90East

Formerly SecureGate

Tumbleweed Messaging Management System Release 4.6 Security Target

February 2002

Prepared for Tumbleweed Communications

Contents

Document Control	Project Manager	Checked by	Approved by
Name	Anne Robins	Peter Lilley	Rod Murn
Title	Senior Consultant	Senior Consultant	General Manager
Version Number	Version Date	Change Details	
2.0	21 February 2001	Reformatting only from version 1.4	
2.1	27 July 2001	Updated to address EORs 17 to 21	
2.2	13 February 2002	Update to address EOR 22	
Document Classification			
COMMERCIAL - IN - CONFIDENCE			

Copyright Notice:

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC.

All operations described above, except for refinement, are used in this Security Target. The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value]. *Italicised text* is used for both official document titles and text meant to be emphasised more than plain text.

Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Administrator - A role which users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Application - Any IT product or system, untrusted or trusted, outside the TOE that interacts with the TOE.

Role - A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity - A representation (eg a string) uniquely identifying an authorised user, that can be either the full or abbreviated name of that user or a pseudonym.

Authentication data - Information used to verify the claimed identity of a user.

Document Organisation

Section 1 provides the introductory material for the Security Target.
Section 2 provides general purpose and TOE description.
Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.
Section 4 defines the security objectives for both the TOE and the TOE environment.
Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.
Section 6 provides a description of the IT security functions of the TOE and identifies the assurance measures that meet the assurance requirements for the TOE.
Section 7 contains any PP claim applicable to the TOE.
Section 8 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. This section then provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the security functional requirements.
Appendix A provides an acronym list to define frequently used acronyms.

1 Introduction

This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets an **Evaluation Assurance Level (EAL) 2** level of assurance.

ST Title:	Tumbleweed Communications MMS™ Release 4.6 Security Target
TOE Identification:	Tumbleweed Communications Messaging Management System Release 4.6
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1 Final
ST Evaluation:	Australasian Information Security Evaluation Program, Defence Signals Directorate, Australian Department of Defence
Author(s)	Anne Robins
Keywords:	Security target, secure messaging, encryption, S/MIME

1.2 Security Target Overview

The Tumbleweed Messaging Management System (MMS)™ is a set of e-mail management products and services that enables organisations to protect valuable corporate information on the Internet. Tumbleweed MMS enables organisations to set and enforce policies for security, archiving, distribution, monitoring and regulatory compliance related to Internet e-mail. Using MMS, organisations can set policies to apply content control, encryption, access control, attachment management, virus scanning and digital signatures to e-mail traffic. These policies are administered centrally and enforced universally across an enterprise.

MMS enables organisations to extend the control and security associated with groupware products to Internet communications. Tumbleweed MMS works with open standards, and enables organisations to extend their communications systems and policies to any Internet user with a standard e-mail program and a Web browser.

Tumbleweed MMS enables organisations to set and enforce policies for key issues related to Internet e-mail:

- security
- archiving
- distribution
- monitoring
- regulatory compliance

Using MMS, organisations can apply any of the following in any combination to e-mail messages meeting criteria defined by business managers and network administrators:

- content control
- encryption
- access control
- attachment management
- virus scanning
- digital signatures

1.3 Common Criteria Conformance

The TOE is conformant with Parts 2 and 3 of the CC, version 2.1.

2 TOE Description

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

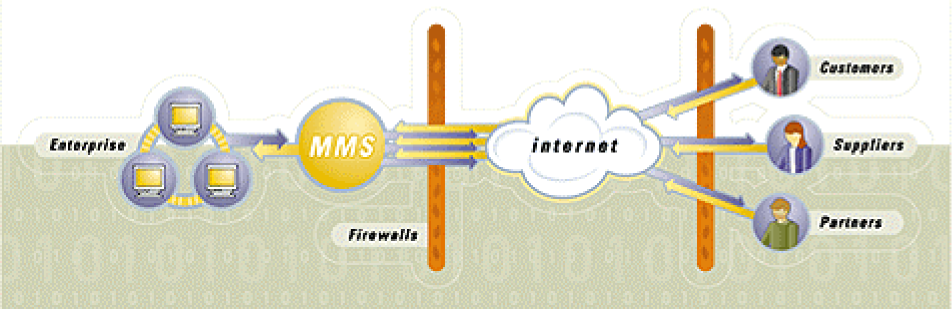
2.1 Overview of the Tumbleweed Messaging Management System

This section presents an overview of the Tumbleweed Messaging Management System Release 4.6 to assist potential users in determining whether it meets their needs. The Tumbleweed MMS, known as the TOE, comprises two main components:

- The **MMS Server** which provides the policy enforcement services for all messages passing through it; and
- The **MMS Administration Workstation** which administrators can use to manage and configure the policies and operation of the MMS Server.

MMS allows administrators and policy-makers to define and enforce security policies to ensure the safe, appropriate and efficient use of corporate e-mail systems. MMS operates on all SMTP-based e-mail, both entering and exiting an organisation. While other products provide encryption or reporting or filtering capabilities, only MMS enables organisations to apply virus scanning, content control, access control, encryption, and digital signature policies across the whole enterprise.

Using a graphical user interface, organisations can set MMS policies that implement a wide range of e-mail controls. These controls are applied to all SMTP-based messages that pass through a corporate firewall, protecting networks and information assets, and allowing organisations to monitor and archive all e-mail communications. The placement of MMS within a network is shown below.



Tumbleweed MMS provides centralised security features on top of existing SMTP-based e-mail systems and behind existing firewalls, fitting easily into existing LAN architectures, and requiring no new desktop software and no end-user training.

To protect intellectual capital, preserve confidentiality, and maintain competitive advantage, organisations need to be able to protect information assets as they travel across the Internet. Organisations must be able to:

- Automatically detect important and sensitive information in e-mail messages;
- Automatically take the proper course of action to securely deliver this information to the proper recipients; and
- Automatically block messages carrying information to inappropriate recipients.

In the case of confidential information, organisations need to be able to secure communications channels. Through its secure messaging capabilities, including server-based S/MIME encryption, MMS enforces security policies to protect information assets as they travel over the Internet, regardless of the desktop software configuration being used by the sender or recipient. Organisations may also choose to use MMS to archive messages, so that they can maintain records of how information has been transferred, and so that they can analyse any patterns of e-mail use or abuse.

Organisations also need to protect their networks from SPAM, viruses and other harmful content that may arrive through e-mail. Content filtering technology can be deployed to automatically examine the contents of incoming e-mail messages, and delete, quarantine, or clean messages carrying viruses or SPAM.

For distributed organisations, or those with tightly coupled partners, suppliers, or clients, a secure e-mail communications network can be established by installing MMS servers at each location. Upon determining that an e-mail message is intended for a recipient at one of these sites, an MMS server can encrypt the message and sign it with the organisation's digital certificate. It then sends the message to its destination, where another MMS server receives it, verifies the authenticity of the digital certificate, and delivers the message in unencrypted form to the mailbox of the recipient. Neither the sender nor the recipient needs to be aware of the role of MMS in the exchange.

The TOE uses S/MIME encryption to encrypt and sign messages. By applying digital certificates at the server, rather than the desktop, MMS enables organisations to take advantage of the benefits of digital certificates for authentication and non-repudiation, without having to acquire and distribute certificates for individual users.

MMS is a policy-based system that can enact a variety of measures based on a particular policy rule. The policies are configured through a number of Policy Managers through which the rules and consequences are defined. These Policy Managers are listed below:

- MMS Content Manager
  - Create policies based on using keywords to scan messages and attachments for specific information, such as confidential or proprietary information, attachment types likely to carry corporate assets, and specific words such as classifications and code names or credit card numbers.

- MMS Security Manager
  - Create policies to enable encryption of potentially sensitive information travelling to and from certain servers using the S/MIME public key of the recipient organisation, thus creating S/MIME VPNs.

- MMS Access Manager
  - Create policies that restrict email from certain senders or to certain recipients to block messages from known problem domains, prevent e-mail going to a competitor's domain, or help preserve bandwidth by blocking large messages.
- MMS Virus Manager
  - Create policies to control the integrated server-based anti-virus software from Network Associates to detect and optionally clean or strip infected attachments in both incoming and outgoing messages. Virus Manager can also enforce periodic or extra-ordinary updates of the anti-virus software.
- MMS Format Manager
  - Create policies to strip or rewrite addresses in message headers to protect the internal network architecture and the privacy of e-mail senders; e.g. removing aliases or addressing information referring to physical location, full name, or organisational position.

One of the possible measures to be taken as the result of policy enforcement may be the archiving of a message. The MMS Message Monitor provides the capability to review archived messages, to group archived messages by violation type, and to enforce a structured review process to ensure that certain messages, or certain types of messages can only be reviewed by certain people, probably in accordance with an organisational privacy policy.

The MMS Message Monitor can also be useful for determining an organisation's level of compliance with standards or regulations. Message Monitor can be used to archive a sample of employee e-mail for periodic review, read and search specific types of messages stored within an archive, and provide a clear demonstration of an organisation's commitment to compliance, particularly with privacy regulations. For example, if an organisation dealt with the private details of citizens (say, an organisation in the health-care industry) then Message Monitor and the MMS Policy Managers could be used to demonstrate that no, or only appropriate, personal details were transmitted by the organisation, and then only when appropriately protected.

MMS provides support for virus detection and sanitisation by offering a policy-based interface for invoking the features of the server-based McAfee anti-virus software supplied with MMS. The MMS policies can be formulated to match existing organisational anti-virus policies. MMS does not itself perform virus scanning and the MMS guidance documentation does not cover the installation and usage of third-party anti-virus software.

MMS is available in three editions[1]:

- Standard Edition – for workgroups;
- Enterprise Edition – for enterprises and organisations with requirements for high-volume archiving and compliance with industry or government regulations; and
- Secure Messaging Redirect – for Enterprise edition customers interested in hosting Tumbleweed IME services on their network.

[1] Only the Standard Edition and Enterprise Edition are part of this Security Target.

2.2 Physical Scope of the TOE

The physical scope of the TOE includes the hardware and software elements identified below.

TOE Components	Hardware/Software Elements
MMS Server	MMS Software Version 4.6 MMS patch *sapassword.exe* Microsoft Windows 2000 OR Microsoft Windows NT 4.0 Server with Service Pack 6.0a With Microsoft Internet Explorer 5.0 And Microsoft Internet Information Server 4.0 Minimum hardware configuration of: - Pentium II 333 MHz - CD-ROM Drive - 8 GB hard drive - 256 MB of memory - Colour monitor - An Ethernet or Token Ring interface card
MMS Administration Workstation	Microsoft Windows 2000 OR Microsoft Windows NT 4.0 Workstation with Service Pack 6.0a The minimum hardware configuration is the minimum necessary to support the chosen operating system PLUS - an Ethernet or Token Ring interface card

Table 1 - TOE Component Identification

2.3 Security Services

The TOE provides the following security features:

TOE Security Services	Description
Message Confidentiality	Encrypt messages
Message Integrity	Digitally sign messages
Message Non-repudiation	Digitally sign messages
Message Archive	Automatically archive some or all ingoing and outgoing e-mail to meet organisational or regulatory requirements
Sender Privacy	Strip out or rewrite message headers to remove information such as e-mail aliases, hostnames, and sub-domain information to help keep internal architectures private and protect details of individuals
Information Confidentiality	Drop, quarantine or return to sender outgoing messages based on the recipient's address or address domain, message content, or attachment type
Information and System Integrity	Drop, quarantine or return to sender incoming messages based on the sender's address or address domain, content of message, or attachment type
Information and System Availability	Drop, quarantine or defer delivery of incoming messages based on sender's address or address domain, content of message, attachment type or size of message
Message Disclosure	Automatically add recipients to certain messages in accordance with organisational requirements for monitoring, auditing and legal compliance
Disclaimer/Warning Annotation	Automatically annotate outgoing messages with appropriate warnings or disclaimers based on the recipient's address or address domain, sender's address, or content of message
Notification of Violations	Notify the sender, recipient or other designated person of a policy violation
System Security Management	Restrict access to the functions for configuring the security attributes and policies to only authorised administrators and all associated activities

Table 2 - TOE Security Services

2.4 Software and Hardware outside the Scope

Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Support for, interaction with, and interfaces to the Tumbleweed Integrated Messaging Exchange (IME) product
- The Secure Messaging Redirect Edition of MMS
- Conversion of messages from MIME to UUENCODE and from UUENCODE to MIME
- Any client-side applications including S/MIME clients
- The functionality of the McAfee anti-virus software supplied with the TOE
- Any encryption functionality not explicitly included in the TSFs, in particular excluding unapproved algorithms such as RC4
- Remote administration of the TOE by other than separately encrypted communication channels
- Operating system services not used by the TOE
- All hardware services provided by the defined hardware platforms

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any *assumptions* about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed *threats* to the assets against which specific protection within the TOE or its environment is required.
- Any *organisational security policy* statements or rules with which the TOE must comply.

