BAE SYSTEMS

BAE Systems Information Technology

Military Message Handling System (MMHS) Filters v1.1.1

Common Criteria Security Target

Version 3.0

April 23, 2006

Prepared by:

CYGNACOM
SOLUTIONS

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3321

Revision History

Version	Date	Description/Author
1.0	July 10, 2003	Submitted to NIAP
2.0	May 24, 2005	Updates based on ADV evidence
3.0	April 23, 2006	Final Submission

Table of Contents

Table of Figures and Tables

1 Introduction

1.1 Identification

TOE Identification: BAE Systems Information Technology Military Message Handling System (MMHS) Filters, v1.1.1

ST Identification: BAE Systems Information Technology Military Message Handling System (MMHS) Filters Security Target

Version Number: Version 3.0

Date: April 23, 2006

ST Author: CygnaCom Solutions, Inc.

Assurance Level: EAL4

Strength of function: SOF Basic.

Registration: <To be filled in upon registration>

Keywords: Guard, Multi-Level Security, MMHS, Message Filter, Security Label, MRSC, MMSL and Security Target

1.2 Security Target Overview

This Security Target (ST) describes the BAE Systems Information Technology Military Message Handling System (MMHS) Filters, developed in response to the Canadian MMHS Request for Proposal (RFP) and General Dynamics Decision Systems MMHS System Design Activities.

The Canadian Department of National Defense (DND) has implemented a messaging system that is a single, multi-level secure system, based on X.400-compliant messages. To pass messages, the DND developed a method to securely connect highly classified computer networks with unclassified computer networks. This multi-level secure system is the Canadian Military Message Handling System (MMHS) Trusted Guard. The MMHS resides at the entrance to secure enclaves. It provides enclave-level security at this boundary by enforcing system and site-specific security policies governing the transfer of electronic messages between workstations within a classified enclave and workstations outside of the classified enclave. Unclassified external mail messaging systems use the Trusted Gateway (TGW) and the Secret external messaging systems use the Multi-Function Gateway (MFGW). Both of these systems, TGW and MFGW, include the MMHS as a gateway subsystem to enforce the security policy decisions related to the release of incoming and outgoing MMHS messages. The Target of Evaluation (TOE) described in this ST is a portion of the MMHS, i.e., six message filters within the MMHS.

1.3 Related Documents

- Common Criteria (CC) Version 2.2 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).
- Common Methodology for Information Security Evaluation (CEM) Version 2.2, January 2004

1.4 Security Target Organization

The main sections of the ST are the TOE Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, PP Claims and Rationale.

Section 2, the TOE Description, provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the ST's evaluation.

The TOE Security Environment in Section 3 describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

a) Assumptions regarding the TOE's intended usage and environment of use

b) Threats relevant to secure TOE operation

c) Organizational security policies with which the TOE must comply

Section 4 contains the security objectives that reflect the stated intent of the ST. The objectives define how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

Section 5 contains the applicable Security Requirements taken from the Common Criteria, with appropriate refinements. The requirements are provided in separate subsections for the TOE and its environment. The IT security requirements are subdivided as follows:

a) TOE Security Functional Requirements

b) TOE Security Assurance Requirements

Section 6 contains the TOE Summary Specification.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

The Rationale in Section 8 presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale is in three main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them. A glossary of acronyms and terms used in the ST is provided in the Appendix.

1.5 Common Criteria Conformance

The TOE is

- Part 2 Conformant with Common Criteria Version 2.2, and,
- Part 3 Conformant with Common Criteria Version 2.2,

The ST has been built with Common Criteria (CC) Version 2.2 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

The ST is conformant with Common Criteria Version 2.2, Part 2, and Part 3 (Evaluation Assurance Level 4).

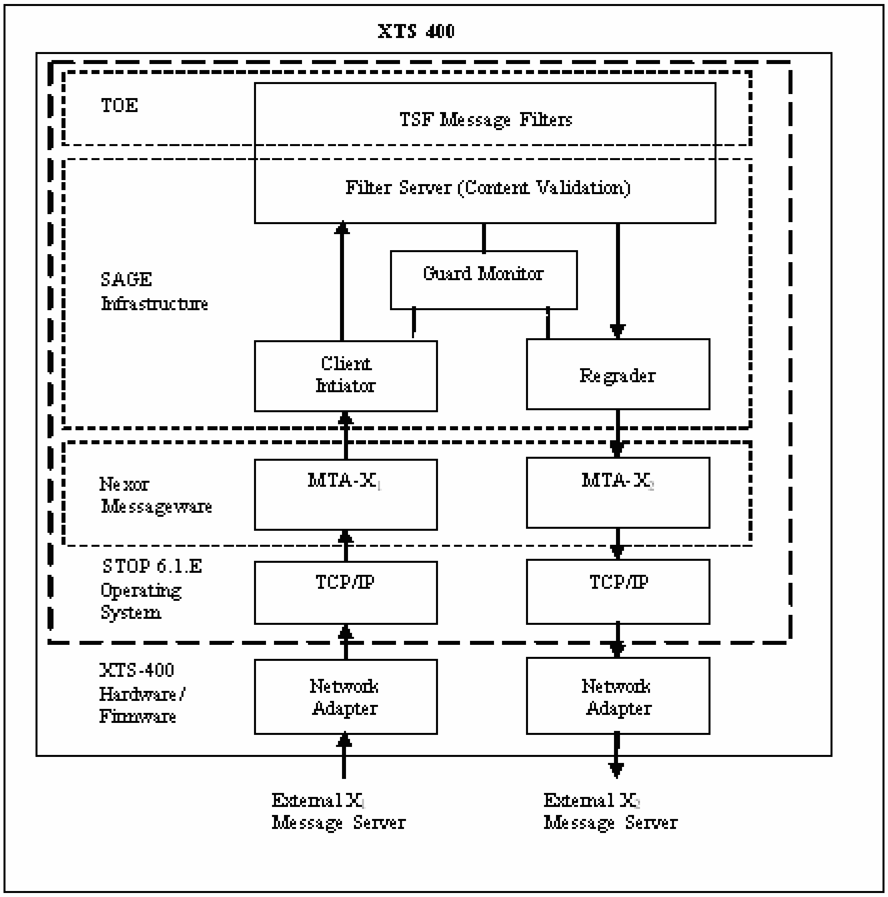
2 TOE Description

2.1 Product Overview

The Canadian Department of National Defense (DND) has implemented a messaging system that is a single, multi-level secure system, based on X.400-compliant messages. To pass messages, the DND developed a method to securely connect highly classified computer networks with unclassified computer networks. This multi-level secure system is the Canadian Military Message Handling System (MMHS) Trusted Guard. The MMHS resides at the entrance to secure enclaves. It provides enclave-level security at this boundary by enforcing system and site-specific security policies governing the transfer of electronic messages between workstations within a classified enclave and workstations outside of the classified enclave. The system is based on the ACP123 Canadian supplement, which governs the origination and reception of military messages. The MMHS interfaces with the Defense Electronic Message System (DEMS) version 2 and external messaging systems (e.g. Automated Defense Data Network (ADDN) and Tactical Message Handling System (TMHS) to form the Defense Message Handling System (DMHS).

