user identity (e.g. email address).

O.Virus_Updates: Virus Definition Updates

The TOE shall download and apply virus definition updates frequently.

4.2 Security Objectives for the Environment

The TOE Environment accomplishes the security objectives delineated within this section.

4.2.1 IT Environment Objectives

OE.Adm_Roles: Administrative roles

Restrict the capabilities for MMS 1st level administrators to add additional administrative accounts, and modify the audit log by providing a MMS 2nd level administrator strictly for those functions.

OE.Audit_Clear: Clearing old audit records

The environment of the IME Server shall remove audit records if they are older than 30 days or if the audit trail exceeds 10048KB.

OE.Audit_Gen: Audit Generation capabilities

Provide information about past MMS Administrators' behavior to an authorized MMS 1st level administrator, MMS 2nd level administrator through system mechanisms to discover system misuse and provide a potential deterrent by warning the administrators. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

OE.Audit_Storage: Audit storage capabilities

Provide the capability for the TOE environment component to store audit data. In addition to storing audit data, provide the capability to prevent audit trail failure and to protect the integrity of the stored audit data.

OE.Audit_Review: Sorting of audit data

The environment of the IME server will provide the capability to sort audit data.

OE.Authentication: Verification of authentication data

The environment of the MMS server will provide the capability to verify a username / password pair passed to it by the MMS server.

OE.Crypto_Operation: Cryptographic operations

Cryptographic interfaces shall protect communication channels from disclosure and modification through encryption. The cryptographic interfaces shall additionally ensure that messages retain their content integrity during storage and transmission.

OE.MsgMod_ID: Identify message modification in messages sent or received remotely or locally

The RSA Crypto-C module will perform an integrity check on a signed message when requested by the TSF and report any modification detected.

OE.NonRepudiate_Sent: Validation of digital signatures

The RSA Crypto-C module will check the validity of a digital signature when requested by the TSF and report any invalid signatures.

OE.SE_Crypto_Ops: Secure Envelope Cryptographic Operations

Provide the encryption, decryption, and hashing of packages sent via Secure Envelope.

OE.SE_Key_Gen: Secure Envelope Key Generation

Provide the generation of keys for packages sent via Secure Envelope.

OE.Timestamp: Time stamping

The underlying operating system of the MMS and IME is trusted to be a reliable source for time.

4.2.2 Non-IT Environment Objectives

OE.Competent_User: Competent User

IME users will be adequately trained to know the implications in selecting the proper security protection level for messages (e.g. sign, encrypt, plaintext).

OE.Physical_Control: Physical Control

Information shall be physically protected to prevent unauthorized disclosure, destruction, or modification.

OE.Trustworthy_Administrators: Trustworthy Administrators

Administrators shall be competent to manage the SQL 2000 Database Servers for MMS and IME, the Internal and External HTTP Gateways, the IIS 5.0 web server for MMS, and the Windows 2000 operating systems of MMS and IME, who are competent to manage the security of the information these systems contain, and who can be trusted not to deliberately abuse their privileges so as to undermine security.

OE.Trustworthy_User: Trustworthy User

All users of the TOE shall be trusted not to disclose their password, to prevent unauthorized access of their account.

5 IT Security Requirements

This section defines functional and assurance requirements for the TOE, and the Security requirements for the IT environment.

Table 1: IT Security Functional Requirements

Functional Requirement:	**Operations Performed:**
Functional Requirements for the TOE	
FAU_SAR.1	Assignment
FDP_ACC.1	Assignment
FDP_ACF.1	Assignment, Selection, Refinement
FIA_UAU.7	Assignment
FMT_MOF.1	Assignment, Selection
FMT_MSA.1	Assignment, Selection
FMT_MTD.1	Assignment, Selection
FMT_SMF.1	Refinement and Assignment
FPT_ITC.1	None Performed
FTP_ITC.1	Assignment, Selection
Explicitly Stated Functional Requirements for the TOE	
FAU_IME_GEN.1	Refinement
FAU_MMS_ARC.1	None Performed
FAU_IME_SAR.2	None Performed
FAU_MMS_SAR.3	None Performed
FAU_MMS_STG.3	None Performed
FCO_IME_NRR.1	None Performed
FCO_MMS_NRV.1	None Performed
FDP_MMS_POL.1	None Performed
FDP_IME_UCT.1	None Performed
FIA_IME_AFL.1	None Performed
FIA_IME_SOS.1	None Performed
FIA_IME_UAU.1	None Performed
FIA_IME_UID.1	None Performed
FIA_MMS_TOA.1	None Performed
FMT_MMS_DNL.1	None Performed
FMT_IME_MSA.3	None Performed
FMT_IME_REV.1	None Performed
FMT_IME_SMR.1	None Performed
FTA_SSL_EXP.3	None Performed

Functional Requirement:	**Operations Performed:**
Functional Requirements for the TOE Environment	
FAU_STG.1	Selection, Refinement
FCS_CKM.1	Assignment, Refinement
FCS_COP.1	Assignment, Refinement
FMT_MSA.2	Refinement
FPT_STM.1	Refinement
Explicitly Stated Functional Requirements for the TOE Environment	
FAU_MMS_GEN.1	Refinement
FAU_MMS_GEN.2	Refinement
FAU_IME_SAR.3	None Performed
FAU_IME_STG.3	None Performed
FCS_MMS_CKM.2	None Performed
FCS_MMS_CKM.4	None Performed
FIA_MMS_AUT.1	None Performed
FMT_MMS_SMR.1	None Performed

5.1 TOE Security Functional Requirements

This section provides the TOE Security Functional Requirements. All security functional requirements within this section are drawn from CC Part 2 security functional requirements.

5.1.1 Security Audit (FAU)

5.1.1.1 Audit Review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide *the MMS 1st level administrator, MMS 2nd level administrator, and IME administrator* with the capability to read *the date and time of an event, type of an event, source of an event, user identity related to an event, and a description of an event, for events corresponding to the respective administrators' server* from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2 User Data Protection (FDP)

5.1.2.1 Subset Access Control (FDP_ACC.1)

FDP_ACC.1.1

The TSF shall enforce the *access control policy in Table 2 (Access Control Policy)* on *individual mail files and server resources, and all operations performed by subjects (i.e., users and administrators) covered by the access control policy in Table 2 (Access Control Policy)*.

5.1.2.2 Security Attribute Based Access Control (FDP_ACF.1)

FDP_ACF.1.1

The TSF shall enforce the *access control policy in Table 2 (Access Control Policy)* to objects based on *role permissions associated with an authenticated identity*.

FDP_ACF.1.2

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

> *(1) MMS 1st level administrator, MMS 2nd level administrator, and IME administrator will be granted access to messaging and server resources in accordance with their granted permissions defined with the access control policy in Table 2 (Access Control Policy)*
> *(2) IME users will be granted full access to their individual messaging resources*

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***no additional rules***.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the ***following rules*****: *no additional explicit denial rules*.**

Table 2: Access Control Policy

Server Component	Role	Access
IME	IME user	Access to messages, the mailbox and address list of that individual user, Group Manager or group member.
IME	IME user	Access to create a Secure Envelope Package.
IME	IME User and IME administrator	Access to change the password of the referenced logged-in account.
IME	IME user and IME administrator	Access to create, delete, or view created folders for the logged-in account.
IME	IME Group Manager	Access to create additional members within an assigned group.
IME	IME Administrator	Access to change any user's password.
IME	IME Group Manager	Access to change an assigned group member's password
IME	IME Group Manager	Access to remove members within the assigned group.
IME	IME Administrator	Access to change the default security associated with an IME user's messages.
MMS	Anyone	Submit a message via SMTP
MMS	MMS 2nd level Administrator	Access to change administrator roles
MMS	MMS 2nd level Administrator	Access to change any user‘s password
MMS	MMS 1st level Administrator	Access to change their own password

5.1.3 Identification & Authentication (FIA)

5.1.3.1 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1

The TSF shall provide only *indication of how many password characters have been typed without showing the characters themselves by substituting each character with a dot, indication of the account name in clear text being authenticated, indication of authentication failure, indication of how many unsuccessful authentication attempts are allowed before the account is locked (IME component only), indication of an invalid account name(IME component only), and indication of the account being locked out (IME component only)* to the user while the authentication is in progress.

745 5.1.4 Security Management (FMT)

5.1.4.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1

The TSF shall restrict the ability to **modify the behavior of** the functions *listed in Table 3a (Security Functions Management)* to *the IME and MMS administrators*.

750 **Table 3a: Security Functions Management**

Server Component	Role	Functions
IME	IME Administrator	Access to view IME system summary information (status information of the server components).
IME	IME Administrator	Access to view and change IME system configuration information.
IME	IME Administrator	Access to view IME system statistics (performance and activity of the IME server and components).
IME	IME Administrator	Access to view IME system events.
IME	IME Administrator	Access to create individual IME accounts.
IME	IME Administrator	Access to delete, enable, disable, re-enable, and update IME accounts.
IME	IME Administrator	Access to revoke an IME user's associated security attributes.
IME	IME Administrator	Access to change the default security associated with the messages each category (type) of IME user.
MMS	MMS 1st level Administrator	Access to administer MMS operation
MMS	MMS 2nd level Administrator	Access to administer MMS operation, modify administrator accounts, and modify the audit log
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to view MMS status information for MMS services, message queues, event warnings, and license/version number.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to setting up or configuring relay centers, queues, global policy settings, security settings, virus scanning options, IME redirect service, and event logging.

Server Component	Role	Functions
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to view or change policies for basic mail filtering, file attachments, virus detection and security.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to view and create folders, domain records, and user records to which the policies apply.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access the mail queue, which allows the following:
		viewing the subject, sender, date and tag applied to each message;
		filtering the messages in the queue;
		releasing or deleting selected messages from the queue;
		saving some or all of the messages to an external file;
		or accessing the queue configuration.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to create event log filters, filter logged events, and find specific events by Instance ID.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to view, and configure event logs. Only MMS 2nd level administrator may delete the events.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to define additional custom events, as well as, modify or delete any custom event definitions.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to configure lists which include wordlists, addresses, attachments, and tags which all can be used to trigger a message policy. Also access is allowed for importing a previously defined list.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to define annotations to be included in messages as a disclaimer or confidentiality statement.
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to define notifications to be sent to the sender and/or the recipient for any specified policy violation.

Server Component	Role	Functions
MMS	MMS 1st level Administrator, and MMS 2nd level Administrator	Access to specify redirect of a message as a policy action.

5.1.4.2 Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1

755 The TSF shall enforce the *access control policy in Table 3b (Management of Security Attributes)* to restrict the ability to **modify** the security attributes, *shown in Table 3b,* to *the corresponding roles in Table 3b.*

Table 3b: Management of Security Attributes

Role	Attributes that role can modify
MMS 2nd level Administrator	Administrative roles, any password.
MMS 1st level administrator owning the password	MMS Administrator’s own password
IME Administrator	Administrative roles, any user password, and default package property security
IME Group Manager	User password for members of the manager’s group.
IME user owning the password	IME User’s own password

760 *5.1.4.3 Management of TSF Data (FMT_MTD.1)*

FMT_MTD.1.1

The TSF shall restrict the ability to **modify** the *MMS and IME configurations* to *the MMS 1st level administrator, and MMS 2nd level administrator, IME Administrator*.

765 *5.1.4.4 Specification of Management Functions (FMT_SMF.1)*

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: as listed in the functions column of Table 3a above.

5.1.5 TOE Protection (FPT)

5.1.5.1 Inter-TSF Confidentiality during Transmission (FPT_ITC.1)

FPT_ITC.1.1

The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

5.1.6 Trusted Path (FTP)

5.1.6.1 Inter-TSF trusted Channel (FTP_ITC.1)

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit **the TSF, the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for *communication between the MMS and IME components, communication between the IME and web server components*.

5.2 Explicitly Stated TOE Security Functional Requirements

This section provides an additional set of requirements that are explicitly stated to identify additional security functionality within the product that is not currently defined by CC.

790 5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FAU_IME_GEN.1)

FAU_IME_GEN.1.1

The TSF of the IME component shall be able to generate an audit record of the following auditable events:

795 a) Events defined within Table 4 (IME Auditable Events).

FAU_IME_GEN.1.2

The TSF of the IME component shall record within each audit record at least the following information:

800 a) Date and time of the event, type of event, source of event, user identity ***(if applicable)***, and a description of the event.

Table 4: IME Auditable Events

Audit Events:
Account creation
Account deletion
Account modification
Account enabling
Account disabling
Login

5.2.1.2 Archival of Triggered Policy Violations (FAU_MMS_ARC.1)

FAU_MMS_ARC.1.1

805 The TSF of the MMS component shall provide a mechanism for archiving messages that trigger policy violations for a later review by an authorized administrator.

5.2.1.3 Restricted Audit Review (FAU_IME_SAR.2)

FAU_IME_SAR.2.1

The TSF of the IME component shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.4 Selective Audit (FAU_MMS_SAR.3)

FAU_MMS_SAR.3.1

The TSF of the MMS component shall provide the ability to perform sorting of audit data based on *the date and time of an event, type of an event, source of an event, and an ID number relating to the description of an event.*

5.2.1.5 Action in case of possible audit data loss (FAU_MMS_STG.3)

FAU_MMS_STG.3.1

The TSF of the MMS component shall take action to delete stored audit records exceeding 30 days if the audit trail exceeds 30 days old.