The TOE is intended to be used in Non-National Security environments where sensitive information up to the Protected level is processed or National Security environments where material up to Restricted is processed.

3.3 Secure Usage Assumptions

The following assumptions relating to the operation of the TOE are made.

Name	Description
A.ADMIN-DOCS	TOE Administrators will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE.
A.ADMIN-COMPETENT	TOE administrators are competent to carry out administration of the TOE, understand the consequences of their actions and the security policies in place.
A.ADMIN-NOEVIL	As the security functions of the TOE can be readily compromised by authorised administrators, it is assumed that they will have successfully completed a security background check before being granted access to the TOE management functions and are assumed to be non-hostile and can be trusted to do their duties correctly.
A.NO-BYPASS	The TOE environment is divided into trusted and untrusted systems. All communication between trusted and untrusted systems is mediated by the TOE. Thus, users cannot bypass the security mechanisms of the TOE.
A.DISASTER	The TOE and its environment have sufficient protections and controls in place to protect the availability of the TOE from natural disasters such as fire or flood, as well as catastrophic failures of power supply and communications.
A.ATTACK	The TOE will be used to protect attractive IT assets and possible attackers can be assumed to have a medium level of expertise, resources and motivation.
A.PHYSICAL	As the TOE operates on an NT platform, logical access controls can be compromised if an attacker gets physical access to the console. Strong physical security countermeasures will therefore be in place.
A.FIREWALL	As the TOE operates on an NT platform, logical access controls can be compromised if an attacker gets online access to the NT computer. Therefore, the TOE will be protected by an EAL-2 -assured or greater firewall product, operated in accordance with government best practice.
A.PLATFORM	The TOE depends on the underlying operating system for security management functions, such as logical access control and auditing for the administration client. The TOE Administrator will operate the TOE from an NT or Windows 2000 workstation in line with the TOE developer's recommendations, as contained in the Administrators Guide.

Name	Description
A.SYSDATA	The TOE relies on an IT system software environment, and TOE users cannot unintentionally overwrite any system programs, logs, or data.
A.NO-USER-CODE	The operating environment provides no user-accessible code, either malicious or non-malicious, that allows modification of the MMS security configuration by other than authorised administrators.

Table 3 - Table of Secure Usage Assumptions

3.4 Threats to Security

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

Threats Addressed by the TOE
The TOE addresses the following threats.

Name	Description
T.ATTACK	An attacker (whether an insider or outsider) performing actions that bypass the TOE security functions may perform actions, including the unauthorised release of information that violate the security policies.
T.CAPTURE	An attacker may eavesdrop on, or otherwise capture, user data or cryptographic key material being transferred across a network.
T.DENY	A user as either originator or recipient may participate in the transfer of information and then deny having done so.
T.IMPERSON	An attacker (an outsider or insider) may, by impersonation of an authorised user of the TOE, gain unauthorised access to user data or cryptographic key material being transferred across a network.
T.CRYPTO	An attacker (whether insider or outsider) may attempt to perform cryptanalysis of data in order to recover user data or cryptographic material.
T.MODIFY	An attacker may, through unauthorised modification or destruction, compromise the integrity of user data or cryptographic key material.
T.BREACH	A user may either deliberately or accidentally attempt to transmit confidential information without appropriate protection measures in place.
T.WRONG	A user may either deliberately or accidentally attempt to transmit information to unauthorised recipients.
T.PRIVATE	An attacker may be able to determine identity details for authorised users in breach of a privacy policy.
T.DOS	An attacker (whether insider or outsider) could execute commands, send data, or perform other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth and processor time.
T.RESOURCES	Non-malicious user action may result in system resources such as bandwidth and processor time being unavailable.
T.FAILURE	Failure of one or more system components of the TOE results in the loss of system-critical functionality.

Table 4 - Table of Threats Addressed by the TOE

Threats Addressed by the Operating Environment

The TOE Operating Environment addresses the following threats.

Name	Description
TE.ADMIN-ERROR	The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.
TE.ENTRY-NON-TECHNICAL	An individual, either internally or externally, using non-technical means may gain access to cryptographic key material or related user data being transferred across a network.
TE.INSTALL	The TOE may be delivered or installed in a manner that undermines security.
TE.OPERATE	Improper operation of the TOE may cause a failure of the TOE security functions.
TE.NO-AUDIT	A TOE Administrator may be able to perform security-relevant actions which cannot be traced or attributed to that person
TE.ACCESS	A person with authorised physical access to the TOE is able to gain unauthorised logical access to the TOE

Table 5 - Table of Threats Addressed by the Operational Environment

3.5 Organisational Security Policies

The table following describes the organisational security policies relevant to the operation of the TOE.

Name	Description
P.AUDIT	Details of user message transactions (including incoming and outgoing messages with details such as sender, recipients, subject, content, etc) will be recorded in an audit trail that must be preserved in line with relevant organisational archive requirements.
P.CRYPTO	All cryptographically-relevant material is to be the subject of rigorous levels of physical and technical control as defined in ACSI 57.
P.NETWORK	The organisation's IT security policy will be maintained in the environment of distributed systems interconnected via insecure networking.
P.INFO-FLOW	The flow of information between IT components in a distributed architecture utilising insecure networks must be controlled and protected from disclosure.
P.ENCRYPT	All confidential, proprietary, or otherwise sensitive information shall be protected, in terms of confidentiality, integrity and authenticity, when transmitted over insecure networks in accordance with the organisational security policy.
P.RECOVERY	The organisation shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.
P.INTEGRITY	The integrity of organisational data will be protected through the identification and treatment of any message content or attachment that might pose a risk. An organisational policy should identify potential risk sources and appropriate actions.
P.AVAILABLE	Organisational bandwidth can be conserved through assigning priorities to messages based on size, content, sender or recipient.
P.PRIVACY	An organisational privacy policy will determine the degree to which an individual’s identity is transmitted out of the organisation, for example through e-mail aliases and sub-domain information.

Table 6 - Table of Organisational Security Policies

4 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterised in the "Security Environment" section of the ST, is to be addressed. Just as some threats are to be addressed by the TOE and others by its intended environment, so some security objectives are for the TOE and others are for its environment. These two classes of security objectives are discussed separately.

4.3 Security Objectives for the TOE

The security objectives for the TOE are as described in the following table.

Name	Description
O.MESSAGE-AUDIT	The TOE must provide the means for recording and archiving messages passing through MMS based on an administrator-defined P.AUDIT Policy.
O.NOREPUD	The TOE must provide a means for generating evidence that can be used to prevent an originator of data from successfully denying ever having sent that data, and evidence that can be used to prevent a recipient of data from successfully denying ever having received that data.
O.MESSAGE-INTEGRITY	The TOE must provide a means of detecting the loss of integrity of messages transferred between users across the telecommunications network.
O.MESSAGE-CONFIDENTIALITY	The TOE must provide the means of protecting the confidentiality of user information when it is transferred across an insecure telecommunications network.
O.INFO-FLOW	The TOE must ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.
O.KEY-CONFIDENTIALITY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are transferred across an insecure telecommunications network.
O.PRIVACY	The TOE must enable the identifying details of users to be protected according to a defined privacy policy.
O.BYPASS	The TOE must prevent users or processes from bypassing or circumventing TOE security policy enforcement.
O.SEPARATION	The TOE must provide a security domain for its own execution that protects it from compromise by unauthorised subjects.
O.STRONG-CRYPTO	The TOE must provide cryptographic service using the strongest possible algorithms and key lengths whilst still maintaining efficiencies.
O.RESOURCES	The TOE must protect itself from user or system errors that result in shared resource exhaustion.

Table 7 - Security Objectives for the TOE

4.4 Security Objectives for the Environment

The security objectives for the TOE environment are those specified in the table below.

Name	Description
OE.INSTALL	Those responsible for the operation of the TOE must ensure that: (a) The TOE is delivered, installed and operated in a manner that preserves IT security. (b) The underlying operating system and / or network services are installed and operated in accordance with the operational documentation for the relevant products.
OE.PHYSICAL	Those responsible for the operation of the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack that might compromise TOE security functions.
OE.FIREWALL	Those responsible for the operation of the TOE must ensure that the TOE is protected from network-based attacks that might compromise TOE security functions.
OE.CRYPTOMANAGE	Those responsible for the TOE must ensure that procedures and / or mechanisms are in place to ensure that storage and handling of cryptographic-related IT assets is conducted in accordance with the rules defined by the P.CRYPTO policy.
OE.TRUST	Those responsible for the TOE must ensure that only highly trusted users are given privileges that enable them to modify the security configurations of the TOE.
OE.ENTRY-NON-TECHNICAL	The TOE environment must provide sufficient protection against non-technical attacks, such as social engineering attacks.
OE.TRAINING	Those responsible for the TOE must ensure that all personnel given administrator privileges or who are to perform crypto-custodian duties are given training sufficient to enable them to fulfill their duties securely.
OE.NO-USER-CODE	TOE administrators must ensure that the TOE environment is such that there is no user-accessible code that could be used to bypass TOE security functions.
OE.PLATFORM	TOE administrators must ensure that they follow the developer's instructions and use the NT User Manager to establish the proper environment for controlling the configuration of the TOE.
OE.I&A	The TOE Operating System must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE facilities.
OE.ADMIN-AUDIT	The TOE Operating System must provide the means for recording security-relevant events in sufficient detail to help an administrator of the TOE to: (c) Detect attempted security violations; and (d) Hold individual users accountable for any actions they perform that are relevant to the security of the TOE.
OE.ADMIN	The TOE, in conjunction with the underlying operating system where necessary, must provide functions to enable an authorised administrator to effectively manage the TOE and its security functions, and ensuring that only authorised administrators can access such functionality.

Table 8 - Security Objectives for the Environment

5 IT Security Requirements

5.3 TOE Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in summary form below.

No.	Component	Component Name
Class FAU: Audit		
1	FAU_ARP.1	Security alarms
2	FAU_GEN.1	Audit data generation
3	FAU_GEN.2	User identity association
4	FAU_SAA.2	Profile based anomaly detection
5	FAU_SAR.1	Audit review
6	FAU_SAR.3	Selectable audit review
7	FAU_SEL.1	Security audit event selection
8	FAU_STG.2	Guarantees of audit data availability
Class FCO: Communication		
9	FCO_NRO.1	Selective proof of origin
10	FCO_NRR.1	Selective proof or receipt
Class FCS: Cryptographic Support		
11	FCS_CKM.1	Cryptographic key generation
12	FCS_CKM.2	Cryptographic key distribution
13	FCS_CKM.4	Cryptographic key destruction
14	FCS_COP.1	Cryptographic operation
Class FDP: User Data Protection		
15	FDP_ETC.2	Export of user data with security attributes
16	FDP_IFC.2	Complete information flow control
17	FDP_IFF.1	Simple security attributes
18	FDP_ITC.2	Import of user data with security attributes
19	FDP_UCT.1	Basic data exchange confidentiality
20	FDP_UIT.1	Data exchange integrity
Class FIA: Identification and Authentication		
21	FIA_ATD.1	User attribute definition
22	FIA_UID.2	User identification before any action
23	FIA_UAU.1	Timing of authentication
Class FMT: Security Management		
24	FMT_MSA.1	Management of security attributes
25	FMT_MSA.2	Secure security attributes
26	FMT_MSA.3	Static attribute initialisation
27	FMT_MTD.1	Management of TSF data
28	FMT_SMR.1	Security roles
Class FPR: Privacy		
29	FPR_PSE.1	Pseudonymity

No.	Component	Component Name
Class FPT: Protection of the TOE Security Functions		
30	FPT_RVM.1	Non-bypassability of the TSP
31	FPT_SEP.1	TSF domain separation
32	FPT_STM.1	Reliable time stamps
33	FPT_TDC.1	Inter-TSF basic TSF data consistency
Class: FRU: Resource Utilisation		
34	FRU_PRS.2	Full priority of service
35	FRU_RSA.1	Maximum quotas
Class FTP: Trusted Path/Channels		
36	FTP_ITC.1	Inter-TSF trusted channel

Table 9 - Functional Components

The following sections contain the functional components from the Common Criteria (CC) Part 2 with the operations completed. The standard CC text is in regular font; the text inserted by the Security Target (ST) author in response to performing CC operations is in red and enclosed in brackets.

5.3.1 Security audit (FAU)

Security alarms (FAU_ARP.1)

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [action to alert the MMS Administrator and other nominated people] upon detection of a potential security violation.