Figure 2.1 depicts the MMHS Trusted Guard.

Figure 2.1 - MMHS Trusted Guard



Unclassified external mail messaging systems use the Trusted Gateway (TGW) and the Secret external messaging systems use the Multi-Function Gateway (MFGW). Both of these systems, TGW and MFGW, include the MMHS as a gateway subsystem to enforce the security policy decisions related to the release of incoming and outgoing MMHS messages. The Target of Evaluation (TOE) described in this ST is a portion of the MMHS, i.e., a set of filters within the MMHS.

2.2 TOE Description

The MMHS TOE consists of six filters within the content Validation Server subsystem in MMHS. The TOE and the TSF are identical. User data is considered to be mail messages transiting the TOE and the security attributes of each mail message. There is no TSF data. The six MMHS filters that comprise the TSF are:

1. No Signed Receipts Request Filter
2. Min/Max Filter
3. Message Precedence (Routine or Lower) Filter
4. Valid Message Format Filter
5. Security Label (Protected B or Lower) Filter
6. No Attachment Filter

These six filters support the following security policies within the MMHS guard:

P.MAILONLY – The TOE enforces the P.MAILONLY security policy by not allowing Mail messages to require a signed receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages. The filters that implement this policy are:

- No Signed Receipts Request Filter
- Message Precedence Filter
- Valid Message Format Filter

P.LABELFILTER – The TOE enforces the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B. The filters that implement this policy are:

- Security Label (Protected B or Lower) Filter
- Min/Max Filter

P.MOD_NOATTACHMENT – The TOE enforces the P.MOD_NOATTACHMENT security policy by not allowing Mail messages to have more than one P772 body part. The filter that enforces this policy is:

- No Attachment Filter

The messages flowing through the Canadian Military Message Handling System are X.400/P772 messages, where X.400 is an international standard for message transport and P772 is the content type.

2.3 TSF Boundary and Scope of the Evaluation

The TOE evaluated configuration consists of the TOE running within the MMHS guard application running on the EAL5 certified XTS-400 Trusted Operating System. The TOE and the TSF are identical. The logical boundary of the TOE includes the six filters described above. The physical boundary of the TOE is the software that implements the six filters; the TOE environment is the entire MMHS guard application running on the XTS-400 Trusted Operating System.

2.4 TOE Environment

The IT environment that executes the TSF is an integration of Commercial Off-The-Shelf (COTS) products. These products include the BAE-IT EAL5+ XTS-400 Hardware with the Secure Trusted Operating Program (STOP), the Standard Automated Guard Environment (SAGE), NEXOR Messageware Mailer MTA software and the MMHS guard application. See Figure 2-1, MMHS Trusted Guard below. Additional security services are provided by a collection of Government Off-The-Shelf (GOTS) software libraries. These libraries provide the TOE with a security services architecture. Table 2.1, Security Services Libraries, lists each library and the security services that it provides.

Table 2.1 - Security Services Libraries

No.	Library version	Security Services
1.	S/MIME Freeware Library (SFL)	Implements the IETF S/MIME v3 RFC 3369 Cryptographic Message Syntax (CMS) and RFC 2634 Enhanced Security Services (ESS) specifications. It supports all of the optional ESS security features such as signed receipts, security labels, secure mail list information, and signing certificate attributes. The SFL high-level library makes calls to an algorithm-independent CTIL API. The underlying, external crypto token libraries are not distributed as part of the SFL source code.
2.	Access Control Library (ACL)	Provides an Access Control Decision Function (ACDF) that determines if a subject's authorizations (contained in an X.501 Clearance attribute) allow the subject to access data labeled with specific sensitivity values (included in a security label). The ACL can be used to meet the Partition Rule Based Access Control (PRBAC) processing requirements specified in the "SDN.801 MISSI Access Control Concept and Mechanisms" document. It can process an X.509 Attribute Certificate (AC) or Version 3 X.509 public key certificate to extract the subject's Clearance attribute. It processes security labels formatted according to the "RFC 2634 Enhanced Security Services for S/MIME" specification. Processes multiple Clearance attributes included in a subject's signature or key management v3 X.509 public key certificate to meet the Canadian Department of National Defense (DND) Military Messaging Handling System (MMHS) access control requirements.
3.	Enhanced SNAAC(eSNAAC) Abstract Syntax Notation.1 (ASN.1)	Performs encoding and decoding using Distinguished Encoding Rules (DER)
4.	Certificate Management Library (CML)	The Certificate Management Library (CML) provides certificate processing services as specified in ITU-T Recommendation X.509 (2000). Applications requiring Public Key Infrastructure (PKI) security services can use the CML to meet their X.509 certificate processing requirements. The CML Abstract Syntax Notation.1 (ASN.1) encodes and decodes X.509 Certificates, Certificate Revocation Lists (CRL) and Attribute Certificates. It implements the X.509 certification path verification processing rules. It verifies digital signatures using a variety of commercial and government cryptographic algorithms. The accompanying Storage and Retrieval Library (SRL) optionally provides local certificate and CRL storage management functions.
5.	Storage and Retrieval Library (SRL)	Included with the CML is the optional Storage and Retrieval Library (SRL) which provides local certificate and CRL storage as well as remote directory retrieval capabilities using the Lightweight Directory Access Protocol (LDAP).
6.	Cryptographic Token Interface Libraries (CTIL)	Isolates SFL high level classes from the specifics of the cryptographic token processing. Calls the cryptographic token functions to perform sign & verify, encrypt & decrypt operations.
7.	CygnaCom Certificate Path Development Library (CPDL)	X.509 certificate path building & validation capabilities

3 TOE Security Environment

This section identifies the secure usage assumptions and threats to security. There are no organizational security policies associated with the TOE.

3.1 Secure Usage Assumptions

TOE secure usage assumptions are defined in Table 3.1 below.

Table 3.1 - Secure Usage Assumptions

#	Assumption ID	Assumption Description
1	A.CONFIG	It is assumed that the TOE will be properly configured and maintained as defined in the MMHS Guard guidance documentation.
2	A.OSPROTECT	It is assumed that all filter application files and directories are protected from unauthorised access by the underlying trusted operating system evaluated at Common Criteria Evaluation Assurance Level 5 or higher.
3	A.NO_TOE_BYPASS	It is assumed that the information cannot flow between different domains without passing through the TOE.

3.2 Threats to Security

Threats to the TOE are defined in Table 3.2. The asset under attack is the information transiting the TOE. In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess “average” expertise, few resources, and moderate motivation, or 2) failure of the TOE. Threats to Security are listed in Table 3.2 below.