5.2.2 Communication (FCO)

5.2.2.1 Selective Proof of Receipt (FCO_IME_NRR.1)

FCO_IME_NRR.1.1

The TSF of the IME component shall be able to generate evidence of receipt for received messages at the request of the originator.

FCO_IME_NRR.1.2

The TSF of the IME component shall be able to relate the identity of the recipient of the information, and the message of the information to which the evidence applies.

FCO_IME_NRR.1.3

The TSF of the IME component shall provide a capability to verify the evidence of receipt of the message to the originator.

5.2.2.2 Non-repudiation verification of origin (FCO_MMS_NRV.1)

FCO_MMS_NRV.1.1

The TSF of the MMS component shall be able to relate the originator of a message to the evidence supplied within the message.

FCO_MMS_NRV.1.2

The TSF of the MMS component shall generate an event if the evidence of origin of information is invalid.

5.2.3 User Data Protection (FDP)

5.2.3.1 Policy Engine (FDP_MMS_POL.1)

FDP_MMS_POL.1.1

The TSF of the MMS component shall provide a mechanism to enforce the actions identified in

Table 6 (Actions Related to Policies) to the policies described in Table 5 (MMS Policies) for each individual message.

Table 5: MMS Policies

Policy:	Description:
Basic Policy	This policy provides basic mail filtering through matching a message's subject, body, and attachments to a specified wordlist.
Attachment Policy	This policy filters attachment types included in messages.
Virus Policy	This policy provides scanning of messages for possible virus threats.
Security Policy	This policy provides the encryption and signature filters, a filter for security stripping so that other policies can apply, and a filter to ensure that encryption is being used for messages.

Table 6: Actions Related to Policies

Action:	Description:
Drop	Stops the message from being delivered and deletes it from the queue.
Return to Sender	Returns the message to the sender.
Quarantine	Stops the message from being delivered and moves it to the quarantine queue until an administrator reviews the message and determines an appropriate action.
Detain	Stops the message from being delivered and moves it to the detention queue where it will reside either for a specified period of time then deleted, or until an administrator has reviewed the message, which ever action occurs first.
Redirect	Redirects the message to the IME Server.
Defer Delivery	Temporarily stops messages that reach a particular size from being delivered until peak operation hours are surpassed.
Deliver Normally	The message may continue its normal delivery process.

5.2.3.2 Basic Data Exchange Confidentiality (FDP_IME_UCT.1)

FDP_IME_UCT.1.1

The TSF of the IME component shall enforce the *access control policy in Table 2 (Access Control Policy)* to be able to **transmit and receive** ***messages*** in a manner protected from unauthorized disclosure.

5.2.4 Identification & Authentication (FIA)

5.2.4.1 Authentication Failure Handling (FIA_IME_AFL.1)

FIA_IME_AFL.1.1

The TSF of the IME component shall detect when 10 consecutive unsuccessful authentication attempts occur related to authentication of an IME user or IME Administrator account.

FIA_IME_AFL.1.2

When the defined number of consecutive unsuccessful authentication attempts has been met or surpassed, the TSF of the IME component shall disable the specified account.

5.2.4.2 TSF Verification of Secrets (FIA_IME_SOS.1)

FIA_IME_SOS.1.1

The TSF of the IME component shall provide a password-based authentication mechanism to verify that secrets generated by IME Users meet the following requirements:

1. Secrets (passwords) must include a minimum of 8 characters;
2. Secrets (passwords) must include at least 1 numeric character, and 1 alphabetic character;

5.2.4.3 Timing of Authentication (FIA_IME_UAU.1)

FIA_IME_UAU.1.1

The TSF of the IME server shall allow *initiation of the log-in process and access to the help database* on behalf of the user to be performed before the user is authenticated.

FIA_ IME_UAU.1.2

The TSF of the IME server shall require each user to be successfully authenticated ***using the password-based authentication mechanism*** before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.4 User identification before any action (FIA_IME_UID.1)

FIA_IME_UID.1.1

The TSF of the IME server shall allow *initiation of the log-in process and access to the help database* on behalf of the user to be performed before the user is identified.

FIA_ IME_UID.1.2

The TSF of the IME server shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.5 External User authentication before any action (FIA_MMS_TOA.1)

FIA_MMS_TOA.1.1

The TSF of the MMS server will deny a user access to the TSF until the MMS Server has requested and obtained the user name and password and had the validity of these credentials confirmed by the environment.

5.2.5 Security Management (FMT)

5.2.5.1 Virus Definition Download (FMT_MMS_DNL.1)

FMT_MMS_DNL.1.1

The TSF of the MMS component shall provide a mechanism for the automatic downloading of virus definition files, at the minimum, on a daily basis and stores them within the MMS SQL database.

5.2.5.2 Static Attribute Initialization (FMT_IME_MSA.3)

FMT_IME_MSA.3.1

The TSF of the IME component shall enforce the access control policy in Table 2 (Access Control Policy) to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_IME_MSA.3.2

The TSF of the IME component shall allow the IME administrator to specify alternative initial values to override the default values when an object or information is created.

5.2.5.3 Revocation (FMT_IME_REV.1)

FMT_IME_REV.1.1

The TSF of the IME component shall restrict the ability to revoke security attributes associated with the users within the TSC to the IME administrator and to the relevant IME group manager.

FMT_IME_REV.1.2

The TSF of the IME component shall enforce the rules to revoke the attributes of the specified user immediately but not force the user to logout.

5.2.5.4 Security roles (FMT_IME_SMR.1)

FMT_IME_SMR.1.1

The TSF of the IME component shall maintain the roles of IME Administrator, IME Group Manager, IME Group Member, and IME Individual Account User.

FMT_IME_SMR.1.2

The TSF of the IME component shall be able to associate users with roles.

5.2.6 TOE Access (FTA)

5.2.6.1 TSF-Initiated Termination (FTA_SSL_EXP.3)

FTA_SSL_EXP.3.1

The TSF of the IME component shall terminate an interactive Administrator session after a 70 minute period of inactivity.

FTA_SSL_EXP.3.2

The TSF of the MMS component shall terminate an interactive Administrator session after a 30 minute period of inactivity.

FTA_SSL_EXP.3.3

The TSF shall terminate an interactive User session after a 70 minute period of inactivity.

5.3 Environmental Security Functional Requirements

The TOE environment must be responsible for providing a protected method for storing audit data, allowing rollback operations to be performed on critical data, and providing a reliable source for timestamps.

5.3.1 Security Audit (FAU)

5.3.1.1 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1

The ***IT Environment*** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The ***IT Environment*** shall be able to **prevent** modifications to the audit records.

5.3.2 Cryptographic Operation (FCS)

5.3.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1

The ***IT Environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm*s* *RSA, 3DES, & RC4* and specified cryptographic key sizes *2048/1024 (RSA), 168 (3DES), & 128 (RC4)* that meet the following *PKCS #1 & PKCS #7 standards (RSA), FIPS 46-3 standards (3DES), & registered algorithm of ISO 9979 (RC4)*.

5.3.2.2 Cryptographic Operation (FCS_COP.1)

FCS_COP.1.1

The ***IT Environment*** shall perform *operations shown in the following Table 7 (Cryptographic Operations)* in accordance with the specified cryptographic algorithm*, shown in the following Table 7 (Cryptographic Operations),* and cryptographic key sizes *shown in the following Table 7 (Cryptographic Operations)* that meet *the list of standards shown in the following Table 7 (Cryptographic Operations)*.

950 **Table 7: Cryptographic Operations**

Cryptographic Operations	Cryptographic Algorithms	Key Sizes (bits)	Conforming Standards
Symmetric session key generation	Triple DES (3DES)	168	FIPS 46-3
Data encryption/decryption	Triple DES (3DES)	168	FIPS 46-3
Public/private key generation	RSA	2048, 1024	PKCS #1, PKCS #7
Cryptographic key encryption/decryption	RSA	2048, 1024	PKCS #1, PKCS #7
Digital signature creation/verification	RSA	2048, 1024	FIPS 186-2, PKCS #1
Private Key Import	RSA	N/A	PKCS #12
Secure hash	MD5	N/A	PKCS #1, RFC 1320
Symmetric file key generation	RC4	128	A registered algorithm of ISO 9979
Data encryption/decryption	RC4	128	A registered algorithm of ISO 9979
Secure Envelope encryption	RC4	128	A registered algorithm of ISO 9979
File key encryption/decryption	RC2	128	RFC 2268
Secure hash	SHA-1	160	FIPS 180-1

5.3.3 Security Management (FMT)

5.3.3.1 Secure Security Attributes (FMT_MSA.2)

FMT_MSA.2.1

The ***IT Environment*** shall ensure that only secure values are accepted for security attributes.

955 5.3.4 TOE Protection (FPT)

5.3.4.1 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1

The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

5.4 Explicitly Stated Environmental Security Functional Requirements

960 The TOE environment must be responsible for providing a protected method for storing audit data, allowing rollback operations to be performed on critical data, and providing a reliable source for timestamps.

5.4.1 Security Audit (FAU)

5.4.1.1 Audit Data Generation (FAU_MMS_GEN.1)

965 **FAU_MMS_GEN.1.1**

The IT Environment of the MMS component shall be able to generate an audit record of the following auditable events:

a) Events defined within Table 8 (MMS Auditable Events).

FAU_MMS_GEN.1.2

970 The IT Environment of the MMS component shall record within each audit record at least the following information:

a) Date and time of the event, type of event, source of event, user identity ***(if applicable)***, and a description of the event.

5.4.1.2 User Identity Association (FAU_MMS_GEN.2)

975 **FAU_MMS_GEN.2.1**

For audit events resulting from actions of identified users, the IT Environment of the MMS component shall be able to associate each auditable event with the identity of the user that caused the event.

5.4.1.3 Action in case of possible audit data loss (FAU_IME_STG.3)

980 **FAU_IME_STG.3.1**

The IT Environment of the IME component shall take action to overwrite stored audit records if they are older than 30 days or if the audit trail exceeds 10048 KB.

Table 8: MMS Auditable Events

Audit Events:
MSSQL Events
Directory Entry: add, delete, update
Policy: add, delete, update
Directory Policy: attach, detach, enable, disable
Event Log(Id): add, delete, update
Tag: add, delete, update
Notification: add, delete, update
Annotation: add, delete, update
Shared List: add, delete, update
Admin UI
Queue Message: add annotation, delete, delete annotation, delete attachment, release to policy engine, release to recipient, return to sender, update SMTP recipients

5.4.1.4 Selective Audit (FAU_IME_SAR.3)

985 **FAU_IME_SAR.3.1**

The IT Environment of the IME component shall provide the ability to perform sorting of audit data based on event type, date, time, event category (IME component), event ID, and host name.

5.4.2 Cryptographic Operation (FCS)

5.4.2.1 Cryptographic Key Distribution (FCS_MMS_CKM.2)

FCS_MMS_CKM.2.1

The IT Environment of the MMS component shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method of a symmetric key wrapped with a public key that meets the following: FIPS 140-1 standard.

5.4.2.2 Cryptographic Key Destruction (FCS_MMS_CKM.4)

FCS_MMS_CKM.4.1

The IT Environment of the MMS component shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that destroys the key from memory after use by overwriting with zeros, destroys public keys by deleting from the MMS SQL database, and destroys private keys by replacing with a new private/public key pair that meets the following: FIPS 140-1 standard.

5.4.3 Identification & Authentication (FIA)

5.4.3.1 Database authentication (FIA_MMS_AUT.1)

FIA_MMS_AUT.1.1

The IT Environment of the MMS component shall confirm the validity of a user name / password pair passed by the MMS server.

5.4.3.2 Security roles (FMT_MMS_SMR.1)

FMT_MMS_SMR.1.1

The IT Environment of the MMS component shall maintain the roles of MMS 1st level administrator, and MMS 2nd level administrator.

FMT_MMS_SMR.1.2

The IT Environment of the MMS component shall be able to associate users with roles.

5.5 TOE Security Assurance Requirements

1015 The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL 2+ level of assurance. The assurance components are summarized in the following table.

Table 9: Assurance Components (EAL 2+)

Assurance Class	Assurance Components	
Class ACM: Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Class ADO: Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Class ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing
Class AVA: Vulnerability Assessment:	AVA_SOF.1	Strength of TOE security functions evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.5.1 ACM: Configuration Management

5.5.1.1 ACM_CAP.3: Authorisation controls

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.3.newC The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.1.2 ACM_SCP.1: TOE CM coverage

Developer action elements:

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.2 ADO: Delivery and Operation

5.5.2.1 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.2.2 ADO_IGS.1 Installation generation and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.5.3 ADV: Development

5.5.3.1 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.5.3.2 ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.5.3.3 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.4 AGD: Guidance Documents

5.5.4.1 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.4.2 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.5 ATE: Tests

5.5.5.1 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.5.2 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.5.3 ATE_IND.2 Independent testing – sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.5.6 AVA: Vulnerability Assessment

5.5.6.1 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.5.6.2 AVA_VLA.1 Developer vulnerability analysis

1240 **Developer action elements:**

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

1245 **AVA_VLA.1.1C** The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

1250 **AVA_VLA.1.2E** The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.6 Strength of Function Claim

A Strength of Function (SOF) claim of SOF-Basic is provided. The SOF claim is valid for the timing of authentication (FIA_IME_UAU.1), verification of secrets (FIA_IME_SOS.1), and authentication failure handling (FIA_IME_AFL.1) TOE security functional requirements. These SFRs identify a password-based authentication mechanism for IME that verifies secrets for IME user accounts and authentication data, and provides authentication failure handling for all four types of IME accounts.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the security requirements stated within section 5.1. A mapping of the security functions identified and their related security requirements can be found within Table 19, section 8.3.1.