Dependencies FAU_SAA.1 Potential violation analysis

Audit data generation (FAU_GEN.1)

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

(e) Start-up and shutdown of the audit functions;

(f) All auditable events for the [not specified] level of audit; and

(g) All auditable events as described in the [none].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

(h) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

(i) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [none].

Dependencies: FPT_STM.1 Reliable time stamps

User identity association (FAU_GEN.2)

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

Profile based anomaly detection (FAU_SAA.2)

Hierarchical to: FAU_SAA.1

FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [groups of all internal message senders and all external recipient domains].

FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [none].

Dependencies FIA_UID.1 Timing of identification

Audit Review (FAU_SAR.1)

Hierarchical No other components

FAU_SAR.2.1 The TSF shall provide [MMS Administrators] with the capability to read [all audit information] from the audit records.

FAU_SAR.2.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies FAU_GEN.1 Audit data generation

Selectable Audit Review (FAU_SAR.3)

Hierarchical No other components

FAU_SAR.3.1 The TSF shall provide the ability to perform [searches and ordering] of audit data based on [violation type].

Dependencies FAU_SAR.1 Audit review

Selective Audit (FAU_SEL.1)

Hierarchical No other components

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [event type]
b) [message content, message size, attachment type, message sender, message recipient].

Dependencies FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Guarantees of audit data availability (FAU_STG.2)

Hierarchical FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [no audit records are lost] when the following conditions occur: [audit storage exhaustion].

Dependencies FAU_GEN.1 Audit data generation

5.3.2 Communications (FCO)

Selective proof of origin (FCO_NRO.1)

Hierarchical to: No other components.

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [e-mail messages] at the request of the [originator, recipient, [MMS Administrator]].

FCO_NRO.1.2 The TSF shall be able to relate the [identity] of the originator of the information, and the [message body part] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [originator, recipient, [MMS Administrator]] given [the period of time for which the MMS Server Certificate is valid].

Dependencies FIA_UID.1 Timing of identification

Selective proof of receipt (FCO_NRR.1)

Hierarchical to: No other components.

FCO_NRO.1.1 The TSF shall be able to generate evidence of receipt for received [e-mail messages] at the request of the [originator, recipient, [MMS Administrator]].

FCO_NRO.1.2 The TSF shall be able to relate the [identity] of the recipient of the information, and the [message body part] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of receipt of information to [originator, recipient, [MMS Administrator]] given [the period of time for which the MMS Server Certificate is valid].

Dependencies FIA_UID.1 Timing of identification

5.3.3 Cryptographic support (FCS)

Cryptographic key generation (FCS_CKM.1)

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [

a) Triple DES (3DES)

b) RSA]

and specified cryptographic key sizes [

a) 168 bit

b) modulus 1024 bits]

that meet the following: [requirements for cryptographic key generation, as defined by the national COMSEC authority, DSD].

Dependencies FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Cryptographic key distribution (FCS_CKM.2)

Hierarchical to: No other components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA] that meets the following: [requirements for cryptographic key distribution as defined by the national COMSEC authority, DSD].

Dependencies FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Cryptographic key destruction (FCS_CKM.4)

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [deletion] that meets the following: [requirements for cryptographic key destruction as defined by the national COMSEC authority, DSD].

Dependencies FCS_CKM.1 Cryptographic key generation

FMT_MSA.2 Secure security attributes

Cryptographic operation (FCS_COP.1)

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [

a) symmetric key generation;
b) data encryption and decryption;
c) public and private key generation;
d) cryptographic key encryption and decryption;
e) digital signature creation;
f) digital signature verification;
g) secure hash]

in accordance with a specified cryptographic algorithm [

a) triple DES (3DES);
b) triple DES (3DES);
c) RSA
d) RSA;
e) RSA;
f) RSA;
g) MD5]

and cryptographic key sizes [

a) 168;
b) 168;
c) 1024;
d) 1024,
e) 1024;
f) 1024;
g) N/A].

that meet the following: [requirements for cryptographic key management (generation, distribution & destruction) as defined by the national COMSEC authority].

Dependencies FCS_CKM.1 Cryptographic key generation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.3.4 User data protection (FDP)

Export of user data with security attributes (FDP_ETC.2)

Hierarchical to: No other components.

FDP_ETC.2.1 The TSF shall enforce the [Security SFP, Content SFP, Access SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: [no additional rules].

Dependencies FDP_IFC.1 Subset information flow control

Complete information flow control (FDP_IFC.2)

Hierarchical to: No other components.

FDP_IFC.2.1 The TSF shall enforce the [Security SFP] on [

- subject: MMS Server; and
- objects: inbound and outbound messages]

and the [Content SFP] on [

- subject: MMS server; and
- objects: inbound and outbound messages]

and the [Access SFP] on [

- subject: MMS server; and
- objects: inbound and outbound messages]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies FDP_IFF.1 Simple security attributes

Simple security attributes (FDP_IFF.1)

Hierarchical to: No other components.

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

- Identity of the sender
- Identity of the recipient
- Content of message]

and the [Content SFP] based on [

- Identity of sender
- Identity of recipient
- Sender's domain
- Content of message
- Type of attachment]

and the [Access SFP] based on [

- Identity of sender
- Identity of recipient
- Sender's domain
- Recipient's domain
- Message size].

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

a) For the Security SFP

- If the message is intended for an MMS-controlled domain then sign the message with the private key of the sender's MMS server;
- If the message is intended for an MMS-controlled domain and it contains information requiring protection then encrypt the message with the public key of the recipient's MMS server and sign the message with the private key of the sender's MMS server;
- If the message is received from an MMS-controlled domain and contains a digital signature then validate the signature using the sender's MMS server public key;
- If the message is received from an MMS-controlled domain and it is encrypted then decrypt the message using the private key of the recipient's MMS server;
- If the message is intended for a recipient with an S/MIME client (with its public key available to the sender's MMS server) then sign the message with the private key of the sender's MMS server;
- If the message is intended for a recipient with an S/MIME client (with its public key available to the sender's MMS server) then encrypt the message with the public key of the recipient client and sign the message with the private key of the sender's MMS server;
- If the message is received from an S/MIME client (with its public key available to the sender's MMS server) and contains a digital signature then validate the signature using the sender's client public key;

- If the message is received from an S/MIME client (with its public key available to the sender's MMS server) and it is encrypted then decrypt the message using the private key of the recipient's client;
- In all other cases do not apply any security service to the message.

b) For the Content SFP

- If a message from within an MMS-controlled domain contains a threshold number of key restricted words or phrases then drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- If a message from a particular sender to a particular recipient contains a threshold number of key restricted words or phrases then drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- If a message from a particular domain contains a threshold number of key restricted words or phrases then drop or quarantine the message, or add additional recipients, add a warning or disclaimer;
- If a message from within an MMS-controlled domain contains a defined type of attachment then either drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- If a message from a particular sender to a particular recipient contains a defined type of attachment then either drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- In all other cases do not restrict the flow of the message.

c) For the Access SFP

- If the sender or the sender's domain is forbidden then drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- If the recipient or the recipient's domain is forbidden then drop, quarantine, add additional recipients, add a warning or disclaimer, or return the message to the sender;
- If the message size is above the defined threshold then either drop, quarantine, or defer delivery of the message;
- In all other cases do not restrict the flow of the message.

FDP_IFF.1.3 The TSF shall enforce [no additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall provide [no additional information flow control SFP capabilities].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules:[no additional rules].

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

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

Import of user data with security attributes (FDP_ITC.2)

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [Security SFP, Content SFP, Access SFP] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [no additional rules]

Dependencies FDP_IFC.1 Subset information flow control

FTP_ITC.1 Inter-TSF trusted channel

FPT_TDC.1 Static attribute initialisation

Basic data exchange confidentiality (FDP_UCT.1)

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the [Security SFP] to be able to [transmit, receive] objects in a manner protected from unauthorised disclosure.

Dependencies FTP_ITC.1 Inter-TSF trusted channel

FDP_IFC.1 Subset information flow control

Data exchange integrity (FDP_UIT.1)

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the [Security SFP] to be able to [transmit, receive] user data in a manner protected from [modification, deletion, insertion, replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion, replay] has occurred.

Dependencies FTP_ITC.1 Inter-TSF trusted channel

FDP_IFC.1 Subset information flow control

5.3.5 Identification and authentication (FIA)

User attribute definition (FIA_ATD.1)

Hierarchical to: No other components.

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

- X.509 identity certificate;
- Internet e-mail address].

Dependencies No dependencies

Timing of authentication (FIA_UAU.1)

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [any message, not requiring the application of digital signature or encryption services, to be processed by the MMS server]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies FIA_UID.1 Timing of identification

User identification before any action (FIA_UID.2)

Hierarchical to: No other components.

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies No dependencies

5.3.6 Security management (FMT)

Management of security attributes (FMT_MSA.1)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [System Security Management SFP] to restrict the ability to [add, change or delete] the security attributes [○ User attributes: (X.509 certificate); ○ Subject (MMS Server) attributes: (those required to define and control information flows); ○ Subject (MMS Server) attributes: (those required to apply security services to information flows)]. to [authorised system administrators].
Dependencies	FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles

Secure security attributes (FMT_MSA.2)

Hierarchical to:	No other components.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
Dependencies	ADV_SPM.1 Informal TOE security policy model FDP_IFC.1 Subset information flow control FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

Static attribute initialisation (FMT_MSA.3)

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [the System Security Management SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [authorised administrator] to specify alternative initial values to override the default values when an object or information is created.
Dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

Management of TSF data (FMT_MTD.1)

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [change_default, modify, delete, clear] the [system configuration and security attributes] to [authorised administrators].

Dependencies FMT_SMR.1 Security roles

Security roles (FMT_SMR.1)

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [MMS Administrator].

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

Dependencies FIA_UID.1 Timing of identification

5.3.7 Privacy (FPR)

Pseudonymity (FPR_PSE.1)

Hierarchical to: No other components

FPR_PSE.1.1 The TSF shall ensure that [entities external to an MMS-controlled domain] are unable to determine the real user name bound to [messages transmitted by entities within an MMS-controlled domain].

FPR_PSE.1.2 The TSF shall be able to provide [at least one] alias of the real user name to [entities external to an MMS-controlled domain].

FPR_PSE.1.3 The TSF shall [determine an alias for a user] and verify that it conforms to the [condition that it does not reveal any unnecessary information as defined by the organisational privacy policy].

Dependencies No dependencies

5.3.8 Protection of the TOE Security Functions (FPT)

Non-bypassability of the TSP (FPT_RVM.1)

Hierarchical to: No other components

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies No dependencies

TSF domain separation (FPT_SEP.1)

Hierarchical to: No other components

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies No dependencies

Reliable time stamps (FPT_STM.1)

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies No dependencies

Inter-TSF basic TSF data consistency (FPT_TDC.1)

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [encryption and digital signatures attributes defined in the S/MIME standard] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [the rules defined in the S/MIME standard] when interpreting the TSF data from another trusted IT product.

Dependencies No dependencies

5.3.9 Resource Utilisation (FRU)

Full priority of service (FRU_PRS.2)

Hierarchical to: FRU_PRS.1

FRU_PRS.2.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.2.2 The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.

Dependencies No dependencies

Maximum Quotas (FRU_RSA.1)

Hierarchical to: No other components

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [network bandwidth] that [users inside an MMS-controlled domain and entities transmitting into an MMS-controlled domain] can use [simultaneously].

Dependencies No dependencies

5.3.10 Trusted Path/Channels (FTP)

Inter-TSF trusted channel (FTP_ITC.1)

Hierarchical to: No other components

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, or 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 [in accordance with the Security SFP].

Dependencies No dependencies

5.4 TOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements are listed in summary form in Table 10, below.

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.2	Configuration items
Class ADO: Delivery and Operation		
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation and start-up
Class ADV: Development		
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high level design
6	ADV_RCR.1	Informal representational correspondence
Class AGD: Guidance documents		
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
Class ATE: Tests		
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing- sample
Class AVA: Vulnerability Assessment		
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Table 10 - TOE Assurance Requirements

5.4.1 Configuration management (ACM)

Configuration Items (ACM_CAP.2)

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

5.4.2 Delivery and operation (ADO)

Delivery procedures (ADO_DEL.1)

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

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

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.

Installation, generation, and start-up procedures (ADO_IGS.1)

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

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

5.4.3 Development (ADV)

Informal functional specification (ADV_FSP.1)

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

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.

Descriptive high level design (ADV_HLD.1)

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C 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.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Informal correspondence demonstration (ADV_RCR.1)

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

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.