Table 3.2 - Threats to Security

#	Threat ID	Threat Description
1	T.ATTACHMENT	An application or an attacker may send a message containing an attachment with harmful intent, such as a virus, to compromise the TOE or the message recipient’s resources.
2	T.CLEARANCE_LEVEL	An application or an attacker may attempt to send a message with a higher clearance to a recipient who is only cleared for lower clearance levels, thereby violating the MMHS guard security policy.
3	T.ILLEGAL_FORMAT	An attacker may attempt to include message content that is not authorized by the MMHS guard security policy and parts of the message content may be in the form of a virus or other rogue programs that are intended to compromise the TOE or the message recipient’s resources.
4	T.PRECEDENCE	An application or attacker may attempt to send a message with an inappropriate or unsupported precedence level or to change a message precedence level in order to compromise system security.
5	T.RECEIPT	An application or an attacker may send a message requiring a return receipt and the intended recipient may receive that message and generate such a receipt, thereby compromising security.
6	T.SECURITY_LABEL	An application or attacker may send a message without a security label or with a security label that is not appropriate for the source and destination network, thereby violating the MMHS guard security policy.

4 Security Objectives

The following section describe the objectives for the TOE, the IT environment and the non-IT environment.

The following conventions are used to identify the above described objectives:

- Objectives for the TOE start with ‘O; Example: O.PRECEDENCE
- Objectives for the IT environment start with ‘OE.’; Example: OE.OS
- Objectives for the non-IT environment start with ‘ON.’; Example: ON.CONFIG

4.1 Security Objectives for the TOE

TOE security objectives are defined in Table 4.1.

Table 4.1 - Security Objectives for the TOE

#	Objective ID	Objective Description
1	O.MIN_MAX	The TOE shall check the message recipient clearance against a defined minimum recipient clearance and check the message security label against a maximum security label for the particular type of recipient and if either check fails, shall not allow the message to pass through the TOE.
2	O.NO_ATTACHMENT	The TOE shall not allow mail messages with attachments, i.e., mail messages with more than two body parts where one is the message itself and the other is the message body text, to pass through the TOE.
3	O.NO_RECEIPT	The TOE shall not allow mail messages that require a receipt to pass through the TOE.
4	O.PRECEDENCE	The TOE shall check all messages for message precedence setting values and where such values are found, allow only those messages that have supported precedence levels to pass through the TOE.
5	O.SECURITY_LABEL	The TOE shall check that each message contains a valid security label and that the security label is appropriate for the message source and message destination networks and will allow only those messages with a valid security label and an appropriate security label for the message source and message destination networks to pass through the TOE.
6	O.VALID_FORMAT	The TOE shall allow only properly formatted messages to pass through the TOE.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

Table 4.2 lists security objectives for the IT environment.

Table 4.2 - Security Objectives for the IT Environment

#	Objective ID	Objective Description
1E	OE.OS	The TOE shall be hosted on a trusted operating system evaluated at a Common Criteria EAL5 level or higher, which will protect filter application files and directories are protected from unauthorized access.

4.2.2 Security Objectives for the Non-IT Environment

Table 4.3 lists the security objective for the non-IT environment.

Table 4.3 - Security Objectives for the Non-IT Environment

#	Objective ID	Objective Description
1N	ON.CONFIG	The TOE shall be properly configured and maintained as defined in the MMHS Guard Guidance documents.
2N	ON.NO_TOE_BYPASS	Those responsible for the TOE must ensure that information cannot flow between different domains except through the TOE.

5 IT Security Requirements

This section defines the TOE security functional requirements and assurance requirements. All requirements are from the CC Parts 2 and 3.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, Section 4.4.1.3.2, as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***italicized bold text****.*
- *Refinements* are identified with <u>***italicized bold and underlined text***</u>.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.1 TOE Security Functional Requirements

This section defines the TOE security functional requirements. A list of the requirements is provided in Table 5.1. All SFRs are from CC Part 2; there are no explicitly stated requirements. The full text of the security functional requirements is contained below. Note that all TOE security functional requirements are iterated, as indicated in the text in Table 5.1.

Table 5.1 - TOE Security Functional Requirements

#	SFR Component	Description	Dependencies
1	FDP_IFC.1	Subset information flow control	FDP_IFF.1 Simple security attributes
2	FDP_IFF.1	Simple Security Attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization

The TOE/TSF supports three Information Flow Control Security Function Policies that are included in the MMHS Guard:

P.MAILONLY – The TSF enforces the P.MAILONLY security policy by not allowing Mail messages to require a signed receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages. The filters that implement this policy are:

- No Signed Receipts Request Filter
- Message Precedence Filter
- Valid Message Format Filter

P.LABELFILTER – The TSF enforces the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B. The filters that implement this policy are:

- Security Label (Protected B or Lower) Filter)
- Min/Max Filter

P.MOD_NOATTACHMENT – The TSF enforces the P.MOD_NOATTACHMENT security policy by not allowing Mail messages to have more than one P772 body part. The filter that enforces this policy is:

- No Attachment Filter

5.1.1 User Data Protection (FDP)

FDP_IFC.1-1 Subset information flow control – P.MAILONLY

Hierarchical to: No other components

FDP_IFC.1.1-1 The TSF shall enforce the ***P.MAILONLY information flow control SFP*** on ***Subjects: mail messages; Information: message content and format; Operations: processing of mail messages through the TOE filters by the MMHS Guard***.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1-1 Simple security attributes – P.MAILONLY

Hierarchical to: No other components

FDP_IFF.1.1-1 The TSF shall enforce the ***P.MAILONLY information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content and format; Security attributes of messages: signed receipt requests, message precedence setting, and message format in conformance with ASN.1 format***.

FDP_IFF.1.2-1 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) ***The message must not contain a signed receipt request.***
2) ***The message must contain an allowed message precedence setting or no message precedence setting.***
3) ***The message must be a properly formatted mail message.***

FDP_IFF.1.3-1 The TSF shall enforce ***no additional rules within the P.MAILONLY information flow control SFP.***

FDP_IFF.1.4-1 The TSF shall provide ***no additional SFP capabilities within the P.MAILONLY information flow control SFP.***

FDP_IFF.1.5-1 The TSF shall explicitly authorize an information flow based on the following rules: ***no additional rules within the P.MAILONLY information flow control SFP.***

FDP_IFF.1.6-1 The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P.MAILONLY information flow control SFP.***

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFC.1-2 Subset information flow control – P.LABELFILTER

Hierarchical to: No other components

FDP_IFC.1.1-2 The TSF shall enforce the ***P.LABELFILTER information flow control SFP*** on ***Subjects: mail messages; Information: message content; Operations: processing of mail messages through the TOE filters by the MMHS Guard***.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1-2 Simple security attributes - P.LABELFILTER

Hierarchical to: No other components

FDP_IFF.1.1-2 The TSF shall enforce the ***P.LABELFILTER information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content; Security attributes of messages: Security Label and Recipient Clearance.***

FDP_IFF.1.2-2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) ***The message must contain a valid Security Label.***

2) ***The message Security Label must not exceed the Implied Classification level of the source network interface.***

3) ***The Security Label defined for the message must be allowed to flow from the source network interface to the destination network interface as defined by the Security Policy Information File contained in the IT Environment.***

FDP_IFF.1.3-2 The TSF shall enforce ***no additional rules within the P.LABELFILTER information flow control SFP.***

FDP_IFF.1.4-2 The TSF shall provide ***no additional SFP capabilities within the P.LABELFILTER information flow control SFP***

FDP_IFF.1.5-2 The TSF shall explicitly authorize an information flow based on the following rules: ***no additional rules within the P.LABELFILTER information flow control SFP.***