The identification & authentication function is the only function realized by a probabilistic or permutational mechanism. The probabilistic or permutational mechanism realized by the identification & authentication function is the password-based authentication mechanism.

6.1.1 Audit Function

The auditing function provides the ability to generate audit data for the IME component. The IME component will record the date and time of the event, type of event, source of event, user identity (if applicable), and a description of the event.

The audit function provides the ability to read all information within the audit data for the MMS and IME components of the TOE. For MMS, both 1st level MMS administrator and 2nd level MMS administrator have access to view the audit data. MMS audit data is available only through the MMS Web-Based Administrative Interfaces and may be accessed by selecting the Event Log menu from the MMS Menu. For IME, audit data is only accessible by the IME Administrator. IME audit data is available only through the IME Web-Based Administrative Interfaces and may be accessed by selecting the Events menu from within the Server menu. IME users are prohibited access to view the audit data generated by MMS or IME. IME users are only capable of accessing IME through the IME Web-Based User Interfaces.

The auditing function provides the capability to sort through the audit data generated by MMS based on the date and time of an event, type of an event, source of an event, and an ID number relating to the description of an event. The sorting of audit data is provided within the MMS Web-Based Administrative Interfaces by selecting, "Event Log", from the, "MMS Menu". The sorting of audit data is only provided by MMS, not IME.

The auditing function provides within the MMS component an archival service. The archival service archives any message that violates any of the MMS policies that are configured to archive a message upon violation so that the message may be reviewed at a later time for reasons of violation. Messages that are archived are stored within the following directory, "%SystemDrive%\Program Files\Tumbleweed\MMS\MMSArchive" and are stored as an ".msg" file format. The archived messages may be viewed by opening the file with any text editor.

The audit function provides MMS the capability to configure the action to be taken in the event of the audit trail becoming full. The action specified for this security function is to overwrite audit data older than 30 days when the audit trail exceeds 30 days old. The configuration of the audit trail is done by accessing the MMS Web-Based Administrative Interfaces, selecting, "Event Log", from the, "MMS Menu", and then selecting "Setup Event Logging". The action is implemented by the MMS Server issuing SQL statements to the MMS SQL Server.

For IME, the audit records are stored within the Windows 2000 Application Event Log, which is located within the following file, "%SystemDrive%\WINNT\system32\config\AppEvent.Evt".

For MMS, the audit records are stored within the MMS database located in the MMS SQL 2000 Database Server. Audit events relating to administrator actions are stored within the "AuditLogEvents" table of the MMS database. All other audit events are stored within the "EventLogEvents" table of the MMS database.

In addition to audit records, the audit function provides IME the ability for a sender to receive a receipt of delivery indicating that the intended recipient(s) has successfully received the message. This is accomplished by a user selecting the option, "Email me when package is viewed", when sending a message. Additionally, IME also provides a column for tracking within the outbox for an IME Group Member, IME Group Manager and IME Individual Account User. This tracking column allows an IME user to view the send and receive status for each message sent. The send and receive status is shown separately for each recipient of the message.

6.1.2 Identification & Authentication Function

The identification & authentication function is realized as a probabilistic or permutational mechanism by the password-based authentication mechanism of the IME component. The identification & authentication function is provided by both the IME and MMS components. However, the I&A process is initiated through the HTTPS protocol which requires the use of a web server and web browser.

The identification & authentication function provides users and administrators the ability to authenticate to the MMS and IME servers via the respective web-based interfaces for each server. The MMS and IME servers both operate within an isolated network and are accessed remotely for use and administration. Therefore, authentication by the operating system is not exercised.

The identification & authentication function provides a password-based authentication mechanism for authentication to the IME component. This is a probabilistic mechanism which claims a SOF of basic for all four types of IME accounts. Although MMS enforces password-based authentication prior to allowing access to manage MMS, the password-based authentication mechanism is not provided by the MMS component. No SOF claim is made for the MMS server. Instead, the password-based authentication mechanism for MMS is provided by the SQL Server installed locally on the MMS Server. IME users are required to identify themselves with either an ID or an e-mail address and then authenticate by providing the correct password associated with that ID or email address. IME and MMS Administrators are required to identify themselves with an ID and then authenticate by providing the correct password associated with that ID.

During the process of authentication to MMS and IME feedback is provided to the user attempting to authenticate. The details of the feedback are outlined in the next two paragraphs.

The IME Server provides feedback for the indication of how many characters have been typed in the password field without showing the characters themselves by substituting each character with a dot, indication of the account name in clear text being authenticated, indication of authentication failure, indication of how many unsuccessful authentication attempts are allowed before the account is locked, indication of an invalid account name, and indication of the account being locked out.

The MMS Server provides feedback for the indication of how many characters have been typed in the password field without showing the characters themselves by substituting each character with a dot; it also provides indication of the account name in clear text being authenticated and of authentication failure.

The identification & authentication function additionally require users to identify themselves successfully before allowing any other actions to be performed on the TOE, with the exception of access to the help database.

Once users initially authenticate themselves to the IME, the IME Security Manager subsystem creates a session for that user. Additionally, at login, the IME HTTP Gateway creates a token, associated with the user's identity which it passes with all requests associated with the session. This protects against session hijack.

The identification & authentication function of IME provides protection against brute force attacks and dictionary attacks. Brute force attacks are countered by providing a policy that temporarily disables a user's account after ten unsuccessful attempts have been reached. This will prevent violations caused by attackers running scripts that attempt authentication to a known user account with a list of known passwords. If a user's account is temporarily disabled, the user's account remains disabled until an IME Administrator has re-enabled the user's account. This capability is not provided by MMS.

The threat of dictionary attacks is countered through the verification of secrets for the password based identification & authentication function of IME Users. Note that this does not apply to IME Administrators. This mechanism verifies that each password selected for authentication of an IME User meets the requirements of having at least 8 characters. Within those 8 characters, at least one is required to be numeric, and at least one is required to be alphabetic

Each password is encrypted and then given a hash through the randomness of the output provided by the pseudorandom number generator that is seeded by system specific data, and resulting with a hash of at least 8 bytes of data. Therefore, the password would be unrecoverable without knowledge of the randomly generated seed that is hashed with the password.

The identification & authentication function provides IME the capability to revoke an IME Group Member and IME Individual Account User's password. These capabilities are provided only to the IME Administrator and IME Group Manager, if the user is managed in a group.

6.1.3 Message Security Function

The message security function provides MMS the ability to check incoming and outgoing messages against defined MMS policies and to enforce actions defined by each policy. The policies enforced by MMS can be pre-defined policies or custom-defined policies. Pre-defined policies include a basic policy, attachment policy, virus policy, security policy. When a message is checked against policies defined within MMS, MMS checks the message against all policies enabled. Then applies actions based on each policy that is triggered. To help enforce the virus policy, the message security function provides a mechanism for the automatic downloading of virus definition files on a daily basis. Therefore, a message is always scanned against the latest viruses available.

The message security function, with support of the IT Environment (i.e. RSA Crypto-C), provides MMS the ability to verify the validity of digital signatures applied to messages sent to MMS. When a signed message is received by MMS, an automatic lookup of the originator's public key certificate is performed. Once the public key certificate is retrieved, the digital signature is then verified. MMS does not require every message to be digitally signed. Yet in the event that a signed message is received, MMS will provide the capability to verify the validity of the digital signature.

6.1.4 Role-Based Access Function

The MMS and IME products provide control of all access to the resources they provide. Therefore, the operating systems that both MMS and IME reside on do not enforce any access to the IME users or MMS and IME administrators. The Role-Based access function provides the ability to have a defined list for access control without the possibility of modifying the access rights. The access control policy defined within Table 2 (Access Control Policy) is a Role-Based policy that cannot be modified at any given time. The access rights are hard coded into the MMS and IME products.

The access control policy provides a secure means of access control for the users of the IME server since the users are only allowed access to their individual mailbox, address list, folders, and password. Through this secure means of access control, the TOE is capable of sending and receiving messages in a manner protected from unauthorized disclosure. The access control policy protects access by enforcing the following restrictions.

- IME Administrators can change any password.
- IME Group Managers can change the password of any member of their group
- All categories of users can change their own password.

Additionally, the access control policy provides the IME Administrator the capability to specify the default package property security delivery method for each user category (type). By allowing this option, the IME Administrator configures this option to set the default delivery method to be account-based security.

When a Secure Envelope package is created, the IME server encrypts the Secure Envelope package using either the package password provided by the sender or the account password of the intended recipient. Therefore when the Secure Envelope package is delivered to the recipient, the recipient must authenticate to the Secure Envelope package using either the package password provided by the sender or the recipient's IME issued account password. Note the authentication occurs outside the TOE and no assurance or SOF is claimed for this mechanism. The TOE claims that it can securely create the packages but cannot assure actions outside the TOE boundary. Once authentication is successfully provided, the recipient is then able to view the Secure Envelope package.

The access control policy provides a secure means of access control for the administrators of the MMS server since there is a separation of administrative roles provided. The MMS 1st level administrator is allowed all administrative actions, except for specifying additional administrative accounts and modifying the audit log. This gives accountability to all MMS 1st level administrators since all their actions are audited, and they are unable to modify the audit log reflecting their actions. Only MMS 2nd level administrators are provided full access to add additional administrative accounts, and modify the audit log (e.g. delete events).

6.1.5 Role Management Function

The role management function provides protection of system data through the use of the access control policy.

The IME component provides a separation of roles for administrators and users of IME. IME associates a role for each user identity. There is only one role for an administrator of IME, which is IME Administrator. The IME Administrator has access to modify all IME User accounts and IME system configurations. However, there are three different IME User roles. The first User role is an IME Group Manager. An IME Group Manager typically is a standard user, yet with the additional capability to add additional users to the group, as well as, remove members and change their passwords. The second user role is an IME Group Member, which is a member of an IME Group. The third IME user role is an IME Individual Account User, not a member of a group, but just an individual user account.

The IME administrator has the capability to determine, as well as modify the current state of the security options and services within the IME component.

Although a separation of roles for administrators of MMS is provided, the MMS component does not directly provide this functionality.

6.1.6 Trusted Path Function

The trusted path function provides a means of secure communication between the MMS and IME components, as well as between the IME and web server components. The communication path is provided by the CORBA / IIOP protocol over SSL encryption. The CORBA portion of the function is based upon an open source protocol developed for integrating various machines and programming languages to a common interface, so that various types of applications can easily communicate. The IIOP portion of the interface provides TCP/IP interoperability within the CORBA protocol so that the CORBA communication path may be established over the internet. To make the interface a whole security package, the CORBA / IIOP communication path is encrypted using the OpenSSL toolkit. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, fully featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The OpenSSL project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

This communication channel protects the data transmissions from unauthorized disclosure by encrypting the contents during transmission. The trusted path function provides assured identification of both components (MMS - IME, IME - web server) prior to initiating the transmission by encrypting the contents with the IME, MMS, or HTTP Gateway's public key thereby only allowing the intended TOE component to be able to decrypt the transmission. In addition, a configuration option is specified within CORBA as to what specific IP is to be communicated with so that the encrypted transmission will only be initiated to this specific IP address.

In addition to CORBA, the trusted path function provides the capability to automatically terminate MMS and IME Administrator sessions and IME user sessions that remain inactive for a period longer than specified.

6.2 Security Mechanisms

There is no security mechanism referred to within this ST.

6.3 Strength of Function Claim

A Strength of Function (SOF) claim of SOF-Basic is provided. The SOF claim made for all four types of IME accounts on the IME server is dependant upon the functional requirements FIA_IME_UAU.1, FIA_IME_SOS.1, and FIA_IME_AFL.1, which identify a password-based authentication mechanism for IME that verifies secrets for all four types of IME accounts' authentication data and provides authentication failure handling. This SOF claim is explicitly stated for the IME component of the TOE. No SOF claim is made in relation to the package passwords.

No SOF claim is made for the MMS Server because the authentication mechanism is primarily enforced by the environment.

6.4 Assurance Measures

The assurance requirements for this TOE are met by EAL 2+, which stresses assurance through Tumbleweed's actions that are within the bounds of good commercial practice. These assurance requirements provide, primarily via review of Tumbleweed-supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

1. Confirmation of system generation and installation procedures
2. Verification that the system security state is not misrepresented
3. Verification of a sample of the vendor functional testing
4. Independent functional testing
5. Searching for obvious vulnerabilities

To define the assurance measures claimed to satisfy the security assurance requirements specified in Section 5.3, a mapping is provided between the Assurance Requirements and the Assurance Measures, which are intended to satisfy the Assurance Requirements. As shown in Table 10 (Assurance Measures that Fulfill Assurance Requirements (EAL 2+)), the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

The following table represents the assurance requirements for an assurance level of EAL 2+, along with a mapping of the assurance measures (Tumbleweed MMS and IME documentation (TW-MMS&IME)) that are required to demonstrate the products conformance to an EAL 2+ assurance level.