5.4.4 Guidance documents (AGD)

Administrator guidance (AGD_ADM.1)

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

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.

User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

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.

5.4.5 Tests (ATE)

Evidence of coverage (ATE_COV.1)

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

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.

Functional testing (ATE_FUN.1)

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

ATE_FUN.1.2D The developer shall provide test documentation.

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.

Independent testing - sample (ATE_IND.2)

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

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.

5.5 Security Requirements for the IT Environment

The TOE has no security requirements allocated to its IT environment.

5.6 Security Requirements for the Non-IT Environment

ENV_NONIT.1 MMS Server protected by Firewall.
The MMS Server must be protected from unauthorised modification by potentially hostile outsiders by a firewall of at least EAL-2 level of assurance, or equivalent.

ENV_NONIT.2 MMS Server is to be Physically Protected.
The MMS Server must be located within a controlled access facility that will prevent unauthorised physical access.

ENV_NONIT.3 Access to the MMS Server is restricted to administrators only.
The MMS Server and associated directly-attached console must be physically secure and available to authorised administrators only.

ENV_NONIT.4 Protection against non-technical attacks.
The TOE environment must provide sufficient protection against non-technical attacks, such as social-engineering attacks.

ENV_NONIT.5 MMS Server administrators are trusted.
The TOE environment must provide a mechanism that ensures that the likelihood of administration staff performing illegal actions is minimised.

ENV_NONIT.6 MMS Server has no user-accessible code.
The TOE environment must ensure that at any time no user-accessible code that may modify TOE security functions exists on the MMS Server.

ENV_NONIT.7 MMS Server is installed and configured according to developer guidance.
The MMS Server must be installed and configured in line with the developer's guidance and administrators must ensure that the configuration remains in step with developer's ongoing guidance.

ENV_NONIT.8 Protection against unauthorised access to / loss of cryptographic keys.
The TOE environment must ensure that at all times cryptographic keys are protected against unauthorised access, loss or destruction.

ENV_NONIT.9 MMS Server administrators are well-trained.
The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

ENV_NONIT.10 Controlled Administrator Access to MMS Server

The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that access is limited to only authorised TOE Administrators. For examples, accounts on the TOE platform should only exist for authorised TOE Administrators.

ENV_NONIT.11 Auditing of MMS Administrator Actions

The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that actions by the MMS Administrator including the modification of security attributes, the modification of MMS policies, and the configuration of the audit function itself are audited.

ENV_NONIT.12 Protection of TSF data and attributes

The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that the storage of TSF data and attributes including cryptographic material, policy configuration data, and message archives are appropriately protected.

ENV_NONIT.13 Facilities to configure the security features of the MMS Server

The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that configuration of the security features through the creation, review and modification of policies and key word lists can be performed.

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.3 IT Security Functions

This section presents the security functions performed by the TOE and provides a mapping between the identified security functions and the Security Functional Requirements that it must satisfy.

6.3.1 Message Confidentiality MES_CON

MMS Server through the Security Manager provides message confidentiality services using S/MIME encryption. Using the Security Manager to define the Security SFP, an MMS Administrator can perform the following functions:

- Establish S/MIME VPNs with other MMS servers;
- Create S/MIME key pairs and certificates on behalf of the local domain;
- Encrypt and decrypt mail on behalf of the domain users;
- Automate certificate exchange and manage correspondents' certificates to facilitate symmetric key management for encryption using triple DES; and
- Perform encryption and decryption actions as directed by other MMS Policy Managers.

6.3.2 Message Integrity MES_INT

MMS Server through the Security Manager provides message integrity services using S/MIME signatures. Using the Security Manager to define the Security SFP, an MMS Administrator can perform the following functions:

- Through the establishment of S/MIME VPNs with other MMS servers, create hashes of messages using MD5 and then digitally sign those hashes using RSA;
- Create S/MIME key pairs and certificates on behalf of the local domain;
- Sign and verify mail on behalf of the domain users;
- Automate certificate exchange and manage correspondents' certificates; and
- Perform signature and verification actions as directed by other MMS Policy Managers.

6.3.3 Message Non-repudiation MES_NOR

MMS Server through the Security Manager provides message non-repudiation services using S/MIME encryption. Using the Security Manager to define the Security SFP, an MMS Administrator can perform the following functions:

- Enable non-repudiation of both sender and recipient through the establishment of S/MIME VPNs with other MMS servers;
- Create S/MIME key pairs and certificates on behalf of the local domain;
- Encrypt, decrypt, sign and verify mail on behalf of the domain users;
- Automate certificate exchange and manage correspondents' certificates; and
- Perform encryption, decryption, signature and verification actions as directed by other MMS Policy Managers.

6.3.4 Message Archive MES_ARC

The MMS Server can enforce an archiving policy on all messages flowing into and out of the MMS-controlled domain. The MMS Configuration Program is used to define where archives should be stored, the storage format, and indexing options. The MMS Server uses its system time to apply a timestamp to the archive. Once archiving has been set up, any other MMS Policy Manager can define archive as an action to be performed on any ingoing or outgoing messages.

Organisational message archiving and monitoring policies will define the rules under which the functionality is applied. The organisational monitoring policy will define when, where, how and who should review and monitor messages which are archived under the organisational message archiving policy.

6.3.5 Sender Privacy SEN_PRI

MMS Server through the Format Manager can provide message header stripping and re-writing services. In conjunction with an organisational privacy policy, the Format Manager can be configured to remove sensitive information such as aliases, distinguished names, and internal domain information from message headers. Format Manager can also replace sensitive header information with other, more generic details. As well as protecting individual user privacy, the Format Manager can also be used to provide some protection against outside attack by removing internal network architecture details from message headers.

6.3.6 Information Confidentiality INF_CON

MMS Server through the Content Manager can prevent sensitive organisational information from leaving the organisation through e-mail. Content filtering, configured through the Content Manager, can be used to monitor the content of messages and attachments and to take actions based on the occurrence of certain words or phrases. Key word weighting, using numeric values assigned to key words and phrases, can be used to ensure that the Content Policy is only triggered when the total numeric value of certain key words reaches or exceeds a pre-defined threshold. The MMS Server includes pre-defined word lists for generic confidential information.

The actions which can be taken once a key word threshold is reached, include:

- Drop the message (i.e. do not transit the message any further)
- Quarantine the message for later review by an MMS Administrator or other designated person
- Return the message to the sender
- Send a violation notification to the MMS Administrator, the sender, or other designated person
- Archive the message
- Annotate the message with a warning that might state that the message contains confidential information, is only intended for the authorised recipient, and should not be further transmitted.

6.3.7 Information and System Integrity INF_INT

MMS Server through the Virus Manager and Access Manager can prevent critical organisational information and systems from being affected by incoming messages containing malicious or unwanted material. Access Controls can be imposed through the Access Manager based on the source or destination address or address domain.

Virus detection and disinfection is configured through the Virus Manager and interfaces with the server-based McAfee anti-virus technology from Network Associates. Through the Virus Manager, MMS Server can detect and optionally clean or strip infected attachments from incoming (outgoing) messages. The Virus Manager can also be used to configure periodic automatic updates of the anti-virus software.

The actions which can be through either of the above Policy Managers, include:

- Drop the message (i.e. do not allow the message into the MMS-controlled domain)
- Quarantine the message for later review by an MMS Administrator or other designated person
- Return the message to the sender
- Send a violation notification to the MMS Administrator, the sender, or other designated person
- Archive the message

6.3.8 Information and System Availability INF_AVA

MMS Server through the Virus Manager, Content Manager and Access Manager can protect the availability of critical organisational information and systems from being affected by incoming messages containing malicious or unwanted material, or by very large incoming or outgoing messages.

Content filtering, configured through the Content Manager, can be used to monitor the content of messages and attachments and to take actions based on the occurrence of certain words or phrases. Key word weighting, using numeric values assigned to key words and phrases, can be used to ensure that the Content Policy is only triggered when the total numeric value of certain key words reaches or exceeds a pre-defined threshold. The MMS Server includes pre-defined word lists for generic SPAM, chain letters, and virus hoax information.

Access Controls can be imposed through the Access Manager based on the source or destination address or address domain, or message size.

Virus detection and disinfection is configured through the Virus Manager and interfaces with the server-based McAfee anti-virus technology from Network Associates. Through the Virus Manager, MMS Server can detect and optionally clean or strip infected attachments from incoming (outgoing) messages. The Virus Manager can also be used to configure periodic automatic updates of the anti-virus software.

The actions which can be through any of the above Policy Managers, include:

- Drop the message (i.e. do not allow the message into or out of the MMS-controlled domain)
- Quarantine the message for later review by an MMS Administrator or other designated person
- Return the message to the sender
- Send a violation notification to the MMS Administrator, the sender, or other designated person
- Defer delivery of the message to an off-peak period

6.3.9 Message Disclosure MES_DIS

For reasons of activity monitoring, or regulatory or legal compliance, an organisation can use MMS Server to automatically add recipients to message coming into or out of an organisation. For example, an outgoing message which was detected (by the Content Manager) to contain information relating to contracts could also be automatically sent to the organisation’s contracts officer. Similarly, an incoming message from a competitor’s e-mail domain (detected by Access Manager) could be automatically sent on to the organisation’s legal department.

6.3.10 Disclaimer/Warning Annotation DIS_ANN

Through the use of the MMS Annotation function, an organisation can automatically add text such as legal and privacy disclaimers or warnings about non-work-related e-mail to any incoming or outgoing messages based on definitions within the Content or Access Policy Managers. Annotations can be inserted into the text of the message or added as attachments.

6.3.11 Notification of Violations NOT_VIO

Upon the detection of a policy violation by any of the policy managers, a notification of the event can be sent to the MMS Administrator, to the sender of the message, or to any other designated person within the organisation. For example, if the policy violation related to offensive or inappropriate material then a notification may be sent to the organisation's HR or legal department. The notification activity can be implemented within any of the MMS policy managers.

6.3.12 System Security Management SYS_MAN

Through the MMS policy managers, including Content, Access, Security and Virus, the MMS Administrator is able to configure the MMS Server to implement the appropriate organisational policies relating to confidentiality, integrity, availability, privacy, and non-repudiation.

The MMS Administrator accesses the policy managers on the MMS Server via a directly connected Windows NT or Windows 2000 workstation. The MMS Administrator must ensure that the following security services relating to the MMS Server platform and the administration workstation are correctly configured:

- User accounts on the MMS Server and workstation should only exist for authorised MMS Administrators;
- Those user accounts should be configured to have to minimum privileges necessary to perform the administration activities;
- A strong password policy should be established for those user accounts;
- The file and directory access controls should be very restrictive, particularly relating to the storage of cryptographic material;
- The Windows NT and Windows 2000 Event Log should be configured to ensure that all security-relevant events conducted by MMS Administrators are audited including changes to the MMS configurations, changes to the operating system configurations, administrator access, and changes to the Event Log. The MMS Administrator should configure the Event Log based on an Audit Policy for the system. The MMS Administrator should have procedures for reviewing and analysing the logs and for preventing log exhaustion.

Configuration and use of these system security administration functions should be performed in accordance with an organisation-defined System Security Management policy.

6.4 Assurance Measures

Tumbleweed MMS Release 4.6 claims to satisfy the assurance requirements for Evaluation Assurance Level EAL2. This section identifies the Configuration Management, System Development Procedures, System Test Documentation and System Installation and Guidance Documentation measures applied by Tumbleweed MMS to satisfy the CC EAL2 assurance requirements as defined in Part 3 of the Common Criteria.