FDP_IFF.1.6-2 The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P.LABELFILTER information flow control SFP.***

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFC.1-3 Subset information flow control – P.MOD_NOATTACHMENT

Hierarchical to: No other components

FDP_IFC.1.1-3 The TSF shall enforce the ***P.MOD_NOATTACHMENT information flow control SFP*** on ***Subjects: mail messages; Information: message content; Operations: processing of mail messages through the TOE filters by the MMHS Guard***.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1-3 Simple security attributes - P.MOD_NOATTACHMENT

Hierarchical to: No other components

FDP_IFF.1.1-3 The TSF shall enforce the ***P.MOD_NOATTACHMENT information flow control SFP*** based on the following types of subject and information security attributes: ***Subjects: mail messages; Information: message content; Security attributes of messages: Message Body Parts.***

FDP_IFF.1.2-3 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1) ***The message must contain only two body parts as defined by X.400: message itself =1 and message body text = 2.***

FDP_IFF.1.3-3 The TSF shall enforce ***no additional rules within the P.MOD_NOATTACHMENT information flow control SFP.***

FDP_IFF.1.4-3 The TSF shall provide ***no additional SFP capabilities within the P.MOD_NOATTACHMENT information flow control SFP***

FDP_IFF.1.5-3 The TSF shall explicitly authorize an information flow based on the following rules: ***no additional rules within the P.MOD_NOATTACHMENT information flow control SFP.***

FDP_IFF.1.6-3 The TSF shall explicitly deny an information flow based on the following rules: ***no additional rules within the P.MOD_NOATTACHMENT information flow control SFP.***

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

5.2 Strength of Function Requirement

The threat level for the TOE authentication function is assumed to be **SOF-basic**. Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE and for this TOE the environment handles the identification and authentication functionality.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) taken from Part 3 of the Common Criteria with no augmentation. EAL4 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. None of the assurance components is refined. The assurance components are listed in Table 5.2.

Table 5.2 - EAL4 Assurance Requirements

Assurance Class	SAR Component	Description
Configuration Management	ACM_AUT.1	Partial CM Automation
	ACM_CAP.4	Generation Support and Acceptance Procedures
	ACM_SCP.2	Problem Tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of Modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.4 Requirements for the IT Environment

The requirements for the IT Environment are listed in Table 5.3.

Table 5.3 - Requirements for the IT Environment

#	SFR Component	Description	Dependency
3	FIA_UAU.2	User authentication before any action	FIA_UID.1
4	FIA_UID.2	User identification before any action	No dependencies
5	FMT_MSA.1	Management of security attributes	FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles
6	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 Management of security attributes. (In environment) FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
7	FMT_SMF.1	Specification of management functions	No dependencies
8	FMT_SMR.1	Security roles	FIA_UID.1

5.4.1 Identification and Authentication (FIA)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The ***IT environment*** 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

FIA_UID.2: User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

5.4.2 Security Management (FMT)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The ***IT environment*** shall enforce the ***Operating System access control SFP*** to restrict the ability to ***modify*** the security attributes ***filter configuration for the No Signed Receipts Request Filter, the Min/Max Filter, the Message Precedence Filter, the Security Label Filter, and the No Attachment Filter*** to the ***administrator***.

Dependencies: FDP_IFC.1 Subset information flow control, FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The ***IT environment*** shall enforce the **Operating System access control SFP** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The ***IT environment*** shall allow the ***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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The ***IT environment*** shall be capable of performing the following security management functions: ***access control to the TOE filter configuration***.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The ***IT environment*** shall maintain the roles ***administrator***.

FMT_SMR.1.2 T he **IT environment** shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6 TOE Summary Specification

6.1 TOE IT Security Function – Message Filtering

This section defines the security mechanism within the TOE that satisfies the functional requirements defined in Section 5.

There is only one TOE IT Security Function defined; The TOE Security Function is Message Filtering.

The TOE Security Function Message Filtering supports three Information Flow Control Security Function Policies that are included in the MMHS Guard:

P.MAILONLY – The TSF enforces the P.MAILONLY security policy by not allowing Mail messages to require a signed receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages. The filters that implement this policy and that map to FDP_IFF.1-1 and FDP_IFC.1-1 are:

- No Signed Receipts Request Filter
- Message Precedence Filter
- Valid Message Format Filter

P.LABELFILTER – The TSF enforces the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B. The filters that implement this policy and that map to FDP_IFF.1-2 and FDP_IFC.1-2 are:

- Security Label (Protected B or Lower) Filter)
- Min/Max Filter

P.MOD_NOATTACHMENT – The TSF enforces the P.MOD_NOATTACHMENT security policy by not allowing Mail messages to have more than one P772 body part. The filter that implements this policy and that maps to FDP_IFF.1-3 and FDP_IFC.1-3 is:

- No Attachment Filter

Mapping of functionality to functional requirements is included in Section 8 of this ST.

The TOE is a mail message filtering system, which applies the Security Policies, P.MAILONLY, P.LABELFILTER and P.MOD_NOATTACHMENT on the received messages and forwards or rejects the mail message according to the Policy.

In addition, the TOE utilizes a collection of Government Off-The-Shelf (GOTS) software libraries. These software libraries provide the TOE with a security services architecture. See section 2.4, TOE Environment, for a list and description of the libraries utilized by the TOE.

An informative description of each of the filters is provided below:

1. No Signed Receipts Request Filter – The No Signed Receipt Request Filter fails messages that contain a 'signedAttribute – receiptRequest' attribute in any of the inner 'signedData' or 'ML ExpansionHistory' components of a received message. For S/MIMEv3 ESS, the receipt request is carried in the inner signature data, but may also be overridden by a Mail List Agent (MLA) in the Mail List (ML) history. The No Signed Receipts Request filter checks both, making sure that no signed receipt requests are included. The TOE environment provides the No Signed Receipt Request Filter with the received message components and provides functions that parse the components for receipt requests. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters. Note that the MLA is a part of the TOE Environment.

2. Min/Max Filter – The Min/Max Filter performs verification of Recipient Clearance against a defined "Minimum Recipient Clearance" and verification of the Message Security Label against a "Maximum

Security Label” for the particular type of recipient. For the Minimum Recipient clearance verification, the clearance privileges found in the recipient’s certificate, in conjunction with the appropriate security policy, are checked against the “Minimum Recipient Clearance” attribute found in the recipient’s associated Security Domain certificate. For the Maximum Security Label verification, the message security label is checked against a maximum “label”. This maximum label is a clearance privilege attribute that is stored in the clearance privilege attribute of the Security Domain certificate. If this check fails, that means the message label contained a classification and/or categories that were not contained in the maximum “label” (privileges) attribute. The TOE applies the min/max check to the “To be Delivered” Recipients in the destination domain.

The TOE environment provides the Min/Max Filter with the received message components and provides functions that retrieve recipient clearance levels from the associated Domain Certificates. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters.