Table 10: Assurance Measures that Fulfill Assurance Requirements (EAL 2+)

Assurance Requirements:	Assurance Requirement Description:	Assurance Measures: (TW-MMS&IME Documentation)
ACM_CAP.3	Authorisation controls	Configuration Management Plan for Tumbleweed MMS ™ and IME ™ Version 5.5.3
ACM_SCP.1	TOE CM coverage	Configuration Management Plan for Tumbleweed MMS ™ and IME ™ Version 5.5.3
ADO_DEL.1	Delivery procedures	Delivery Procedures for Tumbleweed MMS ™ and IME ™ Version 5.5.
ADO_IGS.1	Installation, generation, and start-up procedures	Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5, made within the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.

Assurance Requirements:	Assurance Requirement Description:	Assurance Measures: (TW-MMS&IME Documentation)
ADV_FSP.1	Informal functional specification	Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5.3, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3, made the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5.

Assurance Requirements:	Assurance Requirement Description:	Assurance Measures: (TW-MMS&IME Documentation)
ADV_HLD.2	Security enforcing high-level design	High-Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within the High Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5. Section 3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within the High Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3, made within the High Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help, made within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5.

Assurance Requirements:	**Assurance Requirement Description:**	**Assurance Measures: (TW-MMS&IME Documentation)**
ADV_RCR.1	Informal correspondence demonstration	Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. High-Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5.
AGD_ADM.1	Administrator guidance	Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 References to the following documents made in the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3. • Tumbleweed MMS Administrator's Guide, Release 5.5. • Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5. • Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5.
AGD_USR.1	User guidance	Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help (collection of HTML files).
ATE_COV.1	Evidence of coverage	Testing Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5.
ATE_FUN.1	Functional testing	Testing Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5.
ATE_IND.2	Independent testing - sample	Tumbleweed MMS ™ and IME ™ Version 5.5 products.
AVA_SOF.1	Strength of TOE security function evaluation	Vulnerability Analysis Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5.
AVA_VLA.1	Developer vulnerability analysis	Vulnerability Analysis Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5.

7 Protection Profile Claims

1505 There are no protection profile claims for this security target.

8 Rationale

This section demonstrates the completeness and consistency of this ST.

- *Traceability:* The security objectives for the IT and environment are explained in terms of OSPs, 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:

  a) security objectives to OSPs and/or threats countered

  b) objectives to assumptions met

  c) SFRs to objectives met

- *Assurance Level:* A justification is provided for selecting an EAL 2+ level of assurance for this ST.
- *SOF:* A rationale is provided for the SOF level chosen for this ST.
- *Dependencies:* A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This section provides evidence demonstrating coverage of the security objectives as they were derived exclusively from statements of OSPs, threats and assumptions. The following table and corresponding discussion provides evidence of coverage for each statement of organizational security policy.

Table 11: Security Environment mapped to Security Objectives for the TOE

Objectives for the TOE Security Environment	O.AC_Admin_Limit	O.Admin_Guidance	O.Archive_Messages	O.Audit_Gen	O.Audit_Review	O.Audit_Clear	O.Auth_Failure	O.Data_Exchange_Conf	O.Authentication	O.MsgMod_ID	O.NonRepudiate_Recd	O.NonRepudiate_Sent	O.Pass_Auth	O.Protect_Accounts	O.Pol_Eng	O.SE_Auth	O.Security_Attr_Mgt	O.Security_Func_Mgt	O.Security_Roles	O.Session_Termination	O.Trusted_Path	O.User_Attributes	O.Virus_Updates
Organizational Security Policies																							
P.Message_Archive			X																				
P.Policy_Engine															X								
Threats																							
T.Admin_Err_Commit	X	X		X	X														X				
T.Admin_Err_Omit	X	X		X	X																		
T.Admin_Hostile_Modify	X	X		X	X												X	X	X				
T.Admin_UserPriv	X	X				X			X														
T.Audit_Exhastion						X																	
T.Brute_Force							X		X				X										
T.Hack_Comm_Eavesdrop								X													X		
T.Hack_Masq							X		X				X	X						X			
T.Hack_Msg_Data										X													
T.New_Virus																							X
T.Repudiate_Receive											X												

Objectives for the TOE Security Environment	O.AC_Admin_Limit	O.Admin_Guidance	O.Archive_Messages	O.Audit_Gen	O.Audit_Review	O.Audit_Clear	O.Auth_Failure	O.Data_Exchange_Conf	O.Authentication	O.MsgMod_ID	O.NonRepudiate_Recd	O.NonRepudiate_Sent	O.Pass_Auth	O.Protect_Accounts	O.Pol_Eng	O.SE_Auth	O.Security_Attr_Mgt	O.Security_Func_Mgt	O.Security_Roles	O.Session_Termination	O.Trusted_Path	O.User_Attributes	O.Virus_Updates
T.Repudiate_Send												X											
T.User_Abuse_Conf								X															
T.User_Conf																X							
T.User_Misuse_Avl_Resc																			X			X	
T.User_Modify				X	X																		

1525

Table 12: Security Environment mapped to Security Objectives for the TOE Environment

Objectives for the TOE Environment **Security Environment**	**OE.Adm_Roles**	**OE.Audit_Clear**	**OE.Audit_Gen**	**OE.Audit_Storage**	**OE.Audit_Review**	**OE.Authentication**	**OE.Competent_User**	**OE.Crypto_Operation**	**OE.MsgMod_ID**	**OE.NonRepudiate_Sent**	**OE.Physical_Control**	**OE.SE_Crypto_Ops**	**OE.SE_Key_Gen**	**OE.Timestamp**	**OE.Trustworthy_Administrators**	**OE.Trustworthy_User**
Assumption																
A.Admin															X	
A.Locate											X					
A.Message_Secure							X									
A.Timestamp														X		
A.User_Auth_Credentials																X
Threats																
T.Admin_Err_Commit	X		X	X	X											
T.Admin_Err_Omit	X		X	X	X											
T.Admin_Hostile_Modify	X		X	X	X											
T.Brute_Force						X										
T.Hack_Comm_Eavesdrop								X								
T.Hack_Masq						X										

Objectives for the TOE Environment Security Environment	OE.Adm_Roles	OE.Audit_Clear	OE.Audit_Gen	OE.Audit_Storage	OE.Audit_Review	OE.Authentication	OE.Competent_User	OE.Crypto_Operation	OE.MsgMod_ID	OE.NonRepudiate_Sent	OE.Physical_Control	OE.SE_Crypto_Ops	OE.SE_Key_Gen	OE.Timestamp	OE.Trustworthy_Administrators	OE.Trustworthy_User
T.Hack_Msg_Data								X	X			X	X			
T.Repudiate_Send										X						
T.User_Modify			X	X	X											
TE.Audit_Data_Integrity				X												
TE.Audit_Exhastion		X														

8.1.1 Security Objectives Coverage

1530 **Table 13: Security Objectives Coverage**

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
Assumptions	
A.Admin *It is assumed that one or more authorized administrators are assigned who are competent to manage the SQL 2000 Database Servers for MMS and IME, the Internal and External HTTP Gateways, the IIS 5.0 web server for MMS, and the Windows 2000 operating systems of MMS and IME, who are competent to manage the security of the information these systems contain, and who can be trusted not to deliberately abuse their privileges so as to undermine security.*	**OE.Trustworthy_Administrators** covers this assumption by ensuring that resources containing data maintained by the TOE are managed by administrators whom are competent and trustworthy of performing their administration duties.
A.Locate *The processing resources of the TOE are assumed to be located within controlled access facilities which will restrict unauthorized physical access.*	**OE.Physical_Control** covers this assumption by ensuring that the facilities surrounding the TOE are physically protected from unauthorized entry.
A.Message_Secure *The IME user will select the proper security protections for messages (e.g. encrypt, plaintext)*	**OE.Competent_User** covers this assumption by ensuring that users of the TOE will be adequately trained to know the implications in selecting the proper security protection level for messages (e.g. sign, encrypt, plaintext).
A.Timestamp *A reliable source of time shall be provided by the Windows 2000 operating systems for MMS, IME, and the two HTTP Gateways communicating with IME.*	**OE.Timestamp** covers this assumption by ensuring that the Windows 2000 operating systems for MMS, IME, and the two HTTP Gateways communicating with IME are trusted to be reliable sources for time.
A.User_Auth_Credentials *The user will not disclose their password.*	**OE.Trustworthy_User** covers this assumption by ensuring that all users of the TOE are trusted not to disclose their passwords (e.g. PIN, password), to prevent unauthorized access of their account.
Policies	

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
P.Message_Archive: Archival of messages triggered by policy violations *All messages detected to violate a policy shall be archived for review by a local administrator of the MMS Server's operating system.*	**O.Archive_Messages** covers this policy by archiving all messages that violate any of the MMS defined policies, so that they may be viewed at a later time by the local administrator of the MMS Server's operating system.
P.Policy_Engine: Policy Engine *All messages shall be subject to review by the policies defined within the policy engine.*	**O.Pol_Eng** covers this policy through enforcing all messages to be reviewed by all of the MMS configured policies and apply appropriate actions to any messages in violation of the specified configured policies.
Threats	
T.Admin_Err_Commit: Administrative errors of commission *An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.*	**O.AC_Admin_Limit** covers this threat through designing administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions. **OE.Adm_Roles** covers this threat through restricting the capabilities for MMS 1st level administrators to add additional administrative accounts, and modifying the audit log. This is accomplished by providing an MMS 2nd level administrator strictly for those functions. **O.Admin_Guidance** covers this threat by providing adequate administrator guidance. **O.Audit_Review** mitigates this threat by ensuring that omitted administrator action can be detected and corrected. **OE.Audit_Review** supports **O.Audit_Review** by providing sorting capabilities for IME audit data. **O.Audit_Gen** supports **O.Audit_Review** by generating the IME audit events This objective applies only to the IME. **OE.Audit_Gen** supports **O.Audit_Review** by generating the MMS audit events. **OE.Audit_Storage** supports **O.Audit_Review** by protecting the integrity of the audit trail.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.Admin_Err_Omit: Administrative errors of omission *The MMS 1st level administrator, MMS 2nd level administrator, or IME administrator fails to perform some function essential to security.*	**O.AC_Admin_Limit** covers this threat through designing administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions. **OE.Adm_Roles** covers this threat through restricting the capabilities for MMS 1st level administrators to add additional administrative accounts, and modifying the audit log. This is accomplished by providing an MMS 2nd level administrator strictly for those functions. **O.Admin_Guidance** covers this threat by providing adequate administrator guidance. **O.Audit_Review** mitigates this threat by ensuring that omitted administrator action can be detected and corrected. **OE.Audit_Review** supports **O.Audit_Review** by providing sorting capabilities for IME audit data. **O.Audit_Gen** supports **O.Audit_Review** by generating the IME audit events. This objective applies only to the IME. **OE.Audit_Gen** supports **O.Audit_Review** by generating the MMS audit events. **OE.Audit_Storage** supports **O.Audit_Review** by protecting the integrity of the audit trail.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.Admin_Hostile_Modify: Hostile administrator modification of user or system data *An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.*	**O.AC_Admin_Limit** covers this threat through designing administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions. **OE.Adm_Roles** covers this threat through restricting the capabilities for MMS 1st level administrators to add additional administrative accounts, and modifying the audit log. This is accomplished by providing an MMS 2nd level administrator strictly for those functions. **O.Security_Attr_Mgt** covers this threat by limiting the possible changes to security attributes. **O.Security_Func_Mgt** covers this threat by limiting the possible changes to security mechanisms. **O.Admin_Guidance** covers this threat by providing adequate administrator guidance. **O.Audit_Review** removes this threat by removing the motivation of the attacker through deterrence. **OE.Audit_Review** supports **O.Audit_Review** by providing sorting capabilities for IME audit data. **O.Audit_Gen** supports **O.Audit_Review** by generating the IME audit events. This objective applies only to the IME. **OE.Audit_Gen** supports **O.Audit_Review** by generating the MMS audit events. **OE.Audit_Storage** supports **O.Audit_Review** by protecting the integrity of the audit trail.
T.Admin_UserPriv: Administrator violates user privacy policy *An MMS 1st level administrator, MMS 2nd level administrator, or IME administrator which has full access privileges gains knowledge of privacy-related information such as the identity of an IME user.*	**O.AC_Admin_Limit** covers this threat by designing administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions. **O.Admin_Guidance** covers this threat by providing adequate administrator guidance.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.Audit_Exhaustion: Hacker fills the MMS audit log *A hacker might exhaust the storage capacity of the audit trail of the MMS sever in order to prevent the auditing of unauthorized access.*	**O.Audit_Clear** covers this threat by providing a facility to remove outdated MMS audit records and to overwrite the oldest records when storage limits are reached. This objective applies only to the MMS.
T.Brute_Force: Brute force attack on passwords *A hacker repeatedly attempts password authentication on known IME User accounts to gain unauthorized access of those accounts.*	**O.Authentication** supports this policy by requiring that a valid user identity / password pair be presented before giving any other access to the TOE. **OE.Authentication** supports O.Authentication by providing the MMS server with the environmental capability to verify authentication data. **O.Auth_Failure** covers this threat by providing the ability to temporarily disable IME users' accounts based on a defined number of authentication failures to the specified account. This objective applies only to the IME. **O.Pass_Auth** covers this threat by providing a mechanism that verifies user-generated secrets for password-based authentication of IME Users.
T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications *A hacker obtains IME user data by eavesdropping on communications lines.*	**OE.Crypto_Operation** covers this threat by fully defining cryptographic components, functions, and interfaces. **O.Data_Exchange_Conf** covers this threat by providing the ability to protect IME user data confidentiality. **O.Trusted_Path** covers this threat by providing an encrypted communication channel between components of the TOE and between the TOE and other entities.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.Hack_Masq: Hacker masquerading as a legitimate user or as system process *A hacker masquerades as an authorized user or system process to perform operations that will be attributed to the authorized user or a system process.*	**O.Authentication** supports this policy by requiring that a valid user identity / password pair be presented before giving any other access to the TOE. **OE.Authentication** supports O.Authentication by providing the MMS server with the environmental capability to verify authentication data. **O.Auth_Failure** covers this threat by providing the ability to temporarily disable IME users' accounts based on 10 unsuccessful authentication attempts to the specified account. This objective applies only to the IME. **O.Pass_Auth** covers this threat by providing a mechanism that verifies user-generated secrets for password-based authentication of IME Users. This objective applies only to the IME. **O.Session_Termination** covers this threat by terminating a session after a given interval of inactivity. **O.Protect_Accounts** covers this threat by ensuring that the TOE does not give feedback which might compromise the confidentiality of the passwords during the logon process.
T.Hack_Msg_Data: Message content modification *A hacker modifies information within a message and thereby deceiving the intended recipient.*	**OE.Crypto_Operation** covers this threat by fully defining cryptographic components, functions, and interfaces. **O.MsgMod_ID** covers this threat by detecting modifications made to a signed message during transit or by replay. **OE.MsgMod_ID** supports the above objective in meeting the threat by providing cryptographic support from the environment for the verification of signed messages. **OE.SE_Crypto_Ops** covers this threat by providing the encryption, decryption, and hashing of packages sent via Secure Envelope. **OE.SE_Key_Gen** covers this threat by providing the generation of keys for packages sent via Secure Envelope, and allowing these Secure Envelope packages to retain their content integrity during transmission and storage.
T.New_Virus: Newly discovered virus *An attacker sends a message with a newly discovered virus that is undetected by virus scanners that have not been updated.*	**O.Virus_Updates** covers this threat by automatically checking for and updating with new virus patterns.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.Repudiate_Receive: Recipient denies receiving information *The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.*	**O.NonRepudiate_Recd** covers this threat by providing evidence to prevent IME users from avoiding accountability of received messages.
T.Repudiate_Send: Sender denies sending information *The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.*	**O.NonRepudiate_Sent** covers this threat by evaluating digital signatures provided in messages sent to MMS with the public key certificate related to the originator of the message. **OE.NonRepudiate_Sent** supports the above objective in meeting the threat by providing cryptographic support from the environment.
T.User_Abuse_Conf: Hostile user acts cause confidentiality breaches *An IME user gains unauthorized access to read, modify or remove IME Packages sent or received by another IME User.*	**O.Data_Exchange_Conf** covers this threat by providing the capability of protecting IME Group Member, IME Group Manager and IME Individual Account User data confidentiality.
T.User_Conf: Unauthorised access to message An unauthorised user of low attack potential gains access to a message sent to an individual without an IME account.	**O.SE_Auth** removes this threat removes this threat by requiring that the TOE create Secure Envelope packages at the request of the user, which will force the recipient to authenticate themselves to the environment prior to reading the message.
T.User_Misuse_Avl_Resc: User's misuse causes denial of service *An IME user's unauthorized use of resources causes an undue burden on an affected resource.*	**O.Security_Roles** covers this threat by maintaining security-relevant roles for IME and the association of individuals with those roles. This objective applies only to the IME. **O.User_Attributes** supports the above objectives by maintaining a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity (e.g. email address). This provides the information the above objectives use to make the access control decisions.