6.4.1 Configuration Management CON_MAN

The Configuration Management measures applied by Tumbleweed include assigning a unique product identifier for each release of the TOE. Associated with this Product Identifier is a list of Hardware and Software configuration items that compose a single instance of the TOE. These configuration management measures are documented within the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Administrator's Guide
- Tumbleweed MMS Release 4.6 Release Notes

In addition, the Tumbleweed Configuration Management documentation includes a configuration list, which describes the configuration items that comprise the TOE, and the method used to uniquely identify the configuration items. The Tumbleweed Configuration Management documentation can be found in the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Configuration Management

6.4.2 Delivery and Operation DEL_OPS

The Guidance Documents provided by Tumbleweed include both Installation and Configuration manuals that guide administrators through the process of unpacking, installing, and starting-up the MMS Server. These documents also warn the administrator about common mistakes that could lead to an insecure configuration. These guidance measures are documented within the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Administrator's Guide
- Tumbleweed MMS Release 4.6 Release Notes

The procedures for secure delivery of the MMS system to an end-user are documented in the following Tumbleweed document:

- Tumbleweed MMS Release 4.6 Delivery Procedures

6.4.3 Development DEV_DOC

The documents provided by the developer satisfy the functional specification requirements in that they provide an informal specification describing the TSF interfaces and details of effects and error messages. The documents also satisfy the high level design requirements to describe the structure of the TSF in terms of subsystems and to describe the functions and interfaces of those subsystems. These design descriptions are documented within the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Administrator's Guide
- Tumbleweed MMS Release 4.6 Release Notes
- Tumbleweed MMS Release 4.6 Design

The correspondence between adjacent pairs of TSF representations and associated analyses are provided in this Security Target and in the document:

- Tumbleweed MMS Release 4.6 Representational Correspondence

6.4.4 Guidance ADM_DOC

Guidance is provided to assist administrators in the process of the day-to-day administration of the Tumbleweed MMS Server. These documents also warn the administrator about functions and privileges that should be controlled. The MMS product does not support direct end-users and so no user guidance is required. These guidance measures are documented within the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Administrator's Guide
- Tumbleweed MMS Release 4.6 Release Notes

2.4.1 Testing TST_DOC

Test documentation needs to include test plans, procedures, expected and actual results. Documentation of the developer's functional testing including an analysis of test coverage is included in the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Design
- Tumbleweed MMS Release 4.6 Test Documentation

2.4.2 Vulnerability Assessment VUL_ASS

Two vulnerability assessment activities have been documented by the developer. These included an evaluation of the strength of TOE security functions and a determination of whether the TOE, in its intended environment, has obvious exploitable vulnerabilities. These assessments have been recorded in the following Tumbleweed documents:

- Tumbleweed MMS Release 4.6 Vulnerability Assessment
- Tumbleweed MMS Release 4.6 Design

6.4.5 Mapping of Assurance Measures to Assurance Requirements

The table below describes the mapping between the assurance measures of the TOE and the SARs as required by the assurance level (EAL-2).

Assurance Measures	Security Assurance Requirements												
	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	AVD_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
CON_MAN	✔												
DEL_OPS		✔	✔										
DEV_DOC				✔	✔	✔							
ADM_DOC							✔						
TST_DOC								N/A	✔	✔	✔		
VUL_ASS												✔	✔

Table 11 - Mapping Between SARs and Assurance Measures

The TOE does not have any direct end-users and so no TOE assurance measures are provided. Therefore the AGD_USR.1 SAR is not considered appropriate for this TOE.

7 PP Claims

The Tumbleweed MMS Release 4.6 Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are *suitable*, that is they are *sufficient* to address the security needs, and that they are *necessary*, ie, there are no redundant security objectives.

8.1.1 All Assumptions, Policies and Threats Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section shows that all of the secure usage assumptions, organisational security policies, and threats to security have been addressed.
- The second section shows that each IT security objective and each Non-IT security objective counters at least one assumption, policy, or threat.

Threat Label	Threat Short Description	Associated Security Objective
T.ATTACK	Bypass the TSF to violate security policies	O.BYPASS O.SEPARATION O.INFO-FLOW OE.PHYSICAL
T.CAPTURE	Eavesdrop on information transfer	O.MESSAGE-CONFIDENTIALITY O.KEY-CONFIDENTIALITY
T.DENY	Deny taking part in a message transaction	O.NOREPUD
T.IMPERSON	Impersonate an authorised user to gain unauthorised access	O.MESSAGE-CONFIDENTIALITY O.KEY-CONFIDENTIALITY O.STRONG-CRYPTO
T.CRYPTO	Perform cryptanalysis	O.STRONG-CRYPTO
T.MODIFY	Unauthorised modification or destruction of data or cryptographic material	O.MESSAGE-INTEGRITY
T.BREACH	Transmit confidential information without protection	O.MESSAGE-CONFIDENTIALITY O.KEY-CONFIDENTIALITY O.INFO-FLOW
T.WRONG	Transmit information to the wrong recipient	O.INFO-FLOW
T.PRIVATE	Obtain personal details in breach of privacy	O.PRIVACY
T.DOS	Deliberately make system resources such as bandwidth unavailable	O.RESOURCES
T.RESOURCES	Inadvertently make system resources such as bandwidth unavailable	O.RESOURCES
T.FAILURE	One or more system components may fail	O.BYPASS O.SEPARATION
TE.ADMIN-ERROR	Administration errors could defeat TOE security	OE.INSTALL OE.TRAINING OE.TRUST
TE.ENTRY-NON-TECHNICAL	Entry to the information could be gained through non-technical means	OE.ENTRY-NON-TECHNICAL
TE.INSTALL	The TOE could be installed insecurely	OE.INSTALL
TE.OPERATE	The TOE could be operated improperly or insecurely	OE.INSTALL OE.TRAINING OE.TRUST
TE.NO-AUDIT	A TOE administrator could perform untraceable actions	OE.ADMIN-AUDIT

Threat Label	Threat Short Description	Associated Security Objective
TE.ACCESS	A person with authorised physical access could gain unauthorised logical access	OE.I&A

Table 12 - All Threats to Security Addressed by Objectives

Policy Label	Policy Short Description	Associated Security Objective
P.AUDIT	Archiving of ingoing and outgoing messages	O.MESSAGE-AUDIT
P.CRYPTO	Cryptographic material controlled as defined in ACSI 57	O.KEY-CONFIDENTIALITY OE.CRYPTOMANAGE OE.TRUST
P.NETWORK	IT security policy maintained	O.INFO-FLOW O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY O.MESSAGE-AUDIT O.NOREPUD OE.INSTALL
P.INFO-FLOW	Information in a distributed architecture is controlled and protected	O.INFO-FLOW
P.RECOVERY	Procedures and mechanisms to ensure secure recovery after failure	O.SEPARATION OE.ADMIN OE.NO-USER-CODE
P.INTEGRITY	Protection of the integrity of organisational data from incoming messages	O.INFO-FLOW O.BYPASS OE.NO-USER-CODE
P.AVAILABLE	Prioritising messages to conserve organisational bandwidth	O.INFO-FLOW O.RESOURCES
P.PRIVACY	Identification of the level of personal information is transmitted out of the organisation	O.PRIVACY
P.ENCRYPT	The confidentiality, integrity, and authenticity of messages transmitted over insecure networks is protected using cryptography	O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY O.NOREPUD O.KEY-CONFIDENTIALITY

Table 13 - All Organisational Policies met by Objectives

Assumption Label	Assumption Short Description	Associated Security Objective
A.ADMIN-DOCS	Administrators will follow documented procedures	OE.INSTALL OE.CRYPTOMANAGE OE.TRAINING
A.ADMIN-COMPETENT	TOE Administrators are able to carry out their duties	OE.TRAINING
A.ADMIN-NOEVIL	Administrators are non-hostile	OE.TRUST
A.NO-BYPASS	TOE mediates all communications between trusted and untrusted environments	O.BYPASS O.SEPARATION OE.PHYSICAL
A.DISASTER	Protection against natural disasters	OE.PHYSICAL
A.ATTACK	Attackers have medium levels of skill.	OE.INSTALL OE.PHYSICAL OE.FIREWALL OE.ADMIN
A.FIREWALL	Approved firewall to protect facility.	OE.FIREWALL
A.PHYSICAL	NT workstation protected by strong physical safeguards	OE.PHYSICAL

Assumption Label	Assumption Short Description	Associated Security Objective
A.PLATFORM	TOE depends on the NT operating system for security management functions	OE.ADMIN OE.PLATFORM OE.ADMIN-AUDIT
A.NO-USER-CODE	No user-accessible code in TOE	O.SEPARATION OE.INSTALL OE.NO-USER-CODE
A.SYSDATA	The TOE relies on the IT environment to protect system data.	OE.INSTALL OE.PLATFORM OE.ADMIN-AUDIT OE.ADMIN

Table 14 - All Secure Usage Assumptions met by Objectives

The table below shows that there are no unnecessary IT security objectives.

Objective Label	Objective Short Description	Threat / Policy/ Assumption
O.MESSAGE-AUDIT	Facilities to be provided to archive messages.	P.AUDIT P.NETWORK
O.NOREPUD	Facilities to be provided to prevent repudiation of data sent.	T.DENY P.NETWORK P.ENCRYPT
O.MESSAGE-INTEGRITY	Facilities to be provided to prevent loss of data integrity.	T.MODIFY P.NETWORK P.ENCRYPT
O.MESSAGE-CONFIDENTIALITY	Facilities to be provided to protect data in transit.	T.CAPTURE T.IMPERSON T.BREACH P.NETWORK P.ENCRYPT
O.INFO-FLOW	Facilities to be provided to enforce information flow control policies	T.ATTACK T.BREACH T.WRONG P.NETWORK P.INFO-FLOW P.INTEGRITY P.AVAILABLE
O.KEY-CONFIDENTIALITY	Facilities to be provided to protect cryptographic keys	T.CAPTURE T.IMPERSON T.BREACH P.CRYPTO P.ENCRYPT
O.PRIVACY	Facilities to be provided to protect the privacy of users within the organisation	T.PRIVATE P.PRIVACY
O.BYPASS	No bypass of policy enforcement	T.ATTACK T.FAILURE P.INTEGRITY A.NO-BYPASS
O.SEPARATION	Maintenance of TOE security domain.	T.ATTACK T.FAILURE P.RECOVERY A.NO-BYPASS A.NO-USER-CODE
O.RESOURCES	Facilities to prevent shared resource exhaustion.	T.DOS T.RESOURCES P.AVAILABLE
O.STRONG-CRYPTO	Provision of suitably strong cryptographic services	T.IMPERSON T.CRYPTO

Objective Label	Objective Short Description	Threat / Policy/ Assumption
OE.INSTALL	TOE installed and operated properly	TE.ADMIN-ERROR TE.INSTALL TE.OPERATE P.NETWORK A.ADMIN-DOCS A.ATTACK A.NO-USER-CODE A.SYSDATA
OE.PHYSICAL	Protected from physical attack.	T.ATTACK A.NO-BYPASS A.DISASTER A.ATTACK A.PHYSICAL
OE.FIREWALL	TOE protected from network attacks	A.ATTACK A.FIREWALL
OE.CRYPTOMANAGE	Crypto assets managed properly	P.CRYPTO A.ADMIN-DOCS
OE.TRUST	Administrators are highly trusted	TE.ADMIN-ERROR TE.OPERATE P.CRYPTO A.ADMIN-NOEVIL
OE.ENTRY-NON-TECHNICAL	Protection against non-technical attacks.	TE.ENTRY-NON-TECHNICAL
OE.TRAINING	Operators are given sufficient training to perform their duties	TE.ADMIN-ERROR TE.OPERATE A.ADMIN-DOCS A.ADMIN-COMPETENT
OE.NO-USER-CODE	No user-accessible code in the TOE operating environment	P.RECOVERY P.INTEGRITY A.NO-USER-CODE
OE.PLATFORM	Administrator will operate the server function in line with developer's guidance	A.PLATFORM A.SYSDATA
OE.I&A	Facilities to be provided to prevent unauthorised user activities.	TE.ACCESS
OE.ADMIN-AUDIT	Facilities to be provided to record activity on the TOE.	TE.NO-AUDIT A.PLATFORM A.SYSDATA
OE.ADMIN	Facilities provided to manage the TOE.	P.RECOVERY A.ATTACK A.PLATFORM A.SYSDATA

Table 15 - All Security Objectives Necessary

8.1.2 Security Objectives are Sufficient

The following arguments provided below are offered to demonstrate the sufficiency of the Security Objectives outlined above.