3. Message Precedence Filter – All P772 messages can be marked with message precedence setting values as defined in ACP123 (P772) CANSUPP No. 1. The Message Precedence Filter parses the message content and retrieves the message heading extensions and determines the selected precedence of each message received. This filter determines the ‘primaryPrecedence’ and ‘copyPrecedence’ values if either/both are contained in the message. Both precedence values are subjected to this precedence test. This filter is skipped for messages that do not include any of the precedence extensions. The precedence levels supported by the TOE are as follows:

- EMERGENCY PRECEDENCE - The EMERGENCY PRECEDENCE (EP) is the highest level of precedence. EP messages will be processed ahead of all other precedence messages. Only the Chief of Defense Staff and certain designated Commanders are authorized to use the EP capability.
- FLASH - The FLASH precedence is reserved for initial enemy contact message or operational combat messages of extreme urgency. Brevity is mandatory.
- IMMEDIATE - The IMMEDIATE precedence is reserved for very urgent messages relating to situations which gravely affect the security of national/Allied forces or populace.
- PRIORITY - The PRIORITY precedence is reserved for messages concerning the conduct of operations in progress and for other important and urgent matters when ROUTINE precedence will not suffice.
- ROUTINE - The ROUTINE precedence is to be used for all types of messages which justify transmission by rapid means but are not of sufficient urgency and importance to require a higher precedence.

The TOE environment provides the Message Precedence Filter with the required received message components. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters.

4. Valid Message Format Filter – The Valid Message Format Filter is the first filter to process the message and it verifies that the message is a properly formatted mail message. Only messages that conform to the ASN.1 standard will be accepted. If the message passes this filter it is passed to the other filters for additional validation. If the message fails this filter it is rejected and not passed to any other filters.

The TOE environment provides the Valid Message Format Filter with the message and provides functions that parse and decode the message. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters.

5. Security Label (Protected B or Lower) Filter – Protected B is the highest security label level allowed. Protected A and Unclassified are the only security label levels lower than Protected B. Messages passing through the TOE are required to contain a security label. The MMHS Guard has an **Implied Classification** level set for each source network interface and destination network interface. The **Allowed Classification** levels are set in the GUI to specify what levels are allowed to pass through each message flow. The Security Policy Information File (SPIF) is a file that contains a list of valid security labels. The Security Label Filter checks the X.400/P772 message for the existence of a security label in the signed portion of the message and will deny all messages passage through the MMHS Trusted Guard that do not contain a security label (i.e., the label is “absent” from the message). If the security label exists in the message, then the filter will verify that the security label in the message is a valid security label. If the security label in the message is a valid security label, then the filter will check to verify that a message containing this security label is allowed to pass from the source network interface to the destination network interface. This check is performed in two ways: 1) The filter verifies that a message containing the security label does not exceed the **Implied Classification** level of the source network interface and 2) the filter verifies that a message containing a security label is allowed to flow from the source network interface to the destination network interface.

The TOE environment provides the Security Label Filter with the received message components and provides functions that retrieve the security label of the message and compare the label to the originator’s label and the implied network levels using the SPIF. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters.

6. No Attachment Filter – The No Attachment Filter checks the maximum number of X.400 body parts allowed in the P772 message, which is set to a value of 2 for the MMHS Guard, and if the number of body parts in the message is greater than two ((message itself = 1 body part), (message body text = 2 body part), (attachment = 3 body part)), then the message is not allowed passage through the MMHS Trusted Guard.

The TOE environment provides the No Attachment Filter with the received message body parts for counting. The body parts are parsed while processing the Valid Format Filter. The TOE environment also provides additional filters and the final delivery or rejection of the message as determined by the filters.

6.2 Assurance Measures

The assurance level selected for the TOE was EAL4 because it is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in the TOEs.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

EAL4 represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

Appropriate assurance measures will be employed to satisfy the security assurance requirements. The evaluation confirms whether the assurance measures are sufficient to satisfy the assurance requirements. The assurance measures consist of the set of evaluation evidence listed in Table 6.1 below. The documents listed in the table are used as to satisfy EAL4 evaluation requirements.

Table 6.1 - Assurance Measures

Assurance Requirement	Evidence
ACM_AUT.1	MMHS CM Plan, version FS04-056-03
ACM_CAP.4	MMHS CM Plan, version FS04-056-03
ACM_SCP.2	MMHS CM Plan, version FS04-056-03
ADO_DEL.2	MMHS CM Plan, version FS04-056-03
ADO_IGS.1	MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06
ADV_FSP.2	Functional Specification Document, version FS04-031-04

Assurance Requirement	Evidence
ADV_HLD.2	High Level Design Document, version FS04-030-03
ADV_IMP.1	MMHS Life Cycle Management document, version FS05-053-00 MMHS Low Level Design document, version FS05-050-02 Functional Specification Document, version FS04-031-04 TOE Source Code
ADV_LLD.1	MMHS Low-level Design, version FS05-050-02
ADV_RCR.1	MMHS Trusted Guard Representation Correspondence Demonstration, version FS04-058-01
ADV_SPM.1	This security target
AGD_ADM.1	MMHS Trusted Guard Trusted Facility Manual, version FS01-211-01 MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06
AGD_USR.1	MMHS Trusted Guard Trusted Facility Manual, version FS01-211-01 MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06
ALC_DVS.1	MMHS CM Plan, version FS04-056-03
ALC_LCD.1	MMHS CM Plan, version FS04-056-03 MMHS Life Cycle Management Document, version FS05-053-02 MMHS Factory Procedures for Trusted Delivery, version FS05-049-00
ALC_TAT.1	MMHS CM Plan, version FS04-056-03 MMHS Life Cycle Management document, version FS05-053-02
ATE_COV.2	MMHS Trusted Guard Test Plan, version FS05-042-02
ATE_DPT.1	MMHS Trusted Guard Test Plan, version FS05-042-02
ATE_FUN.1	MMHS Trusted Guard Test Plan, version FS05-042-02
ATE_IND.2	Evaluation Team Plan for MMHS Trusted Guard Version 1.1.1, Version1.0
AVA_MSU.2	MMHS Trusted Guard Independent Vulnerability Analysis, version FS04-032-02
AVA_SOF.1	This security target
AVA_VLA.2	MMHS Trusted Guard Independent Vulnerability Analysis, version FS04-032-02

7 PP Claims

This Security Target does not claim compliance to any Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

Table 8.1 maps assumptions and threats to objectives, demonstrating that all assumptions and threats are mapped to at least one objective. Table 8.2 maps objectives to threats and assumptions, demonstrating that all objectives are mapped to at least one threat or assumption. A discussion of the rationale for threat mappings is provided below the table.

This section describes each threat and enumerates and discusses the security objectives that counter the threat.