Assumptions, Policies, and Threats	Objectives for the TOE and Environment
T.User_Modify: User abuses authorization to modify data *A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.*	**O.Audit_Review** removes this threat by removing the motivation of the attacker through deterrence. **O.Audit_Gen** supports **O.Audit_Review** by generating the IME audit events. This objective applies only to the IME. **OE.Audit_Gen** supports **O.Audit_Review** by generating the MMS audit events. **OE.Audit_Storage** supports **O.Audit_Review** by protecting the integrity of the audit trail.
TE.Audit_Data_Integrity: A user modifies audit records *A user modifies audit records stored in the environment in an attempt to cover up actions that were previously performed.*	**OE.Audit_Storage** removes this threat by protecting the integrity of the stored audit data from unauthorized deletion.
TE.Audit_Exhastion: Hacker fills the IME audit log *A hacker might exhaust the storage capacity of the audit trail of the IME sever in order to prevent the auditing of unauthorized access.*	**OE.Audit_Clear** covers this threat by providing a facility to remove outdated IME audit records and to overwrite the oldest records when storage limits are reached.

8.2 Security Requirements Rationale

This section provides evidence demonstrating that the security objectives for the TOE and the TOE IT Environment is satisfied by the security requirements.

These mappings demonstrate that all TOE security requirements can be traced back to one or 1535 more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Security Requirements Coverage

This section provides evidence demonstrating that the security objectives of the TOE and TOE Environment are satisfied by the security requirements of the TOE and TOE Environment. The 1540 following tables provide the security requirement to security objective mappings.

Table 14: Mapping of Security Objectives to Security Requirements for the TOE

Objectives for the TOE SFRs	O.AC_Admin_Limit	O.Admin_Guidance	O.Archive_Messages	O.Audit_Gen	O.Audit_Review	O.Audit_Clear	O.Auth_Failure	O.Data_Exchange_Conf	O.Authentication	O.MsgMod_ID	O.NonRepudiate_Recd	O.NonRepudiate_Sent	O.Pass_Auth	O.Protect_Accounts	O.Pol_Eng	O.SE_Auth	O.Security_Attr_Mgt	O.Security_Func_Mgt	O.Security_Roles	O.Session_Termination	O.Trusted_Path	O.User_Attributes	O.Virus_Updates
ADO_DEL.1		X																					
ADO_IGS.1		X																					
AGD_ADM.1		X																					
FAU_IME_GEN.1				X																			
FAU_MMS_ARC.1			X																				
FAU_SAR.1					X																		
FAU_IME_SAR.2					X																		
FAU_MMS_SAR.3					X																		
FAU_MMS_STG.3						X																	
FCO_IME_NRR.1											X												
FCO_MMS_NRV.1										X		X											
FDP_ACC.1	X																					X	
FDP_ACF.1	X															X						X	
FDP_MMS_POL.1															X								
FDP_IME_UCT.1								X															
FIA_IME_AFL.1							X																

Objectives for the TOE SFRs	O.AC_Admin_Limit	O.Admin_Guidance	O.Archive_Messages	O.Audit_Gen	O.Audit_Review	O.Audit_Clear	O.Auth_Failure	O.Data_Exchange_Conf	O.Authentication	O.MsgMod_ID	O.NonRepudiate_Recd	O.NonRepudiate_Sent	O.Pass_Auth	O.Protect_Accounts	O.Pol_Eng	O.SE_Auth	O.Security_Attr_Mgt	O.Security_Func_Mgt	O.Security_Roles	O.Session_Termination	O.Trusted_Path	O.User_Attributes	O.Virus_Updates
FIA_IME_SOS.1													X										
FIA_IME_UAU.1									X														
FIA_UAU.7														X									
FIA_IME_UID.1									X														
FIA_MMS_TOA.1									X														
FMT_MMS_DNL.1																							X
FMT_MOF.1																		X					
FMT_MSA.1																	X					X	
FMT_IME_MSA.3																	X					X	
FMT_MTD.1																		X					
FMT_SMF.1																	X	X				X	
FMT_IME_REV.1																						X	
FMT_IME_SMR.1				X															X				
FPT_ITC.1								X													X		
FTA_SSL_EXP.3																				X			
FTP_ITC.1																					X		

Table 15: Mapping of Security Objectives to Security Requirements for the IT Environment

Objectives for the IT Environment SFRs	OE.Adm_Roles	OE.Audit_Gen	OE.Audit_Review	OE.Audit_Storage	OE.Authentication	OE.Crypto_Operation	OE.SE_Crypto_Ops	OE. MsgMod_ID	OE.NonRepudiate_Sent	OE.SE_Key_Gen	OE.Audit_Clear	OE.Timestamp
FAU_STG.1				X								
FCS_CKM.1						X				X		
FCS_COP.1						X	X	X	X			
FMT_MSA.2						X						
FPT_STM.1												X
FAU_MMS_GEN.1		X										
FAU_MMS_GEN.2		X										
FAU_IME_SAR.3			X									
FAU_IME_STG.3				X							X	
FCS_MMS_CKM.2						X						
FCS_MMS_CKM.4						X						
FIA_MMS_AUT.1					X							
FMT_MMS_SMR.1	X											

8.2.2 Requirements Form a Consistent Whole

1545 This section provides justification demonstrating how the security objectives of the TOE and TOE Environment are satisfied by the security requirements of the TOE and TOE Environment. The following tables and corresponding discussions provide the security objective to security requirement mappings and rationale to justify the mapping.

Table 16: IT Security Requirements Justification

Security Objectives	IT Security Requirements
Security Objectives for the TOE	
O.AC_Admin_Limit: Limitation of administrative access control *The TOE shall design administrative functions in such a way that the MMS 1st level administrator, MMS 2nd level administrator, or IME administrators do not automatically have access to IME user objects (i.e., user accounts), except for necessary exceptions.*	**FDP_ACC.1** satisfies this objective by enforcing an access control policy on individual mail files, server resources, and all operations performed by users that are covered by the access control policy. **FDP_ACF.1** satisfies this objective by enforcing the access control policy to grant access to MMS 1st level administrator, 2nd level administrator, and IME administrator to messaging and server resources, and to grant access of IME Group Member and IME Individual Account Users to their individual messaging resources. Additionally, IME group managers are provided access to add, remove, and change passwords of IME Group Members within their group.
O.Admin_Guidance: Administrator guidance documentation *The TOE shall deter administrator errors by providing adequate administrator guidance*	**ADO_DEL.1** satisfies this objective by providing adequate procedures to ensure that the administrator of the Tumbleweed products securely receives the genuine MMS and IME version 5.5 products. **ADO_IGS.1** satisfies this objective by providing adequate procedures to ensure that the administrator of the Tumbleweed products properly installs the MMS and IME products in a manner that provides a reliable and secure environment. **AGD_ADM.1** satisfies this objective by providing adequate documentation to assist the administrator of the Tumbleweed products to appropriately install both MMS and IME products as they are intended.
O.Archive_Messages: Archiving of Messages *The TOE shall archive all messages that violate any of the MMS defined policies, so that they may be viewed at the local administrator's convenience.*	**FAU_MMS_ARC.1** satisfies this objective by archiving messages that trigger policy violations.

Security Objectives	IT Security Requirements
O.Audit_Gen: Generate Audit Data *The IME server shall generate audit data. The date and time of the event, type of event, source of event, user identity (if applicable), and a description of the event will be recorded.*	**FAU_IME_GEN.1** satisfies this objective by providing an audit trail of all IME administrative and IME user actions.
O.Audit_Clear: Clearing old audit records *The MMS server shall remove audit records if they are older than 30 days or if the audit trail exceeds 10048KB.*	**FAU_MMS_STG.3** satisfies this objective by deleting audit records if they are older than 30 days or if the audit trail exceeds 10048KB.
O.Audit_Review *The TOE shall provide the capability for authorized administrators to review the audit trail in a suitable format.*	**FAU_SAR.1** satisfies this objective by providing all audited information to be available to MMS and IME administrators. **FAU_IME_SAR.2** satisfies this objective by restricting read access to the audited information to IME users. **FAU_MMS_SAR.3** satisfies this objective by providing the ability to sort audit data within the MMS server.
O.Authentication: Restrict actions before authentication *The TOE shall require that an IME user, IME administrator, MMS 1st level administrator, or MMS 2nd level administrator present a valid user identity / password before being allowed any other access to the TOE.*	**FIA_IME_UID.1** satisfies this objective by requiring that IME users or administrators provide a valid user identity before being given access to the TOE. **FIA_IME_UAU.1** satisfies this objective by requiring that IME users or administrators are authenticated before accessing the TOE. **FIA_MMS_TOA.1** satisfies this objective by requiring that MMS administrators are authenticated before accessing the TOE. FIA_MMS_AUT.1 supports FIA_MMS_TOA.1 by ensuring that the environment has the capability to verify the user identity / password pairs passed from the MMS component.
O.Auth_Failure: Authentication Failure *The IME Server shall provide the ability to temporarily disable IME users' and administrators' accounts based on a defined number of authentication failures to the specified account.*	**FIA_IME_AFL.1** satisfies this objective by temporarily disabling an IME user's account after 10 unsuccessful authentication attempts have occurred.