Threat Label	Argument to support Security Objective sufficiency
T.ATTACK	The objectives (O.BYPASS, O.SEPARATION, O.INFO-FLOW, OE.PHYSICAL) will provide an effective countermeasure as: - the TSP will prevent bypass of the TSFs - a separate domain is maintained for the TOE's operation - information flow control policies will be enforced - the TOE will be protected against direct physical attack

Threat Label	Argument to support Security Objective sufficiency
T.CAPTURE	The objectives (O.MESSAGE-CONFIDENTIALITY, O.KEY-CONFIDENTIALITY) will provide an effective countermeasure as: - data is protected from eavesdropping while in transit - all cryptographic keys are protected
T.DENY	The objective (O.NOREPUD) will provide an effective countermeasure as: - the TOE prevents repudiation of data sent
T.IMPERSON	The objective (O.MESSAGE-CONFIDENTIALITY, O.KEY-CONFIDENTIALITY, O.STRONG-CRYPTO) will provide an effective countermeasure as: - data is protected against eavesdropping and can only identified as having been sent by an authorized user - keys used to protect data are themselves protected - strong cryptography is used to defeat a direct attack on the protection mechanisms
T.CRYPTO	The objective (O.STRONG-CRYPTO) will provide an effective countermeasure as: - strong cryptography is used to defeat direct attacks on the cryptographic mechanisms
T.MODIFY	The objective (O.MESSAGE-INTEGRITY) will provide an effective countermeasure as: - data is protected against the loss of integrity
T.BREACH	The objectives (O.MESSAGE-CONFIDENTIALITY, O.KEY-CONFIDENTIALITY, O.INFO-FLOW) will provide an effective countermeasure as: - confidential information can be protected against eavesdropping - keys used to protect the data are themselves protected - information flow control policies can be set to ensure that data protection is applied when appropriate
T.WRONG	The objective (O.INFO-FLOW) will provide an effective countermeasure as: - information flow control policies can be set to ensure that data is not sent to unauthorized recipients
T.PRIVATE	The objective (O.PRIVACY) will provide an effective countermeasure as: - personal details of users can be hidden to protect the privacy of the users within an organization
T.DOS	The objective (O.RESOURCES) will provide an effective countermeasure as: - limits can be set to prevent the deliberate exhaustion of system resources
T.RESOURCES	The objective (O.RESOURCES) will provide an effective countermeasure as: - limits can be set to prevent the accidental exhaustion of system resources
T.FAILURE	The objectives (O.BYPASS, O.SEPARATION) will provide an effective countermeasure as: - the TSP will prevent bypass of the TSFs - a separate domain is maintained for the TOE's operation
TE.ADMIN-ERROR	The objectives (OE.INSTALL, OE.TRAINING, OE.TRUST) will provide an effective countermeasure as: - the TOE is installed and operated properly - the TOE administrators are properly trained and trusted

Threat Label	Argument to support Security Objective sufficiency
TE.ENTRY-NON-TECHNICAL	The objective (OE.ENTRY-NON-TECHNICAL) will provide an effective countermeasure as: - protection is provided against non-technical attacks
TE.INSTALL	The objective (OE.INSTALL) will provide an effective countermeasure as: - the TOE is installed and operated properly
TE.OPERATE	The objectives (OE.INSTALL, OE.TRAINING, OE.TRUST) will provide an effective countermeasure as: - the TOE is installed and operated properly - the TOE administrators are properly trained and trusted
TE.NO-AUDIT	The objective (OE.ADMIN-AUDIT) will provide an effective countermeasure as: - facilities are provided to audit administrator activities affecting the TOE
TE.ACCESS	The objective (OE.I&A) will provide an effective countermeasure as: - facilities are provided to control logical access to the TOE

Table 16 - Sufficiency of Security Objectives (1)

Policy Label	Argument to support Security Objective sufficiency
P.AUDIT	The objective (O.MESSAGE-AUDIT) will provide complete coverage as: - it specifies audit trail generation and archive requirements
P.CRYPTO	The objectives (O.KEY-CONFIDENTIALITY, OE.CRYPTOMANAGE, OE.TRUST) will provide complete coverage as: - they specify a key management plan to be implemented by trusted administrators inline with ACSI 57
P.NETWORK	The objectives (O.INFO-FLOW, O.MESSAGE-CONFIDENTIALITY, O.MESSAGE-INTEGRITY, O.MESSAGE-AUDIT, O.NOREPUD, OE.INSTALL) will provide complete coverage as: - they specify a security environment in which the network can operate securely when connected to an untrusted network
P.INFO-FLOW	The objective (O.INFO-FLOW) will provide complete coverage as: - it specifies the requirements by which all information flows, both inwards and outwards, are controlled and handled
P.RECOVERY	The objectives (O.SEPARATION, OE.ADMIN, OE.NO-USER-CODE) will provide complete coverage as: - they provide for the secure operation of the TOE, in a separate execution domain and without the possibility of interference from introduced code
P.INTEGRITY	The objectives (O.INFO-FLOW, O.BYPASS, OE.NO-USER-CODE) will provide complete coverage as: - they provide for the control and management of all incoming data without being bypassed or interfered with by introduced code

Policy Label	Argument to support Security Objective sufficiency
P.AVAILABLE	The objectives (O.INFO-FLOW, O.RESOURCES) will provide complete coverage as: - they provide for the control, limiting and prioritization of all incoming and outgoing messages
P.PRIVACY	The objective (O.PRIVACY) will provide complete coverage as: - it provides the ability to define the level of personal information is revealed when message leave the organization
P.ENCRYPT	The objectives (O.MESSAGE-CONFIDENTIALITY, O.MESSAGE-INTEGRITY, O.NOREPUD, O.KEY-CONFIDENTIALITY) will provide complete coverage as: - they provide for the protection of the confidentiality, integrity and non-repudiation of messages and for the protection of the keys used to provide these services

Table 17 - Sufficiency of Security Objectives (2)

Assumption Label	Associated Security Objective
A.ADMIN-DOCS	The objectives (OE.INSTALL, OE.CRYPTOMANAGE, OE.TRAINING) uphold the assumption as: - the administrators are provided with the appropriate training and documentation to enable them to operate the TOE properly and to manage its sensitive crypto material properly
A.ADMIN-COMPETENT	The objective (OE.TRAINING) upholds the assumption as: - the administrators undergo sufficient and appropriate training for their tasks
A.ADMIN-NOEVIL	The objective (OE.TRUST) upholds the assumption as: - all administrators are sufficiently trusted for the privileged duties they perform
A.NO-BYPASS	The objectives (O.BYPASS, O.SEPARATION, OE.PHYSICAL) uphold the assumption as: - they prevent the bypass of the TSP, provide a separate execution domain for the TOE, and prevent unauthorized physical access to the TOE
A.DISASTER	The objective (OE.PHYSICAL) upholds the assumption as: - it physically protects the TOE against harm
A.ATTACK	The objectives (OE.INSTALL, OE.PHYSICAL, OE.FIREWALL, OE.ADMIN) uphold the assumption as: - the TOE itself does not provide sufficient safeguards against skilled hackers, however the addition of strong physical protection, siting behind an assured firewall, and the implementation of good security practice during the installation and operation will ensure the TOE is able to withstand attacks.
A.FIREWALL	The objective (OE.FIREWALL) upholds the assumption as: - an appropriately configured, managed and assured firewall is provided to protect the TOE against network-based attacks
A.PHYSICAL	The objective (OE.PHYSICAL) upholds the assumption as: - appropriate physical safeguards are used to protect the TOE from physical attacks

Assumption Label	Associated Security Objective
A.PLATFORM	The objectives (OE.ADMIN, OE.PLATFORM, OE.ADMIN-AUDIT) uphold the assumption as: - all access control and security management functions are provided by the underlying operating system and will be configured and used securely
A.NO-USER-CODE	The objectives (O.SEPARATION, OE.INSTALL, OE-NO-USER-CODE) uphold the assumption as: - the TOE operates in a separate execution domain and the administrator will ensure that no user code is either introduced or executed on the same platform
A.SYSDATA	The objectives (OE.INSTALL, OE.PLATFORM, OE.ADMIN-AUDIT, OE.ADMIN) uphold the assumption as: - they provide the necessary safeguards to ensure that system-critical data relating to the TOE is sufficiently protected

Table 18 - Sufficiency of Security Objectives (3)

8.2 Security Requirements Rationale

8.2.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are *suitable* to meet the security objectives. The tables below show that each security requirement (and SFR in particular) is *necessary,* that is, each security objective is addressed by at least one security requirement and vice versa. Note that several objectives are partially satisfied by the TOE and partially satisfied by the IT environment. Security Objectives for the TOE are satisfied by Common Criteria functional components. Security Objectives for the Environment are satisfied by IT requirements for the environment.

Objectives	Requirements
O.MESSAGE-AUDIT	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.2, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2, FPT_STM.1
O.NOREPUD	FCO_NRO.1, FCO_NRR.1, FCS_COP.1, FPT_TDC.1, FIA_ATD.1, FPT_STM.1, FTP_ITC.1
O.MESSAGE-INTEGRITY	FCS_COP.1, FDP_UIT.1, FPT_TDC.1, FIA_ATD.1, FTP_ITC.1
O.MESSAGE-CONFIDENTIALITY	FCS_COP.1, FDP_UCT.1, FPT_TDC.1, FIA_ATD.1, FTP_ITC.1
O.INFO-FLOW	FDP_ETC.2, FDP_IFC.2, FDP_IFF.1, FDP_ITC.2, FIA_UAU.1, FIA_UID.2
O.KEY-CONFIDENTIALITY	FCS_CKM.2
O.PRIVACY	FPR_PSE.1
O.BYPASS	FPT_RVM.1
O.SEPARATION	FPT_SEP.1
O.STRONG-CRYPTO	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
O.RESOURCES	FRU_PRS.2, FRU_RSA.1
OE.INSTALL	ENV_NONIT.7
OE.PHYSICAL	ENV_NONIT.2 ENV_NONIT.3
OE.FIREWALL	ENV_NONIT.1
OE.CRYPTOMANAGE	ENV_NONIT.8
OE.TRUST	ENV_NONIT.5
OE.ENTRY-NON-TECHNICAL	ENV_NONIT.4
OE.TRAINING	ENV_NONIT.9
OE.NO-USER-CODE	ENV_NONIT.6
OE.PLATFORM	ENV_NONIT.10 ENV_NONIT.12
OE.I&A	ENV_NONIT.10
OE.ADMIN-AUDIT	ENV_NONIT.11
OE.ADMIN	ENV_NONIT.13, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1

Table 19 - Security Objective to Functional Component Mapping

Component	Component Name	Objective
FAU_ARP.1	Security alarms	O.MESSAGE-AUDIT
FAU_GEN.1	Audit data generation	O.MESSAGE-AUDIT
FAU_GEN.2	User identity association	O.MESSAGE-AUDIT
FAU_SAA.2	Profile based anomaly detection	O.MESSAGE-AUDIT
FAU_SAR.1	Audit review	O.MESSAGE-AUDIT
FAU_SAR.3	Selectable audit review	O.MESSAGE-AUDIT
FAU_SEL.1	Security audit event selection	O.MESSAGE-AUDIT
FAU_STG.2	Guarantees of audit data availability	O.MESSAGE-AUDIT
FCO_NRO.1	Selective proof of origin	O.NOREPUD
FCO_NRR.1	Selective proof of receipt	O.NOREPUD
FCS_CKM.1	Cryptographic key generation	O.STRONG-CRYPTO
FCS_CKM.2	Cryptographic key distribution	O.KEY-CONFIDENTIALITY
FCS_CKM.4	Cryptographic key destruction	O.STRONG-CRYPTO
FCS_COP.1	Cryptographic operation	O.STRONG-CRYPTO O.NOREPUD O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY
FDP_ETC.2	Export of user data with security attributes	O.INFO-FLOW
FDP_IFC.2	Complete information flow control	O.INFO-FLOW
FDP_IFF.1	Simple security attributes	O.INFO-FLOW
FDP_ITC.2	Import of user data with security attributes	O.INFO-FLOW
FDP_UCT.1	Basic data exchange confidentiality	O.MESSAGE-CONFIDENTIALITY
FDP_UIT.1	Data exchange integrity	O.MESSAGE-INTEGRITY
FIA_ATD.1	User attribute definition	O.NOREPUD O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY
FIA_UID.2	Timing of identification	O.INFO-FLOW
FIA_UAU.1	Timing of authentication	O.INFO-FLOW
FMT_MSA.1	Management of security attributes	OE.ADMIN
FMT_MSA.2	Secure security attributes	OE.ADMIN
FMT_MSA.3	Static attribute initialisation	OE.ADMIN
FMT_MTD.1	Management of TSF data	OE.ADMIN
FMT_SMR.1	Security roles	OE.ADMIN
FPR_PSE.1	Pseudonymity	O.PRIVACY
FPT_RVM.1	Non-bypassability of the TOE	O.BYPASS
FPT_SEP.1	TSF domain separation	O.SEPARATE
FPT_STM.1	Reliable time stamps	O.MESSAGE-AUDIT O.NOREPUD
FPT_TDC.1	Inter-TSF basic TSF data consistency	O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY O.NOREPUD
FRU_PRS.2	Full priority of service	O.RESOURCES
FRU_RSA.1	Maximum quotas	O.RESOURCES
FTP_ITC.1	Inter-TSF trusted channel	O.MESSAGE-CONFIDENTIALITY O.MESSAGE-INTEGRITY O.NOREPUD

Table 20 - Mapping of Functional Requirements to Security Objectives

Requirement Label	Requirement Name	Objective
ENV_NONIT.1	MMS Server protected by firewall	OE.FIREWALL
ENV_NONIT.2	MMS Server is to be physically protected	OE.PHYSICAL
ENV_NONIT.3	Access to MMS Server restricted to administrators only	OE.PHYSICAL
ENV_NONIT.4	Protection against non-technical attacks	OE.ENTRY-NON-TECHNICAL
ENV_NONIT.5	MMS Administrators are trusted	OE.TRUST
ENV_NONIT.6	MMS Server has no user-accessible code	OE.NO-USER-CODE
ENV_NONIT.7	MMS Server is installed and configured properly	OE.INSTALL
ENV_NONIT.8	Protection for cryptographic material	OE.CRYPTOMANAGE
ENV_NONIT.9	MMS Administrators are well trained	OE.TRAINING
ENV_NONIT.10	Controlled administrator access to MMS Server	OE.PLATFORM OE.I&A
ENV_NONIT.11	Auditing of MMS Administrator Actions	OE.ADMIN-AUDIT
ENV_NONIT.12	Protection of TSF data and attributes	OE.PLATFORM
ENV_NONIT.13	Facilities to configure the security functions of the TOE	OE.ADMIN

Table 21 - Mapping of Environment Requirements to Security Objectives

8.2.2 Sufficiency of the Security Requirements

The following table shows that each of the SFRs is *sufficient* to satisfy the objective, whether in a principal or supporting role.