Table 8.1 - Mapping of Assumptions and Threats to Objectives

#	Threat Name	Threat Description	Objective
1	A.CONFIG	It is assumed that the TOE will be properly configured and maintained as defined in the MMHS Guard guidance documentation.	ON.CONFIG
2	A.OSPROTECT	It is assumed that all filter application files and directories are protected from unauthorised access by the underlying trusted operating system evaluated at Common Criteria Evaluation Assurance Level 5 or higher.	OE.OS
3	A.NO_TOE_BYPASS	It is assumed that the information cannot flow between different domains without passing through the TOE.	ON.NO_TOE_BYPASS
1	T.ATTACHMENT	An application or an attacker may send a message containing an attachment with harmful intent, such as a virus, to compromise the TOE or the message recipient's resources.	O.NO_ATTACHMENT
2	T.CLEARANCE_LEVEL	An application or an attacker may attempt to send a message with a higher clearance to a recipient who is only cleared for lower clearance levels, thereby violating the MMHS guard security policy.	O.MIN_MAX
3	T.ILLEGAL_FORMAT	An attacker may attempt to include message content that is not authorized by the MMHS guard security policy and parts of the message content may be in the form of a virus or other rogue programs that are intended to compromise the TOE or the message recipient's resources.	O.VALID_FORMAT
4	T.PRECEDENCE	An application or attacker may attempt to send a message with an inappropriate or unsupported precedence level or to change a message precedence level in order to compromise system security.	O.PRECEDENCE
5	T.RECEIPT	An application or an attacker may send a message requiring a return receipt and the intended recipient may receive that message and generate such a receipt, thereby compromising security.	O.NO_RECEIPT
6	T.SECURITY_LABEL	An application or attacker may send a message without a security label or with a security label that is not appropriate for the source and destination network, thereby violating the MMHS guard security policy.	O.SECURITY_LABEL

A.CONFIG provides the assumption that the TOE will be properly configured and maintained as defined in the MMHS Guard guidance documentation. This assumption is mapped to ON.CONFIG, which states that the TOE shall be properly configured and maintained as defined in the MMHS Guard Guidance documents.

A.OSPROTECT provides the assumption that all filter application files and directories are protected from unauthorised access by the underlying trusted operating system evaluated at Common Criteria Evaluation Assurance Level 5 or higher. This assumption is mapped to OE.OS, which states that the TOE shall be hosted on a trusted operating system evaluated at a Common Criteria EAL5 level or higher, which will protect filter application files and directories are protected from unauthorized access.

A.NO_TOE_BYPASS provides the assumption that information cannot flow between different domains without passing through the TOE. This assumption is mapped to ON.NO_TOE_BYPASS, which states that those responsible for the TOE must ensure that information cannot flow between different domains except through the TOE.

T.ATTACHMENT states that an application or an attacker may send a message containing an attachment with harmful intent, such as a virus, to compromise the TOE or the message recipient's resources. This threat is countered by O.NO_ATTACHMENT, which requires that the TOE not allow mail messages with attachments, i.e., mail messages with more than two body parts where one is the message itself and the other is the message body text, to pass through the TOE.

T.CLEARANCE_LEVEL states that an application or an attacker may attempt to send a message with a higher clearance to a recipient who is only cleared for lower clearance levels, thereby violating the MMHS guard security policy. This threat is countered by O.MIN_MAX, which requires that the TOE check the message recipient clearance against a defined minimum recipient clearance and check the message security label against a maximum security label for the particular type of recipient and if either check fails, shall not allow the message to pass through the TOE.

T.ILLEGAL_FORMAT states that an attacker may attempt to include message content that is not authorized by the MMHS guard security policy and parts of the message content may be in the form of a virus or other rogue programs that are intended to compromise the TOE or the message recipient's resources. This threat is countered by O.VALID_FORMAT, which requires that the TOE only allow properly formatted messages to pass through the TOE.

T.PRECEDENCE states that an application or attacker may attempt to send a message with an inappropriate or unsupported precedence level or to change a message precedence level in order to compromise system security. This threat is countered by O.PRECEDENCE, which requires that the TOE check all messages for message precedence setting values and where such values are found, allow only those messages that have supported precedence levels to pass through the TOE.

T.RECEIPT states that an application or an attacker may send a message requiring a return receipt and the intended recipient may receive that message and generate such a receipt, thereby compromising security. This threat is countered by O.NO_RECEIPT, which requires that the TOE not allow mail messages that require a receipt to pass through the TOE.

T.SECURITY_LABEL states that an application or attacker may send a message without a security label or with a security label that is not appropriate for the source and destination network, thereby violating the MMHS guard security policy. This threat is countered by O.SECURITY_LABEL, which requires that the TOE check that each message contains a valid security label and that the security label is appropriate for the message source and message destination networks and will allow only those messages with a valid security label and an appropriate security label for the message source and message destination networks to pass through the TOE.

All assumptions and threats are mapped to an objective and rationale is provided fore each mapping.

Table 8.2 provides a mapping for the IT security objectives and proves that there are no unmapped IT security objectives for the TOE. Each objective addresses at least one threat or secure usage assumption. The rationale for the mapping is provided above.

Table 8.2 - Mapping Objectives to Threats

#	Objective Name	Objective Description	Threat/Assumption
1	O.MIN_MAX	The TOE shall check the message recipient clearance against a defined minimum recipient clearance and check the message security label against a maximum security label for the particular type of recipient and if either check fails, shall not allow the message to pass through the TOE.	T.CLEARANCE_LEVEL
2	O.NO_ATTACHMENT	The TOE shall not allow mail messages with attachments, i.e., mail messages with more than two body parts where one is the message itself and the other is the message body text, to pass through the TOE.	T.ATTACHMENT
3	O.NO_RECEIPT	The TOE shall not allow mail messages that require a receipt to pass through the TOE.	T.RECEIPT
4	O.PRECEDENCE	The TOE shall check all messages for message precedence setting values and where such values are found, allow only those messages that have supported precedence levels to pass through the TOE.	T.PRECEDENCE
5	O.SECURITY_LABEL	The TOE shall check that each message contains a valid security label and that the security label is appropriate for the message source and message destination networks and will allow only those messages with a valid security label and an appropriate security label for the message source and message destination networks to pass through the TOE.	T.SECURITY_LABEL
6	O.VALID_FORMAT	The TOE shall allow only properly formatted messages to pass through the TOE.	T.ILLEGAL_FORMAT
1E	OE.OS	The TOE shall be hosted on a trusted operating system evaluated at a Common Criteria EAL5 level or higher, which will protect filter application files and directories are protected from unauthorized access.	A.OSPROTECT
1N	ON.CONFIG	The TOE shall be properly configured and maintained as defined in the MMHS Guard Guidance documents.	A.CONFIG
2N	ON.NO_TOE_BYPASS	Those responsible for the TOE must ensure that information cannot flow between different domains except through the TOE.	A.NO_TOE_BYPASS

8.2 Security Requirements Rationale

In this section, the objectives are mapped to the functional requirements and rationale is provided for the selected evaluation assurance level (EAL4) and its components. Note that functional requirements for the TOE map to objectives with an “O.” prefix and functional requirements for the environment map to an “OE.” prefix. Rationale for the mapping is provided below.

8.2.1 Functional Security Requirements Rationale

Table 8.3 maps Security Functional Requirements (SFRs) to the Security Objectives. Table 8.4 maps Security Objectives to SFRs. Rationale for the mapping is provided following the tables.