Security Objectives	IT Security Requirements
O.Data_Exchange_Conf: Enforce data exchange confidentiality *The TOE shall provide the ability to protect IME data confidentiality during the transmission between TOE components.*	**FPT_ITC.1** satisfies this objective by ensuring the confidentiality of the TSF data during transmission. **FDP_IME_UCT.1** satisfies this objective by ensuring that messages transmitted and received are protected from unauthorized disclosure by enforcing the access control policy to ensure that only the intended recipient is granted access to view a message. Additionally when an IME user views or sends a message, the communication path from the IME user to the IME server is encrypted and thereby encrypting the message during transit.
O.MsgMod_ID: Identify message modification in messages sent or received remotely or locally *The TOE initiates a check which recognizes changes to signed messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages. This check is performed by the RSA Crypto-C module in the environment and the TOE is notified in the case of modification*	**FCO_MMS_NRV.1** satisfies this objective by the MMS component recording an event upon detection of an invalid digital signature applied to a message. The verification of the digital signature is provided with support of the IT Environment of the TOE (i.e. RSA Crypto-C) so that appropriate action may be taken in the event a message may be modified.
O.NonRepudiate_Recd: Non-repudiation for received information *The TOE shall provide evidence to prevent IME users from avoiding accountability of received messages.*	**FCO_IME_NRR.1** satisfies this objective by providing the status of the delivery of a message sent through IME. When a user checks their outbox, the status of each sent message is displayed as to if the message has been successfully sent and viewed. This is the default behavior for every user and is not configurable.
O.NonRepudiate_Sent: Non-repudiation for sent information *The TOE initiates a verification of the digital signatures provided in messages sent to MMS for the validity of the signatures. This is performed by the RSA Crypto-C module in the environment and the TOE is notified if the signature is invalid. Based on the validity of the digital signature, the sender cannot repudiate the information sent.*	**FCO_MMS_NRV.1** satisfies this objective by recording an event upon detection of an invalid digital signature applied to a message. The verification of the digital signature is provided with support of the IT Environment of the TOE (i.e. RSA Crypto-C) so that the sender of a digitally signed message cannot repudiate the information sent.
O.Pass_Auth: Password-based authentication *The IME server shall provide a mechanism to verify the strength of IME user-generated secrets for the password-based authentication of IME Users.*	**FIA_IME_SOS.1** satisfies this objective by providing a password-based authentication mechanism for verifying that passwords created by IME Users are at least 8 characters in length and include at least one numeric character and one alphabetic character.

Security Objectives	IT Security Requirements
O.Pol_Eng: Policy Engine *The TOE shall enforce all messages to be reviewed by all of the MMS configured policies and apply appropriate actions to any messages in violation in accordance with the specified configured policy.*	**FDP_MMS_POL.1** satisfies this objective by providing a mechanism for enforcing the actions identified within the MMS configured policies for each message that violates any of the specified MMS configured policies.
O.Protect_Accounts *During the logon process the TOE will not give any feedback which will aid an attacker to gain unauthorized access to a user or administrator account.*	**FIA_UAU.7** satisfies this objective by not giving feedback which might compromise the confidentiality of passwords.
O.SE_Auth: Secure Envelope Authentication *The TOE shall produce Secure Envelope packages on behalf of IME users.*	**FDP_ACF.1** satisfies this objective by providing access for IME users to create Secure Envelope packages.
O.Security_Attr_Mgt: Manage security attributes *The TOE shall provide restricted management mechanisms for the initialization of and configuration of values for, and allowable operations on, security attributes.*	**FMT_MSA.1** satisfies this objective restricting the roles allowed to change user passwords or change default package security. **FMT_SMF.1** supports FMT_MSA.1 by providing the capabilities to enforce these restrictions. **FMT_IME_MSA.3** satisfies this objective by enforcing the access control policy to provide restrictive access to set a value for the default package property security to the IME Administrator. Additionally, the IME Administrator is also allowed to specify alternative values for each user type to override the value set for the default package property security.
O.Security_Func_Mgt: Manage behavior of security functions *The TOE shall provide restricted management mechanisms for security mechanisms.*	**FMT_MOF.1** satisfies this objective by providing a management mechanism for managing security functionalities for IME. Additionally, it is also ensured that IME users cannot determine the behavior of the security settings for the MMS and IME servers. **FMT_MTD.1** satisfies this objective by supporting the management of security functions through restricting the ability to change MMS and IME configurations to the MMS 1st level Administrator, MMS 2nd level Administrator, and IME Administrator. **FMT_SMF.1** supports FMT_MOF.1 and FMT_MTD.1 by providing the capabilities to enforce these restrictions.
O.Security_Roles: Security roles *The TOE shall maintain security-relevant roles for the IME Server and the association of individuals with those roles.*	**FMT_IME_SMR.1** satisfies this objective by providing a separation of roles within the IME server.

Security Objectives	IT Security Requirements
O.Session_Termination: System terminates session for inactivity *The TOE shall terminate a session after a given interval of inactivity.*	**FTA_SSL_EXP.3** satisfies this objective by enforcing IME and MMS to terminate IME Administrator sessions after 70 minutes and MMS Administrator sessions after a 30 minute period of inactivity. Additionally, FTA_SSL_EXP.3 enforces IME to terminate IME User sessions after a 70 minute period of inactivity.
O.Trusted_Path: Trusted communications path *The TOE shall provide a communication channel capable of protecting confidentiality and of providing reliable entity authentication of the endpoints of the communication path.*	**FPT_ITC.1** satisfies this objective by ensuring the confidentiality of the TSF data (user data and server configurations) during transmission through the trusted channel. **FTP_ITC.1** satisfies this objective by providing a trusted channel between the MMS and IME components and between the IME and web server components.
O.User_Attributes: Maintain user attributes *The TOE shall maintain a set of security attributes (which includes user identity, password and group membership.) associated with individual users in addition to user identity (e.g. email address).*	**FDP_ACC.1** satisfies this objective by enforcing the access control policy to provide a restriction to the modification of security attributes. **FDP_ACF.1** satisfies this objective by enforcing the access control policy to provide a restriction to the modification of security attributes. **FMT_MSA.1** satisfies this objective by restricting the roles allowed to change user passwords or change default package security. **FMT_SMF.1** supports FMT_MSA.1 by providing the capabilities to enforce these restrictions. **FMT_IME_MSA.3** satisfies this objective by providing the IME Administrator the capability to maintain the value set for the default package property security. Additionally, the IME Administrator is also allowed to specify alternative values to override the value set for the default package property security. **FMT_IME_REV.1** satisfies this objective by providing the IME Administrator and IME Group Manager the capability to revoke a user's password.
O.Virus_Updates: Virus Definition Updates *The TOE shall download and apply virus definition updates frequently.*	**FMT_MMS_DNL.1** satisfies this objective by automatically downloading virus definition files and storing them within the MMS SQL database on a daily basis.

Security Objectives	IT Security Requirements
Security Objectives for the IT Environment	
OE.Adm_Roles: Administrative roles *Restrict the capabilities for MMS 1st level administrators to add additional administrative accounts, and modify the audit log by providing a MMS 2nd level administrator strictly for those functions.* .	**FMT_MMS_SMR.1** satisfies this objective for the IT environment by providing a separation of roles. By providing separate roles within the MMS server, MMS can specify to only allow an MMS 2nd level administrator to have the privilege to clear audit events from within the log. Therefore, restricting any MMS 1st level administrators from modifying the audit trail. This functionality is provided by the MMS SQL Database Server.
OE.Audit_Gen: Audit Generation capabilities *Provide information about past MMS Administrators' behavior to an authorized MMS 1st level administrator, MMS 2nd level administrator through system mechanisms to discover system misuse and provide a potential deterrent by warning the administrators. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.*	**FAU_MMS_GEN.1** satisfies this objective for the IT environment by providing an audit trail of MMS Administrator actions. This functionality is provided by the MMS SQL Database Server. **FAU_MMS_GEN.2** satisfies this objective for the IT environment by associating an MMS Administrator's user identity with the auditable actions that are recorded for that individual. This functionality is provided by the MMS SQL Database Server.
OE.Audit_Clear: Clearing old audit records *The environment of the IME Server shall remove audit records if they are older than 30 days or if the audit trail exceeds 10048KB.*	**FAU_IME_STG.3** satisfies this objective for the IT environment by protecting the audit trail from becoming full. This functionality is provided by the Event Viewer application included with the Windows 2000 operating system.
OE.Audit_Storage: Audit storage capabilities *Provide the capability for the TOE environment component to store audit data. In addition to storing audit data, provide the capability to prevent audit trail failure and to protect the integrity of the stored audit data.*	**FAU_STG.1** satisfies this objective for the IT environment by preventing unauthorized deletion and modifications to the audit records. This functionality is provided partially by the MMS SQL Database Server for MMS audit data, and partially by the event log storage capability of the Windows 2000 operating system for the IME audit data. **FAU_IME_STG.3** satisfies this objective for the IT environment by protecting the audit trail from becoming full. This functionality is provided by the Event Viewer application included with the Windows 2000 operating system.

Security Objectives	IT Security Requirements
OE.Audit_Review: Sorting of audit data *The environment of the IME server will provide the capability to sort audit data.*	**FAU_IME_SAR.3** satisfies this objective by providing the ability to sort audit data for the IME server.
OE.Authentication: Verification of authentication data The environment of the MMS server will provide the capability to verify a username / password pair passed to it by the MMS server.	**FIA_MMS_AUT.1** satisfies this objective by providing the ability to verify user name / password pair provided by the MMS server.

Security Objectives	IT Security Requirements
OE.Crypto_Operation: Cryptographic operations *Cryptographic interfaces shall protect communication channels from disclosure and modification through encryption. The cryptographic interfaces shall additionally ensure that messages retain their content integrity during storage and transmission.*	**FCS_CKM.1** satisfies this objective for the IT environment by providing the capability to generate 2048/1024-bit RSA keys, thereby allowing for public key encryption/decryption, by providing the capability to generate 168-bit 3DES keys, thereby allowing for symmetric session key encryption/decryption, and by providing the capability to generate 128-bit RC4 keys, thereby allowing for symmetric file key, data, and Secure Envelope encryption/decryption. These functionalities are provided by the RSA Crypto-C Cryptographic Toolkit. **FCS_MMS_CKM.2** satisfies this objective for the IT environment by providing the capability to use an asymmetric cryptographic primitive to distribute a symmetric key using a protocol which has been widely studied, internationally accepted as secure and has been approved for use in the FIPS 140-1 standards. **FCS_MMS_CKM.4** satisfies this objective for the IT environment by providing the capability to destroy keys entirely when the use for such keys are no longer needed, thereby reducing the risk of an attacker gaining knowledge of that key or of information protected by that key. This functionality is provided by the RSA Crypto-C Cryptographic Toolkit. **FCS_COP.1** satisfies this objective for the IT environment by defining the set of allowable cryptographic operations that may be performed within MMS to provide message and communication channel encryption. and by defining the set of allowable cryptographic operations that may be performed within IME to provide message and communication channel encryption. These functionalities are provided by the RSA Crypto-C Cryptographic Toolkit. **FMT_MSA.2** satisfies this objective for the IT environment by ensuring that the cryptographic protection from disclosure and modification is not compromised by the use of short key sizes for cryptographic algorithms. The IT environment ensures that all hash function produce message digests on at least 160 bits, that all symmetric keys are at least 128 bits and that all asymmetric keys are at least 1024 bits.
OE.SE_Crypto_Ops: Secure Envelope Cryptographic Operations *Provide the encryption, decryption, and hashing of packages sent via Secure Envelope.*	**FCS_COP.1** satisfies this objective for the IT environment by providing 128-bit RC4 encryption and decryption of IME packages. The hashing of IME packages is additionally provided using 160-bit SHA1 hashing algorithm. These functionalities are provided by the RSA Crypto-C Cryptographic Toolkit.

Security Objectives	IT Security Requirements
OE.MsgMod_ID: Identify message modification in messages sent or received remotely or locally *The RSA Crypto-C module will perform an integrity check on a signed message when requested by the TSF and report any modification detected.*	**FCS_COP.1** satisfies this objective for the IT environment by providing the capability to verify the validity of RSA based digital signatures.
OE.NonRepudiate_Sent: Validation of digital signatures *The RSA Crypto-C module will check the validity of a digital signature when requested by the TSF and report any invalid signatures.*	**FCS_COP.1** satisfies this objective for the IT environment by providing the capability to verify the validity of RSA based digital signatures.
OE.SE_Key_Gen: Secure Envelope Key Generation *Provide the generation of keys for packages sent via Secure Envelope.*	**FCS_CKM.1** satisfies this objective for the IT environment by providing a means for generating 128-bit RC4 cryptographic keys to encrypt packages sent via Secure Envelope. This functionality is provided by the RSA Crypto-C Cryptographic Toolkit.
OE.Timestamp: Time stamping *The underlying operating system of the MMS and IME is trusted to be a reliable source for time.*	**FPT_STM.1** satisfies this objective for the IT environment by providing reliable timestamps. This functionality is provided by the underlying hardware clock via the Windows 2000 operating system.

1550 8.2.3 Explicitly Stated Requirements Justification

The following table provides justifications for the explicitly stated requirements defined within this ST as to why they were needed to be explicitly stated.