Objective	Security Requirements
O.MESSAGE-AUDIT	The objective is satisfied by the SFRs (FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.2, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.2, FPT_STM.1) as: - the class FAU provides components for undertaking the key audit functions of the selection and generation of audit trails, the association of identities with actions, the provision of functionality to review audit records - also included under FAU is functionality to generate alerts based on audited activities, and prevent the loss of audit data - the functionality of FPT_STM.1 ensures that timestamps are available to be associated with the audit records
O.NOREPUD	The objective is satisfied by the SFRs (FCO_NRO.1, FCO_NRR.1, FCS_COP.1, FPT_TDC.1, FIA_ATD.1, FPT_STM.1, FTP_ITC.1) as: - the functionality to selectively ensure non-repudiation of origin and/or receipt of messages is provided by FCO_NRO.1 and FCO_NRR.1 - the cryptographic functionality (digital signatures) to support those non-repudiation functions is provided by FCO_COP.1 and is bound with timestamping provided by FPT_STM.1 - the functions FPT_TDC.1 and FIA_ATD.1 allow for the digital signatures to be associated with messages and correctly interpreted when imported or exported from the TOE to some other IT product - the function FTP_ITC.1 provides the functionality to support non-repudiation when communication occurs between the TOE and another instance of the TOE

Objective	Security Requirements
O.MESSAGE-INTEGRITY	The objective is satisfied by the SFRs (FCS_COP.1, FDP_UIT.1, FPT_TDC.1, FIA_ATD.1, FTP_ITC.1) as: - the function FDP_UIT.1 ensures the integrity of messages exchanged against modification, deletion, insertion and replay - the cryptographic functionality (hashing and digital signatures) is provided by FCS_COP.1 - the functions FPT_TDC.1 and FIA_ATD.1 allow for the hashes and digital signatures to be associated with messages and correctly interpreted when imported or exported from the TOE to some other IT product - the function FTP_ITC.1 provides the functionality to support integrity checking when communication occurs between the TOE and another instance of the TOE
O.MESSAGE-CONFIDENTIALITY	The objective is satisfied by the SFRs (FCS_COP.1, FDP_UCT.1, FPT_TDC.1, FIA_ATD.1, FTP_ITC.1) as: - the function FDP_UCT.1 ensures the confidentiality of messages exchanged against unauthorized access or eavesdropping - the cryptographic functionality (symmetric encryption) is provided by FCS_COP.1 - the functions FPT_TDC.1 and FIA_ATD.1 allow for the encrypted data to be correctly interpreted when imported or exported from the TOE to some other IT product - the function FTP_ITC.1 provides the functionality to support data confidentiality when communication occurs between the TOE and another instance of the TOE
O.INFO-FLOW	The objective is satisfied by the SFRs (FDP_ETC.2, FDP_IFC.2, FDP_IFF.1, FDP_ITC.2, FIA_UAU.1, FIA_UID.2) as: - the information flow control polices relating to the application of security functions, content scanning, access control and archiving are defined and applied by the components FDP_IFC.2 and FDP_IFF.1 - the functions FDP_ETC.2 and FDP_ITC.2 ensure that data exported from and imported to the TOE can be bound with appropriate security attributes - the function FIA_UID.2 ensures that all messages are identified before any actions are performed by the TOE
O.KEY-CONFIDENTIALITY	The objective is satisfied by the SFR (FCS_CKM.2) as: - the function provides the means for securely distributing and handling all cryptographic keys used by the TOE
O.PRIVACY	The objective is satisfied by the SFR (FPR_PSE.1) as: - the function provides the means to protect personal details of users while still allowing for the unique identification of users
O.BYPASS	The objective is satisfied by the SFR (FPT_RVM.1) as: - the function provides for the implementation of the reference monitor concept which ensures that the TSP cannot by bypassed
O.SEPARATION	The objective is satisfied by the SFR (FPT_SEP.1) as: - the function provides for a separate domain of execution for the TOE to prevent interference and tampering
O.STRONG-CRYPTO	The objective is satisfied by the SFRs (FCS_CKM.1, FCS_CKM.4, FCS_COP.1) as: - the cryptographic functions define the use of algorithms and key lengths which will ensure that any cryptographic operations are sufficiently strong as to be protected from both cryptanalytic and brute force attacks
O.RESOURCES	The objective is satisfied by the SFRs (FRU_PRS.2, FRU_RSA.1) as: - the functions provide for the ability to assign priorities of service based on various criteria and also to enforce maximum quotas to prevent resource exhaustion

Objective	Security Requirements
OE.PLATFORM	The objective for the environment is satisfied by the requirements for the non-IT environment (ENV_NONIT.10, ENV_NONIT.12) as: - the functions provide for the restriction of access to the TOE to only authorized administrators and for the underlying operating system to be correctly installed and configured in order to protect any system critical data including cryptographic material, policy configuration data and message archives
OE.I&A	The objective for the environment is satisfied by the requirement for the non-IT environment (ENV_NONIT.10) as: - the function provides controlled administrator access through logical mechanisms provided by the underlying operating system
OE.ADMIN-AUDIT	The objective for the environment is satisfied by the requirements for the non-IT environment (ENV_NONIT.11) as: - the function provides for the auditing of all administrator related actions
OE.ADMIN	The objective for the environment is satisfied by the requirement for the non-IT environment (ENV_NONIT.13) and the SFRs (FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1) as: - the functions provide the facilities to manage the TOE through the definition of roles, the definition and initialisation of security parameters

Table 22 - SFR sufficiency

8.2.3 Satisfaction of Dependencies

The table below shows the dependencies between the functional and assurance requirements. All except one of the dependencies are satisfied. (Note that (H) indicates the dependency is satisfied through the inclusion of a component that is hierarchical to the one required).

Component Reference	Requirement	Dependencies	Dependency Reference
Functional Requirements			
1	FAU_ARP.1	FAU_SAA.1	4 (H)
2	FAU_GEN.1	FPT_STM.1	32
3	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	2, 22(H)
4	FAU_SAA.2	FIA_UID.1	22(H)
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	2, 27
8	FAU_STG.2	FAU_GEN.1	2
9	FCO_NRO.1	FIA_UID.1	22(H)
10	FCO_NRR.1	FIA_UID.1	22(H)
11	FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	14, 13, 25
12	FCS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	11, 13, 25
13	FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	11,25
14	FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	11,13,25
15	FDP_ETC.2	FDP_IFC.1	16 (H)
16	FDP_IFC.2	FDP_IFF.1	17
17	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	16 (H), 26
18	FDP_ITC.2	FDP_IFC.1, FTP_ITC.1, FPT_TDC.1	16 (H), 36, 33
19	FDP_UCT.1	FTP_ITC.1, FDP_IFC.1	36, 16 (H)
20	FDP_UIT.1	FTP_ITC.1, FDP_IFC.1	36, 16 (H)
21	FIA_ATD.1	No dependencies	
22	FIA_UID.2	No dependencies	
23	FIA_UAU.1	FIA_UID.1	22 (H)
24	FMT_MSA.1	FDP_IFC.1, FMT_SMR.1	16 (H), 28
25	FMT_MSA.2	ADV_SPM.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	16 (H), 24, 28
26	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	24, 28
27	FMT_MTD.1	FMT_SMR.1	28
28	FMT_SMR.1	FIA_UID.1	22 (H)
29	FPR_PSE.1	No dependencies	
30	FPT_RVM.1	No dependencies	
31	FPT_SEP.1	No dependencies	
32	FPT_STM.1	No dependencies	
33	FPT_TDC.1	No dependencies	
34	FRU_PRS.2	No dependencies	
35	FRU_RSA.1	No dependencies	
36	FTP_ITC.1	No dependencies	

Component Reference	Requirement	Dependencies	Dependency Reference
Assurance Requirements			
37	ACM_CAP.2	No dependencies	
38	ADO_DEL.1	No dependencies	
39	ADO_IGS.1	AGD_ADM.1	43
40	ADV_FSP.1	ADV_RCR.1	42
41	ADV_HLD.1	ADV_RCR.1	42
42	ADV_RCR.1	No dependencies	
43	AGD_ADM.1	ADV_FSP.1	40
44	AGD_USR.1	ADV_FSP.1	40
45	ATE_COV.1	ADV_FSP.1, ATE_FUN.1	40, 46
46	ATE_FUN.1	No dependencies	
47	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1	40, 43, 44
48	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	40, 41
49	AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	40, 41, 43, 44

Table 23 - Functional and Assurance Requirements Dependencies

The following dependency is not satisfied in this Security Target because it is not considered relevant:

- ADV_SPM.1 is not an EAL2 assurance component and the requirement for this assurance component comes from the functional component FMT_MSA.2 which relates to secure attribute initialization and all security attributes are determined through organizational security policy definitions, therefore this dependency has been omitted.

8.3 TOE Summary Specification Rationale

8.3.1 IT security functions satisfy the SFRs.

The following two tables show that each SFR is mapped to at least one IT security function and each IT security function is mapped to at least one SFR.

Functional Component	Functional Requirement	TSS Reference	IT Security Function
FAU_ARP.1	Security alarms	NOT_VIO	Notification of violations
FAU_GEN.1	Audit data generation	MES_ARC	Message archiving
FAU_GEN.2	User identity association	MES_ARC	Message archiving
FAU_SAA.2	Profile based anomaly detection	MES_ARC NOT_VIO	Message archiving Notification of violations
FAU_SAR.1	Audit review	MES_ARC	Message archiving
FAU_SAR.3	Selectable audit review	MES_ARC	Message archiving
FAU_SEL.1	Security audit event selection	MES_ARC	Message archiving
FAU_STG.2	Guarantees of audit data availability	MES_ARC	Message archiving
FCO_NRO.1	Selective proof of origin	MES_NOR	Message non-repudiation
FCO_NRR.1	Selective proof of receipt	MES_NOR	Message non-repudiation
FCS_CKM.1	Cryptographic key generation	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FCS_CKM.2	Cryptographic key distribution	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FCS_CKM.4	Cryptographic key destruction	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FCS_COP.1	Cryptographic operation	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FDP_ETC.2	Export of user data with security attributes	MES_CON MES_INT MES_NOR INF_CON	Message confidentiality Message integrity Message non-repudiation Information confidentiality
FDP_IFC.2	Complete information flow control	INF_CON INF_INT INF_AVA	Information confidentiality Information and systems integrity Information and systems availability
FDP_IFF.1	Simple security attributes	MES_CON MES_INT MES_NOR INF_CON INF_INT INF_AVA MES_DIS DIS_ANN	Message confidentiality Message integrity Message non-repudiation Information confidentiality Information and systems integrity Information and systems availability Message disclosure Disclaimer/Warning annotation

Functional Component	Functional Requirement	TSS Reference	IT Security Function
FDP_ITC.2	Import of user data with security attributes	MES_CON MES_INT MES_NOR INF_INT INF_AVA	Message confidentiality Message integrity Message non-repudiation Information and systems integrity Information and systems availability
FDP_UCT.1	Basic data exchange confidentiality	MES_CON	Message confidentiality
FDP_UIT.1	Data exchange integrity	MES_INT	Message integrity
FIA_ATD.1	User attribute definition	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FIA_UID.2	Timing of identification	INF_CON INF_INT INF_AVA	Information confidentiality Information and systems integrity Information and systems availability
FIA_UAU.1	Timing of authentication	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FMT_MSA.1	Management of security attributes	SYS_MAN	System security management
FMT_MSA.2	Secure security attributes	SYS_MAN	System security management
FMT_MSA.3	Static attribute initialisation	SYS_MAN	System security management
FMT_MTD.1	Management of TSF data	SYS_MAN	System security management
FMT_SMR.1	Security roles	SYS_MAN	System security management
FPR_PSE.1	Pseudonymity	SEN_PRI	Sender privacy
FPT_RVM.1	Non-bypassability of the TSP	MES_CON MES_INT MES_NOR INF_CON INF_INT INF_AVA	Message confidentiality Message integrity Message non-repudiation Information confidentiality Information and systems integrity Information and systems availability
FPT_SEP.1	TSF domain separation	SYS_MAN	System security management
FPT_STM.1	Reliable time stamps	MES_ARC	Message archiving
FPT_TDC.1	Inter-TSF basic TSF data consistency	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation
FRU_PRS.2	Full priority of service	INF_AVA	Information and systems availability
FRU_RSA.1	Maximum quotas	INF_AVA	Information and systems availability
FTP_ITC.1	Inter-TSF trusted channels	MES_CON MES_INT MES_NOR	Message confidentiality Message integrity Message non-repudiation

Table 24 - Mapping of Functional Requirements to TOE Summary Specifications

The table below shows that all of the IT Security Functions in the TOE Summary Specification (TSS) help meet TOE Security Functional Requirements.