Table 8.3 - Mapping of Functional Requirements to IT Security Objectives

#	SFR	SFR Component	Objective
1a	FDP_IFC.1-1	Subset information flow control – P.MAILONLY	O.NO_RECEIPT O.PRECEDENCE O.VALID_FORMAT
2a	FDP_IFF.1-1	Simple security attributes – P.MAILONLY	O.NO_RECEIPT O.PRECEDENCE O.VALID_FORMAT
1b	FDP_IFC.1-2	Subset information flow control – P.LABELFILTER	O.SECURITY_LABEL O.MAX_MIN
2b	FDP_IFF.1-2	Simple security attributes – P.MOD_NOATTACHMENT	O.SECURITY_LABEL O.MAX_MIN
1c	FDP_IFC.1-3	Subset information flow control	O.NO_ATTACHMENT
2c	FDP_IFF.1-3	Simple security attributes	O.NO_ATTACHMENT
3	FIA_UAU.2	User authentication before any action	OE.OS
4	FIA_UID.2	User identification before any action	OE.OS
5	FMT_MSA.1	Management of security attributes	OE.OS
6	FMT_MSA.3	Static attribute initialization	OE.OS
7	FMT_SMF.1	Specification of management functions	OE.OS
8	FMT_SMR.1	Security roles	OE.OS

Table 8.4 - Mapping of Objectives to Functional Requirements

#	Objective	Objective Description	SFR
1	O.MIN_MAX	The TOE shall check the message recipient clearance against a defined minimum recipient clearance and check the message security label against a maximum security label for the particular type of recipient and if either check fails, shall not allow the message to pass through the TOE.	FDP_IFC.1-2 FDP_IFF.1-2
2	O.NO_ATTACHMENT	The TOE shall not allow mail messages with attachments, i.e., mail messages with more than two body parts where one is the message itself and the other is the message body text, to pass through the TOE.	FDP_IFC.1-3 FDP_IFF.1-3
3	O.NO_RECEIPT	The TOE shall not allow mail messages that require a receipt to pass through the TOE.	FDP_IFC.1-1 FDP_IFF.1-1
4	O.PRECEDENCE	The TOE shall check all messages for message precedence setting values and where such values are found, allow only those messages that have supported precedence levels to pass through the TOE.	FDP_IFC.1-1 FDP_IFF.1-1

#	Objective	Objective Description	SFR
5	O.SECURITY_LABEL	The TOE shall check that each message contains a valid security label and that the security label is appropriate for the message source and message destination networks and will allow only those messages with a valid security label and an appropriate security label for the message source and message destination networks to pass through the TOE.	FDP_IFC.1-2 FDP_IFF.1-2
6	O.VALID_FORMAT	The TOE shall allow only properly formatted messages to pass through the TOE.	FDP_IFC.1-1 FDP_IFF.1-1
1E	OE.OS	The TOE shall be hosted on a trusted operating system evaluated at a Common Criteria EAL5 level or higher, which will protect filter application files and directories are protected from unauthorized access.	FIA_UAU.2 FIA_UID.2 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1
1N	ON.CONFIG	The TOE shall be properly configured and maintained as defined in the MMHS Guard Guidance documents.	AGD_ADM.1 AGD_USR.1
2N	ON.NO_TOE_BYPASS	Those responsible for the TOE must ensure that information cannot flow between different domains except through the TOE.	AGD_ADM.1

O.MIN_MAX states that the TOE shall check the message recipient clearance against a defined minimum recipient clearance and check the message security label against a maximum security label for the particular type of recipient and if either check fails, shall not allow the message to pass through the TOE. This objective is mapped to FDP_IFC.1-2 and FDP_IFF.1-2, which provide requirements that enforce the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B.

O.NO_ATTACHMENT states that the TOE shall not allow mail messages with attachments, i.e., mail messages with more than two body parts where one is the message itself and the other is the message body text, to pass through the TOE. This objective is mapped to FDP_IFC.1-3 and FDP_IFF.1-3, which provide requirements that enforce the P.MOD_NOATTACHMENT security policy by not allowing Mail messages to have more than one P772 body part

O.NO_RECEIPT states that the TOE shall not allow mail messages that require a receipt to pass through the TOE. This objective is mapped to FDP_IFC.1-1 and FDP_IFF.1-1, which provide requirements that enforce the P.MAILONLY security policy by not allowing Mail messages to require a receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages.

O.PRECEDENCE states that the TOE shall check all messages for message precedence setting values and where such values are found, allow only those messages that have supported precedence levels to pass through the TOE. This objective is mapped to FDP_IFC.1-1 and FDP_IFF.1-1, which provide requirements that enforce the P.MAILONLY security policy by not allowing Mail messages to require a receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages.

O.SECURITY_LABEL states that the TOE shall check that each message contains a valid security label and that the security label is appropriate for the message source and message destination networks and will allow only those messages with a valid security label and an appropriate security label for the message source and message destination networks to pass through the TOE. This objective is mapped to FDP_IFC.1-2 and FDP_IFF.1-2, which provide requirements that enforce the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B

O.VALID_FORMAT states that the TOE shall allow only properly formatted messages to pass through the TOE. This objective is mapped to FDP_IFC.1-1 and FDP_IFF.1-1, which provide requirements that enforce the P.MAILONLY security policy by not allowing Mail messages to require a receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages.

OE.OS states that the TOE shall be hosted on a trusted operating system evaluated at a Common Criteria EAL5 level or higher, which will protect filter application files and directories are protected from unauthorized access. This objective is mapped to FIA_UAU.2, FIA_UID.2, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, all of which are capabilities included in a trusted operating system.

ON.CONFIG states that the TOE shall be properly configured and maintained as defined in the MMHS Guard Guidance documents. This objective is mapped to the AGD_ADM.1 and AGD_USR.1 assurance requirements, which require administrator and user guidance that defines configuration and maintenance of the TOE.

ON.NO_TOE_BYPASS states that those responsible for the TOE must ensure that information cannot flow between different domains except through the TOE. This objective is mapped to the AGD_ADM.1 assurance requirement, which requires administrator guidance that defines configuration and maintenance of the TOE.

8.2.2 Dependency Rationale

Table 8.5 Lists the Functional Requirements and their dependencies. Note that dependencies to assurance requirements show a reference of "Assurance" and that these requirements are included in the assurance requirements for the TOE.

Table 8.5 - Functional Requirements Dependencies

#	Requirement	Component	Dependencies	Reference
1	FDP_IFC.1	Subset information flow control	FDP_IFF.1 Simple security attributes	2
2	FDP_IFF.1	Simple Security Attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	1 6
3	FIA_UAU.2	User authentication before any action	FIA_UID.1 (met by FIA_UID.2, which is hierarchical to FIA_UID.1)	4
4	FIA_UID.2	User identification before any action	No dependencies	N/A
5	FMT_MSA.1	Management of security attributes	FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles	1 8
6	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 Management of security attributes. (In environment) FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles	5 7 8
7	FMT_SMF.1	Specification of management functions	No dependencies	N/A
8	FMT_SMR.1	Security roles	FIA_UID.1 (met by FIA_UID.2, which is hierarchical to FIA_UID.1)	4

8.2.3 Rationale that TOE SFRs are Internally Consistent and Mutually Supportive

The main security service provided by the MMHS filters is the filtering of mail messages to support the three Information Flow Control Security Function Policies:

- **P.MAILONLY** – The TSF enforces the P.MAILONLY security policy by not allowing Mail messages to require a receipt, allowing only routine or lower priority messages, and only allowing properly formatted mail messages.
- **P.LABELFILTER** – The TSF enforces the P.LABELFILTER security policy by only allowing Mail messages marked at one of the security levels Unclassified, Protected A, or Protected B.

- **P.MOD_NOATTACHMENT** – The TSF enforces the P.MOD_NOATTACHMENT security policy by not allowing Mail messages to have more than one P772 body part.

The TOE SFRs consist of two functional requirements, FDP_IFC.1 and FDP_IFF.1, which together perform user information flow control, in this case, for mail messages. The two functional requirements are each iterated three times: once for each of the Information Flow Control Security Function Policies. The requirements and policies do not overlap and are mutually supportive.

8.3 TOE Summary Specification Rationale

The text below shows that all of the IT Security Functions in the TOE Summary Specification (TSS) are necessary. Explanation and rationale for the mappings are provided in Sections 6.1 and 6.2 and are repeated in Sections 8.3.1 and 8.3.2. There is only one IT Security Function: Message Filtering. The two functional requirements for the TOE, FDP_IFC.1 and FDP_IFF.1 are iterated three times each to support three Information Flow Control Security Function Policies for message filtering.

8.3.1 Strength of Function Rationale

As stated in Section 5.2, the threat level for the TOE authentication function is assumed to be SOF-basic. Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. There are no probabilistic or permutational mechanisms and, therefore, a SOF analysis is not applicable to the TOE.

8.3.2 Assurance Measures Rationale

The assurance measures rationale shows how all assurance requirements were satisfied. The rationale is provided in Table 8.6.

EAL 4 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. EAL 4 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

Table 8.6 - Assurance Measures Rationale

Assurance Requirement	Evidence	Rationale
ACM_AUT.1	MMHS CM Plan, version FS04-056-03	This evidence describes the automated functionality in the configuration management system that is used to develop the TOE and how it is used in the CM system.
ACM_CAP.4	MMHS CM Plan, version FS04-056-03	The CM Plan identifies the method used to uniquely identify each Configuration Item (CI), provides evidence that all CIs have been and are under control of the CM system, and shows that only authorized changes can be made to CIs. It meets all requirements of ACM_CAP.4.

Assurance Requirement	Evidence	Rationale
ACM_SCP.2	MMHS CM Plan, version FS04-056-03	The CM Plan shows how the CM system tracks the TOE implementation representation (software, firmware, and hardware description), design documentation, user and administrator guidance documentation, test and test software documentation, and the CM system documentation. It also describes how reported security flaws are tracked through the system.
ADO_DEL.2	MMHS CM Plan, version FS04-056-03	The CM Plan describes the delivery and distribution procedures to assure that the security of the TOE is maintained during the distribution of the TOE to users.
ADO_IGS.1	MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06	Provides detailed instructions on how to install the TOE.
ADV_FSP.2	Functional Specification Document, version FS04-031-04	This document describes the security functions of the TOE and the externally visible interfaces. It also includes rationale that the TSF is completely represented.
ADV_HLD.2	High Level Design Document, version FS04-030-03	This document describes the TSF in terms of subsystem and fully describes the TSF external interfaces.
ADV_IMP.1	MMHS Life Cycle Management document, version FS05-053-00 MMHS Low Level Design document, version FS05-050-02 Functional Specification Document, version FS04-031-04 TOE Source Code	Developer provided implementation representation
ADV_LLD.1	MMHS Low-level Design, version FS05-050-02	Low level design description of TSF modules and their interrelationships and interfaces.
ADV_RCR.1	MMHS Trusted Guard Representation Correspondence Demonstration, version FS04-058-01	Maps the security target security functions, the functional specification, high level design, low level design, and implementation representation.
ADV_SPM.1	This security target	The ST describes the security policies implemented by the TOE, including subjects, information, and operations.
AGD_ADM.1	MMHS Trusted Guard Trusted Facility Manual, version FS01-211-01 MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06	Describes how to administer the TOE securely.
AGD_USR.1	MMHS Trusted Guard Trusted Facility Manual, version FS01-211-01 MMHS Trusted Guard Version 1.1.1 Installation Guide FS02-011-06	Describes the secure use of the TOE.
ALC_DVS.1	MMHS CM Plan, version FS04-056-03	Provides physical, procedural, personnel and other development security measures necessary to protect the confidentiality and integrity of the TOE design.

Assurance Requirement	Evidence	Rationale
ALC_LCD.1	MMHS CM Plan, version FS04-056-03 MMHS Life Cycle Management Document, version FS05-053-02 MMHS Factory Procedures for Trusted Delivery, version FS05-049-00	Describes the life cycle model and its' definitions
ALC_TAT.1	MMHS CM Plan, version FS04-056-03 MMHS Life Cycle Management document, version FS05-053-02	Provides a detailed definition of all development tools
ATE_COV.2	MMHS Trusted Guard Test Plan, version FS05-042-02	The Test Plan demonstrates the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification document.
ATE_DPT.1	MMHS Trusted Guard Test Plan, version FS05-042-02	Provides a description of testing at TSF subsystem level by the TOE developer.
ATE_FUN.1	MMHS Trusted Guard Test Plan, version FS05-042-02	Documents the testing performed by the TOE developer and demonstrates that all security functions perform as specified. Includes test plans and procedures and expected and actual results.
ATE_IND.2	Evaluation Team Plan for MMHS Trusted Guard Version 1.1.1, Version1.0	Documents independent test, demonstrates that the security functions perform as specified.
AVA_MSU.2	MMHS Trusted Guard Independent Vulnerability Analysis, version FS04-032-02	Ensures that there is no misleading, unreasonable and conflicting guidance is absent from the guidance documentation and that secure procedures for all modes of operation were addressed.
AVA_SOF.1	This security target	Provides a rationale that any mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.2	MMHS Trusted Guard Independent Vulnerability Analysis, version FS04-032-02	Ascertains the presence of security vulnerabilities if any, and confirms that they can not be exploited in the intended environment for the TOE.

Appendix – Acronyms

Acronym	Definition
ACL	Access Control Library
ADDN	Automated Defense Data Network
ASN.1	Abstract Syntax Notation.1
CC	Common Criteria
CEM	Common Methodology for Information Security Evaluation
CML	Certificate Management Library
COTS	Commercial Off-the-Shelf
CPDL	CygnaCom Certificate Path Development Library
CTIL	Cryptographic Token Interface Libraries
DEMS	Defense Electronic Message System
DMHS	Defense Message Handling System
EAL	Evaluation Assurance Level
IP	Internet Control Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFGW	Multi-Function Gateway
MLA	Mail List Agent
MMHS	Military Message Handling System
MTA	Message Transfer Agents
PP	Protection Profile
SAGE	Secure Automated Guard Environment
SF	Security Function
SFL	S/MIME Freeware Library
SFP	Security Function Policy
SOF	Strength of Function
SRL	Storage and Retrieval Library
ST	Security Target
STOP	Secure Trusted Operating Program
TCP	Transmission Control Protocol
TGW	Trusted Gateway
TMHS	Tactical Message Handling System
TOE	Target of Evaluation
TSF	TOE Security Function