Table 17: Explicitly Stated Requirements Justification

Explicitly Stated Requirements	Justification
Explicitly Stated Functional Requirements for the TOE	
FAU_IME_GEN.1	*FAU_IME_GEN.1 was explicitly stated since the TOE does not provide auditing for the start-up and shutdown of audit functions and to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FAU_MMS_ARC.1	*FAU_MMS_ARC.1 was explicitly stated since no functional requirement within the FAU family of CC Part 2 version 2.1 identify the functionality for archiving data as a result of a form of audit violation, or in this case a policy violation.*
FAU_IME_SAR.2	*FAU_IME_SAR.2 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FAU_MMS_SAR.3	*FAU_MMS_SAR.3 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FAU_MMS_STG.3	*FAU_MMS_STG.3 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FCO_IME_NRR.1	*FCO_IME_NRR.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FCO_MMS_NRV.1	*FCO_MMS_NRV.1 was explicitly stated because the FCO_NRO.1 requirement, that this requirement is modeled after, requires the generation of evidence of the originator. However, this component of the TOE only provides the capability to verify evidence provided by an originator that has been generated before the information has reached the TOE.*
FDP_MMS_POL.1	*FDP_MMS_POL.1 was explicitly stated since no functional requirement within the FDP family of CC Part 2 version 2.1 identify the functionality for specifying a set of policies in which user data shall be subject to being checked against.*
FDP_IME_UCT.1	*FDP_IME_UCT.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FIA_IME_AFL.1	*FIA_IME_AFL.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FIA_IME_SOS.1	*FIA_IME_SOS.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*

Explicitly Stated Requirements	
FIA_IME_UAU.1	*FMT_IME_MSA.3 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FIA_IME_UID.1	*FIA_IME_UID.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FIA_MMS_TOA.1	*FIA_MMS_TOA.1 was explicitly stated since no functional requirement within the FIA family accurately describes the interaction between the MMS server and its environment during the identification and authentication process. Specifically, the TOE demands the user identity and the password and denies access until these have been confirmed but it is the environment that actually checks the validity of these credentials. The requirement FIA_MMS_TOA.1 covers the fact that the MMS server enforces the rule of not allowing access to TOE functionality (apart from help) until the user has been authenticated (by the environment).*
FMT_MMS_DNL.1	*FDP_MMS_DNL.1 was explicitly stated since no functional requirement within the FMT family of CC Part 2 version 2.1 identify the functionality for the management of a mechanism that downloads virus definition updates.*
FMT_IME_MSA.3	*FMT_IME_MSA.3 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FMT_IME_REV.1	*FMT_IME_REV.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FMT_IME_SMR.1	*FMT_IME_SMR.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FTA_SSL_EXP.3	*FTA_SSL_EXP.3 was explicitly stated to identify functionality differently for two separate roles of the TOE.*
Explicitly Stated Functional Requirements for the TOE Environment	

Explicitly Stated Requirements	
FAU_MMS_GEN.1	*FAU_MMS_GEN.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole and because the range of auditable events generated was slightly different from that stated in the 'standard' requirement.*
FAU_MMS_GEN.2	*FAU_MMS_GEN.2 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FAU_IME_SAR.3	*FAU_IME_SAR.3 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FIA_MMS_AUT.1	*FIA_MMS_AUT.1 was explicitly stated since no functional requirement within the FIA family accurately describes the interaction between the MMS server and its environment during the identification and authentication process. Specifically, the TOE demands the user identity and the password and denies access until these have been confirmed but it is the environment that actually checks the validity of these credentials. The requirement FIA_MMS_AUT.1 covers the fact that the environment provides the authentication but the MMS Server itself restricts access until this authentication has been successfully performed.*
FCS_MMS_CKM.2	*FCS_MMS_CKM.2 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FCS_MMS_CKM.4	*FCS_MMS_CKM.4 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*
FMT_MMS_SMR.1	*FMT_MMS_SMR.1 was explicitly stated to identify a functionality that pertains to only a specific component of the TOE and not the TOE as a whole.*

1555

1555 8.2.4 Requirements are Justified

The following table provides a cross reference for each security functional requirement within this ST and their dependencies, showing overall that all requirements are satisfied.

Table 18: Security Functional Requirements Dependencies Mapping

Security Functional Requirements	Dependencies
FAU_IME_GEN.1	FPT_STM.1
FAU_MMS_GEN.1	FPT_STM.1
FAU_MMS_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	FAU_GEN.1
FAU_IME_SAR.2	FAU_SAR.1
FAU_MMS_SAR.3	FAU_SAR.1
FAU_IME_SAR.3	FAU_SAR.1
FAU_STG.1	FAU_GEN.1
FAU_IME_STG.3	FAU_STG.1
FAU_MMS_STG.3	FAU_STG.1
FCO_IME_NRR.1	FIA_UID.1
FCO_MMS_NRV.1	FIA_UID.1
FCS_CKM.1	FCS_CKM.4, FCS_COP.1, FMT_MSA.2
FCS_MMS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_MMS_CKM.4	FCS_CKM.1, FMT_MSA.2
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_MMS.POL.1	*No Dependencies*
FDP_IME_UCT.1	FDP_ACC.1, FTP_ITC.1
FIA_IME_AFL.1	FIA_UAU.1
FIA_IME_SOS.1	*No Dependencies*
FIA_IME_UAU.1	*No Dependencies*
FIA_IME_UID.1	*No Dependencies*

Security Functional Requirements	
FIA_MMS_AUT.1	*No Dependencies*
FIA_MMS_TOA.1	*No Dependencies*
FIA_UAU.7	FIA_UAU.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_IME_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
FMT_IME_REV.1	FMT_SMR.1
FMT_IME_SMR.1	FIA_UID.1
FMT_MMS.DNL.1	*No Dependencies*
FMT_MMS_SMR.1	FIA_UID.1
FMT_SMF.1	*No Dependencies*
FPT_ITC.1	*No Dependencies*
FPT_STM.1	*No Dependencies*
FTA_SSL_EXP.3	*No Dependencies*
FTP_ITC.1	*No Dependencies*

8.2.4.1 Justification of Unsupported Dependencies Regarding ADV_SPM.1

FMT_MSA.2 requires the dependency of ADV_SPM.1 to provide a security policy model reflecting the meaning of “secure” for the secure values within the security attributes for cryptographic operations. However FMT_MSA.2 is a security requirement of the TOE environment. As such it is neither appropriate nor possible to provide assurance requirements. This approach to the satisfaction of dependencies of requirements on the IT environment is consistent with NIAP precedent decision PD-0091: Dependencies of Requirements on the IT Environment which states that ‘a dependency on an SFR allocated to the IT environment, it need not be explicitly satisfied/verified’.

8.2.4.2 Justification of Supported Dependencies Regarding FAU_GEN.1

FAU_GEN.2 and FAU_SAR.1 requires the dependency of FAU_GEN.1 to provide audit data generation. Audit data generation is provided through FAU_IME_GEN.1 and FAU_MMS_GEN.1 for the intent that is required by FAU_GEN.2 and FAU_SAR.1. However, FAU_GEN.1 was explicitly stated since the auditing of the startup and shutdown of audit functions could not be provided and because the MMS and IME components provide audit data generation differently. Therefore the dependency for FAU_GEN.1 is satisfied through FAU_IME_GEN.1 and FAU_MMS_GEN.1.

8.2.4.3 Justification of Supported Dependencies Regarding FIA_UAU.1

FIA_IME_AFL.1, FIA_UAU.7 require the dependency FIA_UAU.1 to provide an authentication requirement. FIA_IME_AFL.1, FIA_UAU.7 both make claims about the mechanism demanding authentication credentials, in this case a password. For the MMS server FIA_MMS_TOA.1 requires that the TOE requests and receives a valid password from each user. This satisfies the dependency for the MMS Server. For the IME Server, FIA_IME_UAU.1 satisfies the dependency since it provides the same functionality as FIA_UAU.1 but is restricted to the IME server.

8.2.4.4 Justification of Supported Dependencies Regarding FIA_UID.1

FAU_MMS_GEN.2, FCO_IME_NRR.1, FCO_MMS_NRV.1, FMT_IME_SMR.1 and FMT_MMS_SMR.1 requires the dependency of FIA_UID.1 to provide an identity of users. Within this product the users identify themselves to the TOE but, for the MMS server, this identity is verified by the local SQL server in the IT environment. Therefore on the MMS server this dependency is satisfied by FIA_MMS_TOA.1, supported by FIA_MMS_AUT.1 For the IME server the dependency is directly satisfied by FIA_IME_UID.1 which provides the same functionality as FIA_UID.1 but is restricted to the IME server.

8.2.4.5 Justification of Supported Dependencies Regarding FCS_CKM.4

FCS_CKM.1, FCS_MMS_CKM.2, and FCS_COP.1 require the dependency of FCS_CKM.4 to provide cryptographic key destruction. These Security Functional Requirements are all environmental. Following NIAP Precedent Decision 0091 an explicit justification for not meeting these dependencies is beyond the scope of this document. Nevertheless, one can be assured that the key lifecycle is well managed since it all taken place within a dedicated, integrated module in the environment (RSA Crypto-C), which is both CC and FIPS 140-2 certified.

8.2.4.6 Justification of Supported Dependencies Regarding FMT_MSA.3

FDP_ACF.1 requires the dependency of FMT_MSA.3 to provide static attribute initialization. Static attribute initialization is provided through FMT_IME_MSA.3 for the intent that is required by FDP_ACF.1. However, FMT_MSA.3 was explicitly stated since static attribute initialization functionality is only provided by the IME component of the TOE. Therefore the dependency for FMT_MSA.3 is satisfied through FMT_IME_MSA.3.

8.2.4.7 Justification of Supported Dependencies Regarding FMT_SMR.1

FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_IME_MSA.3, FMT_MTD.1, and FMT_IME_REV.1 require the dependency of FMT_SMR.1 to provide role management capabilities. The role management capabilities are provided through FMT_IME_SMR.1 and FMT_MMS_SMR.1 for the intent that is required by FDP_ACF.1. However, FMT_SMR.1 was explicitly stated since the MMS and IME components provide the role management capabilities differently. Therefore the dependency for FMT_SMR.1 is satisfied through FMT_IME_SMR.1 and FMT_MMS_SMR.1.

8.2.5 Assurance Level Justification

Tumbleweed has chosen to pursue an EAL 2+ assurance level of the MMS and IME version 5.5 products
because of government customer requirements that are mandated by NSTISS 11 Policy Letter, which
require a Common Criteria certification for a product to be sold to the Department of Defense and other
1615 government agencies.

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Satisfy Functional Requirements

The following table represents a mapping between the security functions identified in Clause 6.1 to their related TOE security functional requirements identified in section 5.1 and to their related explicitly stated TOE security functional requirements within section 5.2. 1620

Table 19: Mapping of Security Functions to Security Functional Requirements

Security Functions (6.1)	Security Functional Requirements (5.1)
Audit Function	FAU_MMS_ARC.1, FAU_IME_GEN.1, FAU_SAR.1, FAU_IME_SAR.2, FAU_MMS_SAR.3, FAU_MMS_STG.3, FCO_IME_NRR.1
Identification & Authentication Function	FIA_IME_AFL.1, FIA_IME_SOS.1, FIA_UAU.7, FIA_IME_UAU.1, FIA_IME_UID.1, FIA_MMS_TOA.1, FMT_IME_REV.1
Message security Function	FCO_MMS_NRV.1, FDP_MMS_POL.1, FMT_MMS_DNL.1
Role-Based Access Function	FDP_ACC.1, FDP_ACF.1, FDP_IME_UCT.1, FMT_MOF.1, FMT_MSA.1, FMT_IME_MSA.3, FMT_MTD.1, FMT_SMF.1
Role Management Function	FMT_IME_SMR.1
Trusted Path Function	FTA_SSL_EXP.3, FPT_ITC.1, FTP_ITC.1

Table 20: Reverse Mapping of Security Functional Requirements to Security Functions

Functional Requirement:	TOE Security Functions:	Rationale:
Functional Requirements for the TOE		
FAU_SAR.1	Audit Function	The Audit Function satisfies this requirement by providing the capability for MMS Administrators to view audit data from the MMS component, and for the IME Administrator to view audit data from the IME component.
FDP_ACC.1	Role-Based Access Function	The Role-Based Access Function satisfies this requirement by enforcing the access control policy within Table 2 (Access Control Policy) on the individual mail files, server resources, and all operations performed by users and administrators of both MMS and IME.
FDP_ACF.1	Role-Based Access Function	The Role-Based Access Function satisfies this requirement by enforcing the access control policy within Table 2 (Access Control Policy) for both MMS and IME based upon an authenticated user's associated role.
FIA_UAU.7	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement by restricting feedback to the user while the authentication is in progress. Feedback that is allowed includes indication of how many characters of the password have been typed without showing the characters themselves by substituting each character with a dot and indication of the account name in clear text being authenticated, indication of authentication failure. The IME server also provides an indication of how many unsuccessful authentication attempts are allowed before the account is locked, indication of an invalid account name, and indication of the account being locked out.
FMT_MOF.1	Role Management Function	The Role-Based Access Function satisfies this requirement by restricting access to modify the behavior of or change the configurations of the security functions for IME to the IME Administrator, and by restricting access to modify administrator accounts and the audit log of the MMS Server to the 2nd level MMS Administrator.

Functional Requirement:	**TOE Security Functions:**	**Rationale:**
FMT_MSA.1	Role-Based Access Function	The Role-Based Access Function satisfies this requirement for the MMS component by restricting access to add or remove administrators to the MMS 2nd level administrator. The Role-Based Access Function satisfies this requirement for the IME component by restricting access to modify passwords as follows. IME Administrators can change any password. IME Group Managers can change the password of any member of their group All categories of users can change their own password. It also restricts the ability to set the default package property security to the IME Administrator. This evaluated configuration requires the IME administrator to set the default delivery method to be account-based security.
FMT_MTD.1	Role-Based Access Function	The Role-Based Access Function satisfies this requirement by restricting access to modify the configurations of MMS and IME to the MMS and IME Administrators.
FMT_SMF.1	Role Management Function	The Role-Based Access Function satisfies this requirement by providing mechanisms to enforce the restrictions stated in FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1.
FPT_ITC.1	Trusted Path Function	The Trusted Path Function satisfies this requirement by restricting the disclosure of information in transit through the use of the CORBA/IIOP Over SSL protocol.
FTP_ITC.1	Trusted Path Function	The Trusted Path Function satisfies this requirement by providing a trusted communication channel for communication between IME and MMS, and between IME and the web servers.

Functional Requirement:	TOE Security Functions:	Rationale:
Explicitly Stated Requirements for the TOE		
FAU_IME_GEN.1	Audit Function	The Audit Function satisfies this requirement by providing audit data generation for the IME component.
FAU_MMS_ARC.1	Audit Function	The Audit Function satisfies this requirement by archiving messages that trigger policy violations for a later review by an authorized Administrator.
FAU_IME_SAR.2	Audit Function	The Audit Function satisfies this requirement by restricting all users other than IME administrators from reading the audit logs within the IME component.
FAU_MMS_SAR.3	Audit Function	The Audit Function satisfies this requirement by providing the capability within the MMS component to sort audit data.
FAU_MMS_STG.3	Audit Function	The Audit Function satisfies this requirement by taking action to delete stored audit data for MMS that exceed 30 days old.
FCO_IME_NRR.1	Audit Function	The Audit Function satisfies this requirement by providing evidence that a message sent has been successfully sent to and retrieved by the intended recipient.
FCO_MMS_NRV.1	Message Security Function	The Message Security Function satisfies this requirement with support of the IT Environment by verifying the digital signatures of messages sent to MMS and providing an automatic lookup of an individual's public key certificate to verify against the signature.
FDP_IME_UCT.1	Role-Based Access Function	The Role-Based Access Function satisfies this requirement by enforcing the access control policy within Table 2 (Access Control Policy) so that messages sent or received are protected from unauthorized disclosure.
FIA_IME_AFL.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement by providing the capability to temporarily disable an IME user's or IME Administrator's account after 10 unsuccessful authentication attempts.
FIA_IME_SOS.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement by providing a password-based authentication mechanism within IME that verifies passwords for IME Users to be a minimum of eight characters, include at least one numeric character, and include at least one alphabetic character.

Functional Requirement:	**TOE Security Functions:**	**Rationale:**
FIA_IME_UAU.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement for the IME component by allowing the initiation of the login process to be provided prior to being authenticated using the password-based authentication mechanism, and by not allowing any other actions to be performed prior to successful authentication, with the exception of access to the help database.
FIA_IME_UID.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement for the IME component by requiring each user to be successfully identified before allowing the user to perform any other action, other than access help.
FIA_MMS_TOA.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement for the MMS component by requiring each user to provide a user name and password to the TOE which is validated by the environment before the TOE allows the user to perform any other action.
FMT_IME_MSA.3	Role-Based Access Function	The Role-Based Access Function satisfies this requirement by restricting access to override the default settings for the package delivery method to the IME Administrator.
FMT_IME_REV.1	Identification & Authentication Function	The Identification & Authentication Function satisfies this requirement by restricting the ability to revoke security attributes associated with users. IME Administrators can do this for any user and IME Group Managers can do this for users who are a member of that IME Group Manager's group.
FMT_IME_SMR.1	Role Management Function	The Role-Based Access Function satisfies this requirement by providing roles and associating each user to a role.
FTA_SSL_EXP.3	Trusted Path Function	The Trusted Path Function satisfies this requirement by terminating sessions remaining idle over a specified period of time.
FDP_MMS_POL.1	Message Security Function	The Message Security Function satisfies this requirement by providing a policy engine that checks each incoming and outgoing message against the policies defined within MMS and applying the specified actions.
FMT_MMS_DNL.1	Message Security Function	The Message Security Function satisfies this requirement by automatically checking for new virus definition patterns on a daily basis.

1625 8.3.2 Assurance Measures Meet Assurance Requirements

Table 21: Assurance Measures that Fulfill Assurance Requirements (EAL 2+)

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ACM_CAP.3	Configuration Management Plan for Tumbleweed MMS ™ and IME ™ Version 5.5.3	The document provides a reference for the TOE which is Tumbleweed MMS Server 5.5 and Tumbleweed IME Server 5.5. It also describes the CM system used by Tumbleweed and provides all activities performed in the TOE development environment, the roles and responsibilities of individuals that support the maintenance of the TOE, procedures used within the TOE development environment, evidence of the application of the procedures, the approach to the version control of the TOE, and a configuration item list.
ACM_SCP.1	Configuration Management Plan for Tumbleweed MMS ™ and IME ™ Version 5.5.3	The document provides a configuration item list of all the components of the TOE.
ADO_DEL.1	Delivery Procedures for Tumbleweed MMS ™ and IME ™ Version 5.5.3	The document describes the procedures that Tumbleweed follows to deliver MMS and IME version 5.5 to a user. These procedures are intended to maintain the integrity of the TOE during deliver to the client site. Tumbleweed asserts that it has followed these procedures to deliver both MMS and IME and thereby providing evidence to the Common Criteria Testing Laboratory that these procedures are followed accordingly.

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ADO_IGS.1	Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within sections 2.5.4, 3.2.3, and 3.3.2 of the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within sections 2.2, 2.2.3, 2.3.3, 2.4.3, 3.1.5, and 3.3.1 of the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5, made within sections 3.2.3 and 3.3.3 of the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3	These documents outline procedures for the secure installation, generation, and start-up of the TOE. These documents are sufficient to ensure that the TOE is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification. This includes the initialization, generation, and start-up procedures.

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ADV_FSP.1	Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within section 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within section 3.1.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5, made within section 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5,3 made within sections 3.1.3 and 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help, made within sections 3.2.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5.	The functional specification identifies and describes the security functions of the TOE and the external interfaces. The details of input parameters, effects, errors, and exceptions of the external interfaces defined within the functional specification are provided within the listed documents

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ADV_HLD.2	High-Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5 References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within section 3.4.3 of the High Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5. Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed MMS Administrator's Guide, Release 5.5, made within section 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5, made within section 3.1.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5 References to the Tumbleweed Secure Redirect Administrator's Guide MMS Release 5.5 to IME 5.5, made within section 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5 References to the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 made within sections 3.1.3 and 3.4.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. References to the Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help, made within sections 3.2.3 of the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5.	The high-level design identifies and describes the subsystems of the TOE and their interfaces. Sufficient detail is given to allow a good understanding of the security relevant subsystems and interfaces. Subsystems and interfaces which are claimed to not be security relevant are described in sufficient detail to allow an evaluation of this claim. The high-level design references the FSP to satisfy some of the requirements.

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ADV_RCR.1	Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. High-Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5	Tumbleweed has provided a correspondence analysis between all adjacent pairs of TSF representations that are provided. The correspondence analysis between TSS and FSP is provided within the Functional Specification for Tumbleweed MMS ™ and IME ™ Version 5.5. The correspondence analysis between FSP and HLD is provided within the High-Level Design for Tumbleweed MMS ™ and IME ™ Version 5.5.
AGD_ADM.1	Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 References to the following documents made in the Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3 • Tumbleweed MMS Administrator’s Guide, Release 5.5. • Tumbleweed IME Server for Windows Administrator’s Guide, Release 5.5. • Tumbleweed Secure Redirect Administrator’s Guide MMS Release 5.5 to IME 5.5.	Tumbleweed has provided documentation addressed to administrative personnel. This documentation is given in a level of detail to allow a competent operator to administer the TOE securely.
AGD_USR.1	Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help (collection of HTML files)	Tumbleweed has provided user guidance which describes the security functions and interfaces in a way which allows a user to interact with the TOE securely.
ATE_COV.1	Testing Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5	Tumbleweed has provided an analysis of the testing coverage. The testing coverage analysis provides a mapping to provide evidence of the security functions of the TOE which have been tested.
ATE_FUN.1	Testing Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5	Tumbleweed has tested the TSF of MMS and IME 5.5 which verified all testable behavior arising from the use of TOE security functions. The results of these tests are included.

Assurance Requirements:	Assurance Measures: (TW-MMS&IME Documentation)	Rationale:
ATE_IND.2	Tumbleweed MMS ™ and IME ™ Version 5.5 products	Tumbleweed has provided Tumbleweed MMS ™ and IME ™ Version 5.5 products to the Common Criteria Testing Laboratory for testing.
AVA_SOF.1	Vulnerability Analysis Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5	Tumbleweed has provided a strength of TOE security function analysis for each mechanism identified within the ST having an SOF claim. This document provides evidence and analysis to support the claim that the password based authentication mechanism has a strength of function of, at least, basic.
AVA_VLA.1	Vulnerability Analysis Documentation for Tumbleweed MMS ™ and IME ™ Version 5.5	Tumbleweed has performed and documented an analysis of obvious vulnerabilities in which a user may violate the TSP. This document examines all public vulnerabilities which might apply to the product and shows, for each one, why it is not possible to exploit this vulnerability in the evaluated configuration.

8.3.3 Validation of Strength-of-Function

The strength of the IME Security Function claim SOF-Basic is provided. The SOF claim is valid for the timing of authentication (FIA_IME_UAU.1), verification of secrets (FIA_IME_SOS.1), and authentication failure handling (FIA_IME_AFL.1) TOE security functional requirements. The SOF claim relates to the TOE Identification & Authentication function and satisfies the TOE Security Objectives O.Authentication, O.Auth_Failure and O.Pass_Auth by providing a mechanism within IME for verifying passwords generated by IME user accounts and a mechanism to disable all four types of IME accounts after a defined number of unsuccessful authentication attempts have occurred. The SOF claim ensures that the mechanism is resistant to a low attack potential. A low attack potential is chosen for the TOE since IME user accounts' password contents are inspected and enforced during password creation, and adminstrator account passwords required by administrative guidance, to be at least eight characters with at least one alphabetic character and one numeric character. Additionally, all four types of IME accounts only allow for ten unsuccessful authentication attempts to occur before disabling the account. Therefore, the attack potential of an attacker to gain access to an account is considered to be a low risk. No strength of function claim is made for the MMS component because the authentication mechanism is primarily enforced by the environment.

8.4 PP Claims Rationale

There are no protection profile claims for this security target.

9 References

1650 9.1 Acronyms

This section provides a list of acronyms used within the ST

CC:	Common Criteria version 2.1 (IS 15408)
CORBA:	Common Object Request Broker Architecture
EAL:	Evaluation Assurance Level
IA:	Information Assurance Defense in Depth strategy
IIOP:	Internet Inter-ORB Protocol
SFP:	Security Function Policy
S/MIME:	Secure Multi-purpose Internet Mail Extension
SMTP:	Simple Mail Transfer Protocol
SOF:	Strength Of Function
SPN:	Secure Public Network
ST:	Security Target
TOE:	Target Of Evaluation
TSF:	TOE Security Function(s)
TSP:	TOE security Policy
TSM&M:	Tumbleweed MMS and IME

9.2 Vocabulary

This section provides definition to any complex terms used.

CORBA / IIOP: The Common Object Request Broker Architecture (CORBA) is structured to allow integration of a wide variety of object systems. The CORBA model is derived from the abstract Core Object Model defined by the Object Management Group in the Object Management Architecture Guide.

The Internet Inter-ORB Protocol (IIOP) element specifies how General Inter-ORB Protocol (GIOP) messages are exchanged using TCP/IP connections. The IIOP specifies a standardized interoperability protocol for the Internet, providing "out of the box" interoperation with other compatible Object Request Brokers (ORBs) based on the most popular product- and vendor-neutral transport layer. It can also be used as the protocol between half-bridges.

To find additional information and specifications on CORBA / IIOP, please refer to http://www.omg.org/.

Packages: Encrypted messages and attachments.

9.3 Interpretations

The following table identifies the national and international interpretations applied when constructing this ST. In addition, it identifies which requirements were affected by which interpretations.

Table 22: Interpretations

Interpretation:	**Interpretation Description:**	**Requirements Affected by Interpretation:**
International Interpretations		
INTERP-003	Unique identification of configuration items in the configuration list	ACM_CAP
INTERP-004	ACM_SCP.*.1C requirements unclear	ACM_SCP.1.1D
INTERP-065	No component to call out security function management	FMT_SMF.1
National Interpretations		
NIAP-0375	Elements Requiring Authentication Mechanism	FIA_UAU.1.2
NIAP-0407	Empty Selections Or Assignments	FDP_ACF.1.3, FDP_ACF.1.4
NIAP-0410	Auditing Of Subject Identity For Unsuccessful Logins	FAU_IME_GEN.1.2, FAU_MMS_GEN.1.2, FAU_MMS_GEN.2.1

The components of requirements FAU_IME_GEN.1.1 and FAU_MMS_GEN.1.1 are derived from the standard component FAU_GEN.1.1 but have been extended in such a way that interpretation NIAP-0407 does not apply to them.