TSS Reference	IT Security Function	Functional Component	Functional Requirement
MES_CON	Message Confidentiality	FCS_CKM.1	Cryptographic key generation
		FCS_CKM.2	Cryptographic key distribution
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1	Cryptographic operation
		FDP_ETC.2	Export of user data with security attributes
		FDP_IFF.1	Simple security attributes
		FDP_ITC.2	Import of user data with security attributes
		FDP_UCT.1	Basic data exchange confidentiality
		FIA_ATD.1	User attribute definition
		FIA_UAU.1	Timing of authentication
		FPT_RVM.1	Non-bypassability of the TSP
		FPT_TDC.1	Inter-TSF basic TSF data consistency
		FTP_ITC.1	Inter-TSF trusted channels
MES_INT	Message Integrity	FCS_CKM.1	Cryptographic key generation
		FCS_CKM.2	Cryptographic key distribution
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1	Cryptographic operation
		FDP_ETC.2	Export of user data with security attributes
		FDP_IFF.1	Simple security attributes
		FDP_ITC.2	Import of user data with security attributes
		FDP_UIT.1	Data exchange integrity
		FIA_ATD.1	User attribute definition
		FIA_UAU.1	Timing of authentication
		FPT_RVM.1	Non-bypassability of the TSP
		FPT_TDC.1	Inter-TSF basic TSF data consistency
		FTP_ITC.1	Inter-TSF trusted channels
MES_NOR	Message Non-repudiation	FCO_NRO.1	Selective proof of origin
		FCO_NRR.1	Selective proof of receipt
		FCS_CKM.1	Cryptographic key generation
		FCS_CKM.2	Cryptographic key distribution
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1	Cryptographic operation
		FDP_ETC.2	Export of user data with security attributes
		FDP_IFF.1	Simple security attributes
		FDP_ITC.2	Import of user data with security attributes
		FIA_ATD.1	User attribute definition
		FIA_UAU.1	Timing of authentication
		FPT_RVM.1	Non-bypassability of the TSP
		FPT_TDC.1	Inter-TSF basic TSF data consistency
		FTP_ITC.1	Inter-TSF trusted channels

TSS Reference	IT Security Function	Functional Component	Functional Requirement
MES_ARC	Message Archiving	FAU_GEN.1 FAU_GEN.2 FAU_SAA.2 FAU_SAR.1 FAU_SAR.3 FAU_SEL.1 FAU_STG.2 FPT_STM.1	Audit data generation User identity generation Profile based anomaly generation Audit review Selectable audit review Security audit event selection Guarantees of audit data availability Reliable time stamps
SEN_PRI	Sender Privacy	FPR_PSE.1	Pseudonymity
INF_CON	Information Confidentiality	FDP_ETC.2 FDP_IFC.2 FDP_IFF.1 FIA_UID.2 FPT_RVM.1	Export of user data with security attributes Complete information flow control Simple security attributes Timing of identification Non-bypassability of the TSP
INF_INT	Information Integrity	FDP_IFC.2 FDP_IFF.1 FDP_ITC.2 FDP_UIT.1 FIA_UID.2 FPT_RVM.1	Complete information flow control Simple security attributes Import of user data with security attributes Data exchange integrity Timing of identification Non-bypassability of the TSP
INF_AVA	Information Availability	FDP_IFC.2 FDP_IFF.1 FDP_ITC.2 FIA_UID.2 FPT_RVM.1 FRU_PRS.2 FRU_RSA.1	Complete information flow control Simple security attributes Import of user data with security attributes Timing of identification Non-bypassability of the TSP Full priority of service Maximum quotas
MES_DIS	Message Disclosure	FDP_IFF.1	Simple security attributes
DIS_ANN	Disclaimer/Warning Annotation	FDP_IFF.1	Simple security attributes
NOT_VIO	Notification of Violations	FAU_ARP.1 FAU_SAA.2	Security alarms Profile based anomaly detection
SYS_MAN	System Security Management	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_MTD.1 FMT_SMR.1 FPT_SEP.1	Management of security attributes Secure security attributes Static attribute initialisation Management of TSF data Security roles TSF domain separation

Table 25 - Mapping of TOE Summary Specifications to Functional Requirements

8.3.2 IT Security Function Suitability

The table below provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

Security Functional Requirement	IT Security Functions
FAU_ARP.1	The TOE SFR is satisfied by the IT Security Function (NOT_VIO) as: - the function provides for the notification to nominated parties, including administrators, of violations of the defined security policies
FAU_GEN.1	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function provides for the configurable archiving of messages based on a defined security policy
FAU_GEN.2	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function provides for the association of identities of both the sender and the recipient of a message with a message archive
FAU_SAA.2	The TOE SFR is satisfied by the IT Security Functions (MES_ARC, NOT_VIO) as: - the functions provide the means to analyse the message archives both manually and automatically and configure alarms to be raised if certain patterns are detected
FAU_SAR.1	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function is provided to review the message archives
FAU_SAR.3	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function is provided to select criteria by which the message archives are reviewed
FAU_SEL.1	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function is provided to configure the parameters used for message archiving in accordance with a defined archive policy
FAU_STG.2	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function is provided to select the location and format of the archive storage to ensure that it is appropriately protected from unauthorised deletion. - the function is provided to ensure that archive sizes are monitored and action can be preempted if quotas are being reached
FCO_NRO.1	The TOE SFR is satisfied by the IT Security Function (MES_NOR) as: - the function is provided to selectively prevent repudiation of the origin of a message

Security Functional Requirement	IT Security Functions
FCO_NRR.1	The TOE SFR is satisfied by the IT Security Function (MES_NOR) as: - the function is provided to selectively prevent repudiation of the receipt of a message
FCS_CKM.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions provide the means to generate both symmetric and asymmetric cryptographic keys as necessary to perform their functions
FCS_CKM.2	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions provide the means to distribute and/or validate both symmetric and asymmetric cryptographic keys as necessary to perform their functions
FCS_CKM.4	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions provide the means to destroy both symmetric and asymmetric cryptographic keys as necessary when either the keys expire or they are no longer required
FCS_COP.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions provide various cryptographic functions including data encryption and decryption, digital signature creation and validation and hashing
FDP_ETC.2	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR, INF_CON) as: - the message-related functions provide the means to associate security attributes with all messages being exported from the TOE - the information-related function will ensure that, based on security attributes, only authorized data is exported, and when that occurs, the security attributes are maintained
FDP_IFC.2	The TOE SFR is satisfied by the IT Security Functions (INF_CON, INF_INT, INF_AVA) as: - these functions implement information flow control policies on all messages entering and exiting an organization
FDP_IFF.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR, INF_CON, INF_INT, INF_AVA, MES_DIS, DIS_ANN) as: - all of these functions use defined security attributes as the basis for the implementation of a number of information flow control security functional policies

Security Functional Requirement	IT Security Functions
FDP_ITC.2	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR, INF_INT, INF_AVA) as: - the message-related functions provide the means to associate security attributes with all messages being imported into the TOE - the information-related functions will ensure that, based on security attributes, only authorized data is imported, and when that occurs, the security attributes are maintained
FDP_UCT.1	The TOE SFR is satisfied by the IT Security Function (MES_CON) as: - the function provides confidentiality for messages
FDP_UIT.1	The TOE SFR is satisfied by the IT Security Function (MES_INT) as: - the function provides for maintenance of the integrity of messages
FIA_ATD.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - these functions provide for the definition of the security attributes used within the various information flow control policies
FIA_UID.2	The TOE SFR is satisfied by the IT Security Functions (INF_CON, INF_INT, INF_AVA) as: - these functions ensure that all messages are identified and then matched against the appropriate information flow control policies prior to being allowed into or out of the organization
FIA_UAU.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - these functions ensure that message-based security is applied only once the sender and recipient have been appropriately authenticated
FMT_MSA.1	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides for the management of the security parameters relating to the configuration of the TOE
FMT_MSA.2	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides for the secure management of the security parameters relating to the configuration of the TOE - the choice of secure parameters is determined by the organisational policies defining the environment for secure operation of the TOE, hence the function provides the ability to set parameters in line with defined policies.

Security Functional Requirement	IT Security Functions
FMT_MSA.3	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides for the secure initialisation of the security parameters relating to the configuration of the TOE - the function also provides the ability to set the value of security parameters in accordance with defined organisational policies and hence override any default values.
FMT_MTD.1	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides the facilities to enable security and configuration related changes to the TOE to be restricted to only authorized administrators
FMT_SMR.1	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides for the maintenance of a restricted security administrators role for management of the TOE
FPR_PSE.1	The TOE SFR is satisfied by the IT Security Function (SEN_PRI) as: - the function provides the means to hide certain personal details of users from possible unauthorized viewing by outsiders thus maintaining the users' privacy
FPT_RVM.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR, INF_CON, INF_INT, INF_AVA) as: - these functions all ensure that every message coming into the TOE (either from within the organization or externally) is evaluated against all of the defined information flow control policies before it can be passed through the TOE - these functions also ensure that any attempt to bring information into or out of the organization will be mediated through the execution of all of the information flow control policies
FPT_SEP.1	The TOE SFR is satisfied by the IT Security Function (SYS_MAN) as: - the function provides for the maintenance of a separate and protected domain for the execution of the TOE
FPT_STM.1	The TOE SFR is satisfied by the IT Security Function (MES_ARC) as: - the function provides a timestamp value which can be associated with the creation of a message archive
FPT_TDC.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions ensure that messages transferred between instances of the TOE will be protected and have their security attributes maintained
FRU_PRS.2	The TOE SFR is satisfied by the IT Security Function (INF_AVA) as: - the function provides for a priority to be assigned to the handling of all messages in accordance with a defined information flow control policy

Security Functional Requirement	IT Security Functions
FRU_RSA.1	The TOE SFR is satisfied by the IT Security Function (INF_AVA) as: - the function provides for limits to be assigned such that messages which exceed those limits can be handled differently to ensure that services can be maintained
FTP_ITC.1	The TOE SFR is satisfied by the IT Security Functions (MES_CON, MES_INT, MES_NOR) as: - the functions provide for the protection of the confidentiality, integrity and non-repudiation of messages exchanged between instances of the TOE

Table 26 - IT Security function / TSF satisfaction

8.3.3 Demonstration of Mutual Support

The dependency analysis and the other analyses provided above demonstrate that the IT security functions work together to satisfy the TSFs, that is, they demonstrate mutual support between function components.

By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

8.3.4 Assurance Security Requirements Rationale

Given the threats and security objectives outlined, it could be assumed that the assurance level of the TOE should be relatively high, however there are a number of factors that mitigate the threats and associated TOE security and assurance requirements. These are:

1. It is intended that the TOE (server function) be sited behind an assured firewall product that would intercept and block a significant number of network attacks at the TCP/IP port level.
2. It is intended that the server host be sited in a physically secure environment that has constraints on the egress of unauthorised individuals.
3. The server host, while running Windows NT, will have no user-executable applications on it other than the TOE and logon access will be restricted to trusted administrators only.
4. Other than for the cryptographic functions that are outside the scope of a CC evaluation, there are no Strength of Function requirements.

Given this situation, it's considered that an EAL-2 level of assurance is entirely appropriate.

8.3.5 Strength of function claims

Consequent upon the factors just outlined the TOE makes no Strength of Function claims.

8.4 Rationale for Extensions

Not applicable.

8.5 PP Claims Rationale

Not applicable.

Appendix A - Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IME	Integrated Messaging Exchange
IT	Information Technology
MMS	Message Management Server
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy