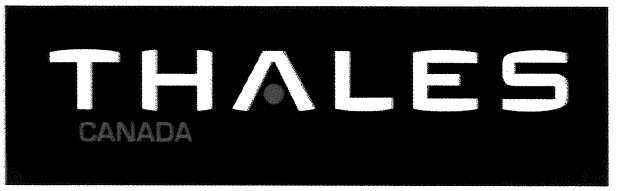
MESSAGE HANDLING SYSTEM

SECURITY TARGET DOCUMENT

16 April 2004

Document Control No: **1165C.011-ST REV. 07**



MESSAGE HANDLING SYSTEM (MHS)

SECURITY TARGET DOCUMENT

Contact Info:

Thales Systems Canada
a Division of Thales Canada Inc.
49 Auriga Drive
Ottawa, Ontario, K2E 8A1
Phone: (613) 723-7000
Fax: (613) 723-5600

Prepared by:

Mark Wilson
Software Team Leader

Approved by:

Brad Watters
Project Manager

REVISION CONTROL SHEET

Rev. #	Pages Affected	Description	By	Date of Issue
1.1	All	Completion of draft revisions on all sections.	William Sandberg-Maitland	04 Oct 2002
02	All	Implemented changes requested by CSE.	William Sandberg-Maitland	27 Mar 2003
03	All	Implemented changes requested by Domus's OR-1 Document (DCD Ref # 03-04419), OR-4 Document (DCD Ref # 03-04902, 03-05075)	Mark Wilson	16 Sep 2003
04	All	Implemented changes requested by Domus's OR-5 Document (DCD Ref # 03-05332)	Mark Wilson	06 Oct 2003
05	All	Changes as a result of working on Domus's OR-7 Document (DCD Ref # 03-06445), FPT_STM.1 is now a SFR of the IT Environment and minor updates.	Mark Wilson	10 Dec 2003
06	All	Implemented changes requested by Domus's OR-11 Document (DCD Ref # 04-00900, 04-01130, 04-01131).	Mark Wilson	25 Feb 2004
07	All	Added registry number.	Mark Wilson	16 April 2004

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

LIST OF ACRONYMS AND ABBREVIATIONS

ACP	Allied Communication Publication
CC	Common Criteria
CCCS	Canadian Common Criteria Scheme
CEM	Common Methodology for Information Technology Security (CEM-99/045)
CO	Commanding Officer
COTS	Commercial-Off-The-Shelf
EAL	Evaluation Assurance Level
LAN	Local Area Network
IT	Information Technology
MCDV	Maritime Coastal Defence Vessel
MHS	Message Handling System
NATO	North Atlantic Treaty Organization
PC	Personal Computer
PP	Protection Profile
RATT	Radio Teletype
SARs	Security Assurance Requirements
SFP	Security Functional Policy
SFRs	Security Functional Requirements
ST	Security Target
TBD	To Be Determined
TCP/IP	Transfer Control Protocol/Internet Protocol
Thales Systems	Thales Systems Canada
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

MHS SECURITY TARGET DOCUMENT

1 INTRODUCTION

1.1 Identification

Title:	Thales Message Handling System Security Target
Version:	Version 3.0
Level of Assurance:	EAL3
TOE Software Identification:	MHS Server, Version 5.1; and MHS Client, Version 1.0.
Registration:	383-4-19
Keywords:	Message Handling System, Conditional Access

1.2 Overview of Document

Thales Systems Canada's (Thales Systems') Message Handling System (MHS) is an application which prepares, transmits, receives, and distributes radio teletype messages in accordance with military organizational requirements and security policy. The MHS is designed for use in high-assurance military networks that support the Allied Communication Publication (ACP) 127 message format. The MHS provides the user with the ability to modify, store, distribute, send, and receive messages over tactical communications channels in the communication system. It supports message drafting, review, and release operations for outgoing messages and secure delivery of incoming messages.

The MHS is the target of evaluation (TOE) of this Security Target (ST) document. Its security-relevant characteristics are described in the Description below (Section 2), as is the boundary of this evaluation.

The Common Criteria (CC) Evaluation Assurance Level 3 evaluation documented herein describes assumptions, threats, security objectives that pertain to the product in its normal use and presents findings that establish its functional security properties at that level. This documentation is presented in Sections 2 to 6. Section 7 presents the rationale that the evaluation criteria

presented is consistent and complete, and that the functional and assurance requirements cited are fulfilled by the TOE.

1.3 CC Conformance Claim

The Thales Systems' MHS is conformant to Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, August 1999, Version 2.1, CCIMB-99-032 and Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, August 1999, Version 2.1, CCIMB-99-033.

The MHS is being evaluated to Evaluation Assurance Level 3 under the Canadian Common Criteria Scheme (CCCS) of the Common Criteria Standard Version 2.1.

1.4 Relation to Protection Profiles

This ST does not claim conformance to a specific CC protection profile (PP).

1.5 Trademark Information

Microsoft, Windows, are either registered trademarks or trademarks of Microsoft Corporation. Jaz is a registered trademark or trademark of Iomega Corporation in the United States and/or other countries. Pentium and the Pentium processor logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. InterBase and Borland are trademarks or registered trademarks of Borland Software Corporation. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Norton AntiVirus is a registered trademark of Symantec Corporation in the United States and other countries. All other trademarks or registered trademarks are the property of their respective owners.

2 TOE DESCRIPTION

2.1 Overview

Thales Systems' MHS is a multi-user, network based, Commercial-Off-The-Shelf (COTS), configurable application which prepares, transmits, receives, and distributes radio teletype messages. The system provides the user with the ability to create, modify, store, distribute, send, and receive messages simultaneously over all channels in the communication system.

The MHS was originally developed for the Canadian Navy's Maritime Coastal Defence Vessel (MCDV) and still serves that class of 12 ships today. Subsequently upgraded to run under WindowsNT and with a new Java client, the MHS product has been procured by other navies and is currently being offered around the world as the MHS product of choice for all Thales communications systems. It is being considered for use in various naval, maritime, and airborne communications systems.

The MHS is a mail handling system based on the ACP 127 message format, a radio teletype standard. This message protocol is widely used in naval systems, thus ensuring a broad applicability for the MHS. In particular, the MHS does not support industry-standard email protocols, and has a distinct security mode of operation that applies well to military organizational and communications requirements.

The MHS provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks to violate system security, particularly from within the physical zone or domain of deployment. No mechanism to address malicious system development or administrative personnel is claimed. The MHS is designed to be suitable for use in well-protected military environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

Due to the extensive deployment of MHS in naval applications, the terms 'ship' and 'off-ship' are used in this ST to denote the physically isolated and protected environment in which the MHS is installed, and those environments external to it. The MHS may be deployed in any environment satisfying adequate physical, procedural and communications security requirements.

2.2 Detailed Description

2.2.1 Software Components

The TOE consists of the following distributed software components:

- MHS Server, Version 5.1; and
- MHS Client, Version 1.0.

2.2.2 Logical Interfaces

The logical interfaces with which the TOE interacts to obtain data, control information or deliver data are as follows:

Table 2-1: Logical Interfaces

Logical Interface	MHS Component(s)	Characteristics
User Interface	MHS Client	A Windows NT application on the User PC terminal allowing control of TOE functions and input, modification and display of messages.
LAN Interface	MHS Client, MHS Server	An ethernet Transfer Control Protocol/Internet Protocol (TCP/IP) communications interface used to communicate all control information and data between the two distributed components of the TOE.
Printer Interface	MHS Client, MHS Server	The LAN interface connects the TOE components to the Printer entity, for user printing services.
RATT Communications Interface	MHS Server	A cryptographic and communications interface that accepts plain (unencrypted) text radio teletype (RATT) message transmissions for subsequent encryption and transmission on a designated circuit, and delivers plain text ACP 127 messages originating from external sources.

2.2.3 Architecture

The basic system layout of a TOE deployment is formed around an Ethernet LAN, which interconnects all message terminals to the central server. The server interfaces with the external connection lines and radios through serial connections to cryptographic equipment. It provides central printing services for the network and provides paper tape input/output facilities for off-line cryptographic purposes. The message terminals are located in the various ship offices, all connected by a network.

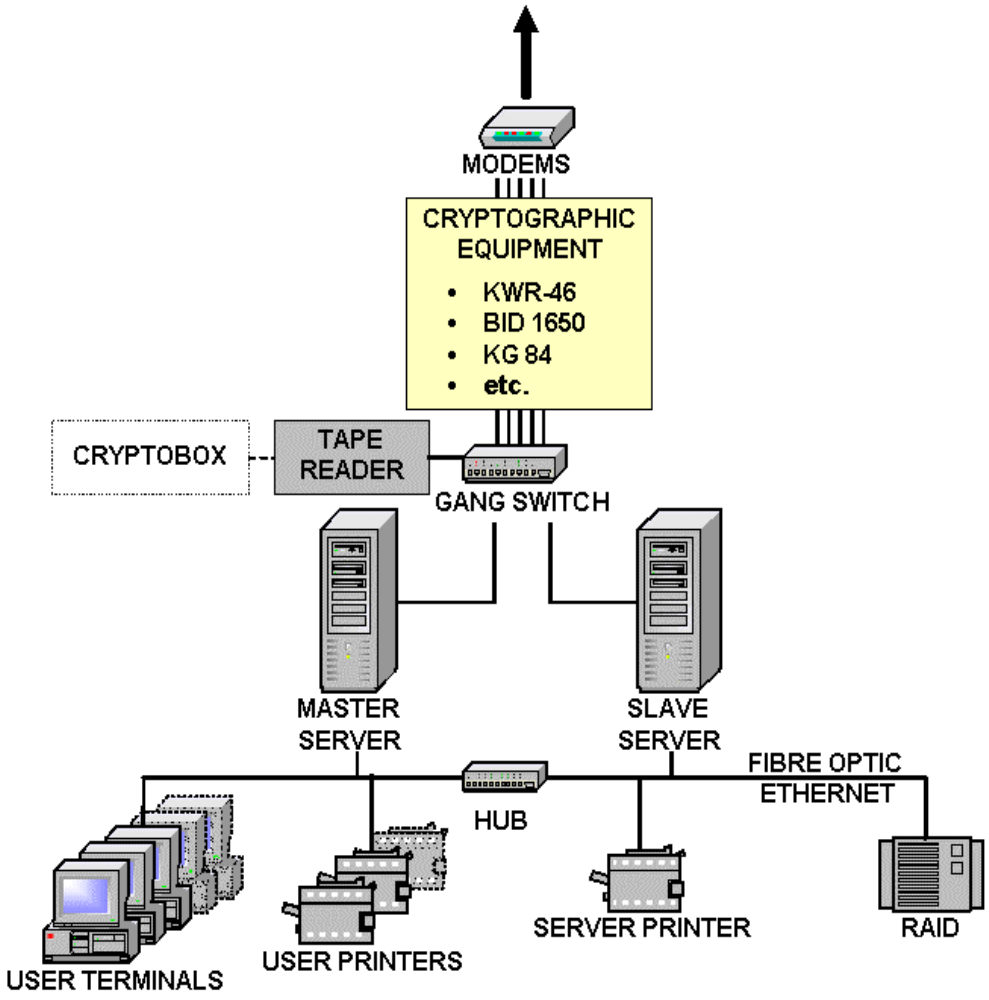


Figure 2-1: Network Environment of Thales MHS

Figure 2-1 shows the network environment in which the MHS operates. The master server and slave server are the platforms on which the MHS Server component of the TOE is installed. The user terminals are platforms for the MHS Client component of the TOE. The network consisting of the hub and fibre optic ethernet provides connectivity between the client and server installed components. The gang switch provides connectivity to the cryptographic units and external communications circuits.

A logical deployment architecture is shown in Figure 2-2 on the next page. This view shows the logical software components of the MHS and the network entities that it interacts with.

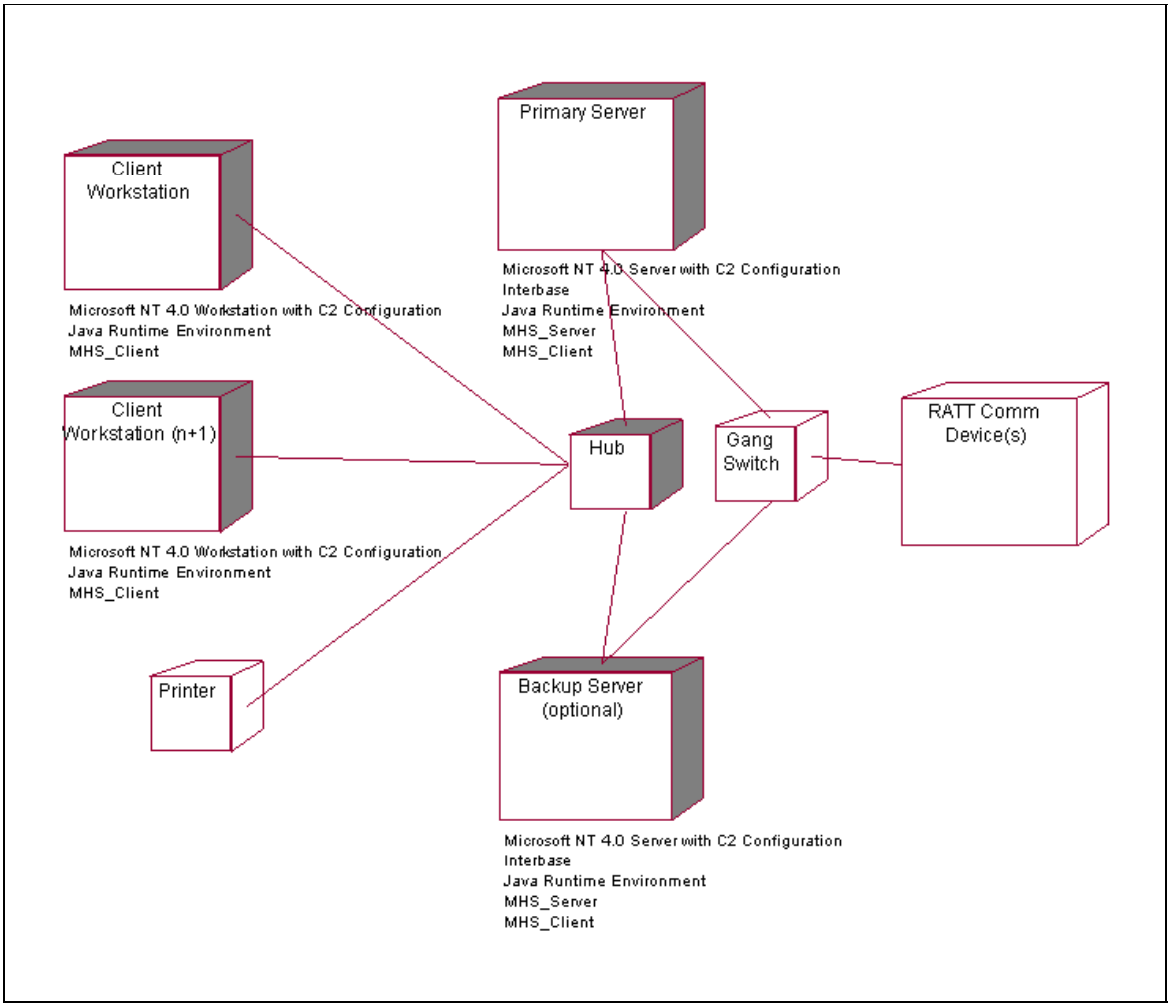


Figure 2-2: Logical View of MHS Environment

2.2.4 Security Functions and Services

The TOE security services under evaluation are:

- Enforcement of the MHS Discretionary Access Control Policy for all outgoing and incoming messages; and
- Audit of specified security events.

2.2.5 Security Role Types

The following role types are supported by the TOE:

- Administrator;
- Supervisor; and

- User.

Each of the role types has specific responsibilities and privileges in the system. These are described below:

Table 2-2: Security Role Types

Role Types	Responsibility	Privileges
Administrator	Administers system accounts for users.	Has no access to message objects. Creates user accounts; sets user clearance and distribution attributes; revokes accounts.
Supervisor	Sends all messages that have been released by users by adding to send queues.	Has read, write, delete privileges to all outgoing messages. Performs export of outgoing message objects.
User	May draft a message, review a message and release a message for transmission.	Has read, write, delete privileges to all outgoing messages owned by user. May or may not have release clearance for an outgoing message. Has read privilege to all incoming messages that have a classification that does not exceed the clearance of the user.

2.2.6 TOE Information Model

The following information model is included as a reference for certain security functional and TSP statements in the ST, especially Section 5.1.2. The purpose of the model is to provide greater descriptive accuracy in dealing with the CC concepts of user data, TSF data and security attributes of information objects. The information model for the TOE is partitioned into two main classes:

- Local Data, consisting of the following two subclasses:
  - User Data; and
  - TSF Data.
- External Data.

Non-local Data is considered to be a synonym for External Data. This includes outgoing messages after transmission and incoming messages before reception. There are no other explicit data objects that belong to this class, as its scope of control lies outside the TOE boundary. However there is a single subclass of subjects called user, which represents the TOE environment community of users. The user subject class has the following attributes:

Table 2-3: User Subject Attributes

User Subject Attribute	Description
name	The system identity of the user subject.
role_type	Denotes the current role type under which the User instance is operating. The Role attribute may have values 'ADMINISTRATOR', 'SUPERVISOR' or 'USER' only, denoting the system role of the user.
password	The password of the user.
read_clearance	The highest classification of message that the user may have read access (see message.classification for values, also called levels).
release_clearance	The highest classification of message that the user may release for transmission (see message.classification for values, also called levels).
boss	The immediate user to whom the human user in question reports in the management hierarchy. Define the *Boss Hierarchy* of a user to be the ordered set resulting from the concatenation of user's boss and the boss hierarchy of the user's boss. The boss hierarchy of the commanding officer (CO) is the empty set.

The derived attribute user.access_privilege is determined functionally from user.role_type, user.read_clearance and user.release_clearance by the TSF within the constraints of the TOE security policy described in the next section. The set of values of user.access_privilege are {READ, WRITE, DELETE, RELEASE}.

The user subject may perform the following operations:

Table 2-4: User Subject Operation

User Subject Operation	Description
draft	The initial action of creating a message.
redraft	After creating a message, the action of modifying any of the message attributes, including message.content.
forward	The action of sending the message (and transferring ownership) to another user.
review	The action of exercising read-access to an owned message.
release	The action of forwarding the message to the Supervisor for transmission. This is reserved only for user instances satisfying user.release_clearance = message.classification (see object attribute definitions for class **message** below).
queue	The action of enqueueing the message for transmission. This is reserved only for user instances satisfying user.role_type = SUPERVISOR.

Below is the detailed definition of Local Data. The underlined attributes in the class definitions are CC security attributes.

Table 2-5: CC Security Attributes

Main Class	Subclass	Attribute	Attribute Values	Description
User_Data	message	classification	UNCLASSIFIED RESTRICTED CONFIDENTIAL SECRET NATO UNCLASSIFIED NATO RESTRICTED NATO CONFIDENTIAL NATO SECRET	Each classification value denotes the sensitivity of the message.content attribute. For outgoing messages (i.e. message.state = OUTGOING), the classification attribute is controlled by the current owner of the message. It cannot be modified after the supervisor has sent the message to the queue for transmission. Incoming messages (i.e. message.state = INCOMING), cannot be modified with regard to either attributes or content. *This is a **security attribute** in the MHS.*
		content	<ASCII>	Each message.content value denotes the current message content as created, modified or released by the message.owner user.
		owner	<User_ID>	The owner of each message object is assumed to be uniquely representable as a value <User_ID>, such that some instance of class user exists satisfying: user.name = message.owner.
		state	OUTGOING INCOMING QUEUED	The state of a message describes its stage of development upon creation (outgoing), queueing for transmission by the Supervisor (queued), and reception from an external source (incoming).

Main Class	Subclass	Attribute	Attribute Values	Description
TSF_Data	password	content	<ASCII>	The class represents the user's current password stored in a hashed form by the TOE. *This is a **security attribute** in the MHS.*
		owner	<User_ID>	The owner of each instance of a password is assumed to be uniquely representable as a value <User_ID>.

Class Nomenclature

The nomenclature above is used according to the following syntax rules:

- An attribute of an instantiated object is expressed <Main class> . <Subclass> . <Attribute>; and
- An attribute assignment of an instantiated object is expressed <Main class> . <Subclass> . <Attribute> = <Attribute Value>.

An example is User_Data.P.Owner = "jean_rivard", where P is an instantiation of subclass Password. Without loss of precision, we may omit the main class in the text, e.g. P.Owner = "jean_rivard".

This model effectively classifies all TOE information objects according to the CC model of User data, TSF Data and Security attribute.

2.2.7 Security Policy

Message objects have content and a set of attributes based on the ACP 127 model. Only the attributes defined in the previous section will be referenced, as only these have security relevance. The statement of security policy presented here is informal, and does not represent a claim to the CC SAR ADV_SPM.1. It is intended that the terminology used in the statements be easily mapped to the information model described above. For example, the phrase "outgoing message" denotes a message class instance M, where M.state = OUTGOING.

The following statements represent the Informal TOE Security Policy (TSP).

Informal Outgoing Message TSP

DAC_OM.1	*Every outgoing message has, at any given time after creation and prior to release, a unique owner user who has sole read-access, write-access and delete-access to the message.*
DAC_OM.2	*Every owner of an outgoing message may forward the message for review to any other user having read clearance for the classification of the message, in which case the owner's access privileges are transferred to the recipient of the outgoing message.*
DAC_OM.3	*For each classification C of outgoing message, there may exist a release authority based on external organizational policy. If defined, only that release authority has release privilege for an outgoing message of the classification C.*
DAC_OM.4	*For each outgoing message, if no release authority is defined, the default release authority is the boss of the current owner of the message.*
DAC_OM.5	*Prior to release, an outgoing message may be re-classified by the current owner of the message to a classification of equal or less sensitivity to the release privilege of the owner.*

Informal Incoming Message TSP

DAC_IM.1	*The TSF grants a user read-access to all incoming messages containing a Classification level of equal or less sensitivity to the Classification attribute of that specific user*

Informal General Message TSP

DAC_GM.1	*Read-access to a message is denied to any user whose read clearance is less than the classification of the message.*

Informal Message Export TSP

EP_OM.1	*Only the release authority having release permission for an outgoing message can transfer release permission for the message to the Supervisor.*
EP_OM.2	*Only the Supervisor can execute the export of an outgoing message.*

EP_OM.3 — *After sending of an outgoing message, message classification is time-invariant for all TSF operations.*

Informal Message Import TSP

IP_IM.1 — *The TSF preserves the time-invariance of the Classification and all non-security attributes and content of every incoming message imported by the TSF.*

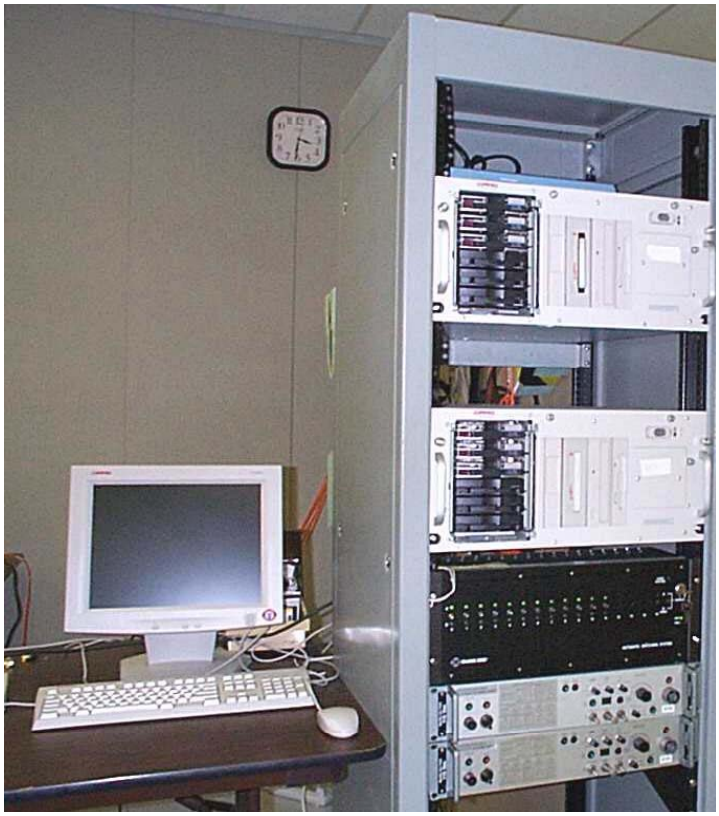


Figure 2-3: Typical Deployment of MHS

2.2.8 Hardware and Software Requirements

A typical deployment of the TOE is shown in Figure 2-3 on the previous page. The figure shows the monitor and keyboard of the PC terminal platform for MHS Client and the Rack-mounted MHS Server platform, optionally including a RAID Level 5 hard disk, and JAZ drive for backups and offline storage. Redundant server configurations can also be included for reliability.

The TOE software architecture supports the following server specification:

(a) Minimum CPU is a Pentium II 300 MHz;

(b) 384 MB RAM;

(c) 1 GB Free Hard Drive space;

(d) CD-ROM drive;

(e) 1.44 MB floppy drive;

(f) VGA video adapter capable of 1024x768 resolution;

(g) Colour monitor;

(h) Keyboard and Mouse;

(i) Minimum of one RS-232C Serial Port;

(j) Microsoft Windows NT Server 4.0;

(k) Microsoft Service Pack SP6a;

(l) File partitions are NTFS based;

(m) TCP/IP Protocol Drivers;

(n) Microsoft's C2Config.exe configured as per Installation Instructions Document;

(o) Borland's Interbase 6 Database software;

(p) Sun's Java 2 Runtime Environment, Standard Edition, Version 1.3.0_02;

(q) Norton Antivirus;

(r) MHS Server, Version 5.1 and

(s) MHS Client, Version 1.0.

The TOE software architecture supports the following workstation specification:

(t) Minimum CPU is a Pentium II 300 MHz;

(u) 128 MB RAM;

(v) 500 MB Free Hard Drive space;

(w) CD-ROM drive;

(x) 1.44 MB floppy drive;

(y) VGA video adapter capable of 1024x768 resolution;

(z) Colour monitor;

(aa) Keyboard and Mouse;

(bb) Microsoft Windows NT Workstation 4.0;

(cc) Microsoft Service Pack SP6a;

(dd) File partitions are NTFS based;

(ee) TCP/IP Protocol Drivers;

(ff) Microsoft's C2Config.exe configured as per Installation Instructions Document;

(gg) Sun's Java 2 Runtime Environment, Standard Edition, Version 1.3.0_02;

(hh) Norton Antivirus; and

(ii) MHS Client, Version 1.0.

2.2.9 Evaluated Configuration

The Evaluated Configuration for the TOE is designed to model the mode of operation in an actual network deployment. The elements of this configuration are shown in Figure 2-4 on the next page.

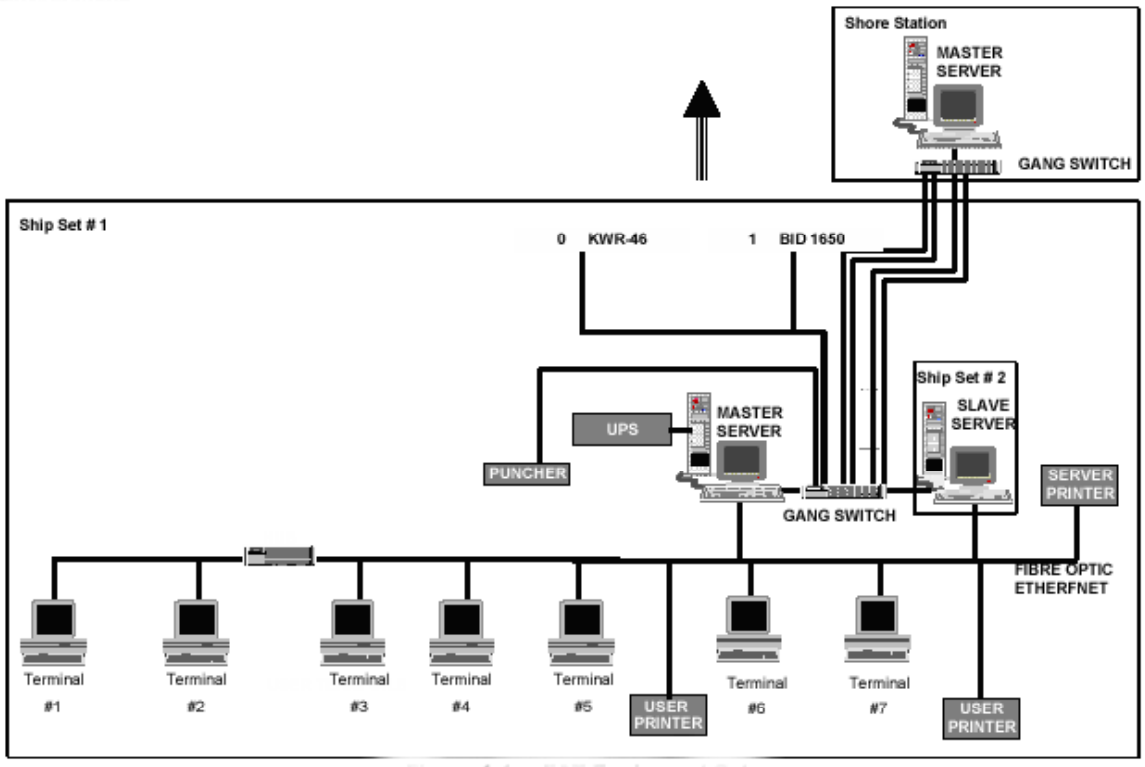


Figure 2-4: TOE Evaluated Configuration

2.2.10 TOE Boundary

The TOE Boundary includes only the two software components of the MHS:

- MHS Client; and
- MHS Server.

There are no hardware or firmware components within the TOE boundary.

3 SECURITY ENVIRONMENT

The TOE performs its security functionality in the security environment defined below. Listed below are the assumptions required for the environment and external components that interface to the TOE.

3.1 Assumptions

The list of assumptions regarding the security aspects of the environment in which the TOE is intended to be used is presented in the following subsections 3.1.1 to 3.1.4.

3.1.1 Physical Assumptions

It is assumed that the following physical conditions will exist in the environment of the TOE:

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification, interference and by-pass.

3.1.2 Personnel Assumptions

It is assumed that the following personnel conditions will be enforced by the organization in control of the environment of the TOE:

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The system administrative personnel are not careless, will fully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

3.1.3 Procedural Assumptions

The secure operation of the TOE is dependent on the presence of adequate security procedures. It is assumed that the following procedures are in place:

A.AUTHENTICATION Users will be procedurally authenticated and logged on physical entry to the zone in which the TOE operates through a sign-in procedure.

A.TIME_CHANGE The Supervisor will make an entry into the system log on each change or resetting of the server clock or system time.

3.1.4 Connectivity Assumptions

There are no server-to-server connections in the TOE network architecture. As described in Section 2.2.7, TOE connectivity within a ship-based LAN to client PC platforms is required. The following connectivity conditions are assumed:

A.CONNECT All connections to peripheral devices reside within the controlled access facilities. TOEs only address security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

A.INTERNAL_CHANNEL The internal communication channel between the TOE Client and Server platforms is a LAN that resides within the controlled access facilities and is separated by air gap from any external communications system. Internal communication paths connecting TOE Client and Server platforms are assumed to be adequately protected.

A.CHANNEL The Environment will provide communication channels between the TOE and authorized remote messaging systems that are logically distinct from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure.

3.2 Threats

This ST derives most security objectives from the statement of Organizational Security Policy found in the following section. However, some properties of the TOE require a statement of the following explicit threats countered by the TOE. A threat agent in the content of this TOE is an authorized user without

proper permission or an unauthorized user. The goal of the threat agent is to access or compromise classified message objects.

T.IMPORT	A threat agent could downgrade the classification bound to an imported message object and thereby destroy the binding between message object and classification internally within the TOE.
T.EXPORT	A threat agent could downgrade the classification bound to an exported message object and thereby destroy the binding between message object and classification external to the TOE.
T.READ_ACCESS	A threat agent could exploit a subject within the TSF Scope of Control (TSC) to execute a read access by a subject of lower classification to an object of higher classification.
T.WRITE_ACCESS	A threat agent could exploit a subject within the TSC to execute a write access by a subject of higher classification to an object of lower classification.
T.MODIFY_ACCESS	A threat agent could modify the classification information bound to a message object without authorization or detection, thus downgrading the classification of the message object prior to queueing for transmission.

3.3 Organizational Security Policies

An Organizational Security Policy is a set of rules or procedures imposed by an organization upon its operations to protect its sensitive data. The following policies are required to be enforced in the organization that hosts the TOE.

P.AUTHORIZED_USERS	Only those users who have been authorized to access the information within the system may access the system.
P.NEED_TO_KNOW	The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information.
P.ACCOUNTABILITY	The users of the system shall be held accountable for their actions within the system.

4 SECURITY OBJECTIVES

4.1 TOE Security Objectives

The Security Objectives of the TOE comprise the following:

O.AUTHORIZATION	The TSF must ensure that only authorized users gain access to the TOE and its resources.
O.DISCRETIONARY_ACCESS	The TSF must control access to resources based on identity of end users. The TSF must allow authorized users to specify which resources may be accessed by which users.
O.AUDITING	The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.
O.RESIDUAL_INFORMATION	The TSF must ensure that any information contained in a protected resource is not released when the resource is recycled.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.
O.ENFORCEMENT	The TSF must be designed and implemented in a manner, which ensures that the organizational policies are enforced in the target environment, without by-pass and interference.
O.IMPORT	All message objects imported to the TOE must preserve the security label information bound to the message object and retain the binding between message object and security label internally within the TOE.
O.EXPORT	All message objects exported from the TOE must export the security label information internally bound to the message object and export the binding relationship between message object and security label.

O.READ_ACCESS	All subjects within the TSC must prevent read access by a subject of lower security sensitivity to a message object of higher security sensitivity.
O.WRITE_ACCESS	Only the Supervisor may have access to the message object prior to queueing for transmission. After queueing, the TSF must prevent write access by any subject to any message attribute.
O.MODIFY_ACCESS	The TSF must detect and record in its audit trail all attempts to change the security label of a message object, and must prevent the change of security label bound to any transmitted message.

4.2 Environmental Security Objectives

4.2.1 IT Environmental Security Objectives

The IT Environmental Security Objectives comprise the following:

O.ENFORCEMENT	The TSF must be designed and implemented in a manner, which ensures that the organizational policies are enforced in the target environment, without by-pass and interference.

4.2.2 Non-IT Environmental Security Objectives

The non-IT Environmental Security Objectives comprise the following:

O.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives
O.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives, and by sitting the TOE network environment in an adequately protected location. All connections to peripheral devices must reside within the controlled access facilities and internal communication paths to access points such as terminals are protected by their physical location.

O.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives.
O.AUTHENTICATION	Those responsible for the TOE must ensure that the Users will be procedurally authenticated and logged on physical entry to the zone in which the TOE operates through a sign-in procedure.
O.TIME_CHANGE	Those responsible for the TOE must ensure that the Supervisor will make an entry into the system log on each change or resetting of the server clock or system time.
O.COMMS	Those responsible for the TOE must ensure that connectivity to external communication channels between the TOE and authorized remote messaging systems are logically distinct from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure.
O.INTERNAL_CHANNEL	Those responsible for the TOE must ensure that LAN connectivity services between the TOE Server and Client platforms are physically separated from external communication channels, provide assured identification of their end points and protect the channel data from modification or disclosure.

5 IT SECURITY REQUIREMENTS

5.1 Security Functional Requirements

5.1.1 Statement of Security Functional Requirements

This section contains the security functional requirements for the TOE. The following CC Part 2 Components are referenced, with definitions reproduced verbatim, from the text of the CC or completed where required. Completed definition text (i.e., added text not defined by the CC) is indicated below by *Italics*.

5.1.1.1 Security Audit (FAU)

5.1.1.1.1 Audit Data Generation (FAU_GEN.1)

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

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

(b) All auditable events for the *basic* level of audit except FIA_UID.1's user identity during failures; and

(c) *Events listed in column "Event" of Table 5-1*.

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

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

(b) For each audit event type, based on the auditable event definitions of the functional components included in the ST *as specified in the "Event" column of*

(c) *Table* 5-1 *(Auditable Events)*.

Table 5-1: Auditable Events

Component	Event	Note
FAU_GEN.1	Start-up and shutdown of the audit functions.	
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	The identity of the object.
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	
FIA_UAU.1	All use of the authentication mechanism.	
FIA_UID.1	All use of the user identification mechanism, including the identity provided during successful attempts.	The origin of the attempt (e.g. terminal identification.)
FIA_USB.1	Success and failure of binding user security attributes to a subject to create a subject). (e.g. success and failure	
FMT_MSA.1	All modifications of the values of security attributes.	
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.	
FMT_MTD.1(a)	All modifications to the values of TSF audit trail data.	
FMT_MTD.1(b)	All modifications to the values of TSF audited events data.	The new value of the TSF data.
FMT_MTD.1(c)	All modifications to the values of TSF user attribute data.	The new value of the TSF data.
FMT_MTD.1(d)(e)	All modifications to the values of TSF user authentication data.	
FMT_REV.1	All attempts to revoke security attributes.	
FMT_REV.1	All modifications to the values of TSF data.	
FMT_SMR.1	Modifications to the group of users that are part of a role type.	
FMT_SMR.1	Every use of the rights of a role type. (Additional /Detailed)	The role type and the origin of the request.
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the test.	
FPT_STM.1	Changes to the time.	

5.1.1.1.2 User Identity Association (FAU_GEN.2)

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

5.1.1.1.3 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide authorized administrator with the capability to read all audit information from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.1.4 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.

5.1.1.1.5 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches* of audit data based on the following attributes:

(a) User identity; and

(b) subject, severity (outcome), and date.

5.1.1.1.6 Selective Audit (FAU_SEL.1)

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) User identity; and

(b) Subject, severity (outcome), and date.

5.1.1.1.7 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

5.1.1.2 User Data Protection (FDP)

5.1.1.2.1 Complete Access Control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the *Discretionary Access Control Policy* on *the MHS server acting on the behalf of users, message objects* and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.1.2.2 Security Attribute Based Access Control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the *Discretionary Access Control Policy* to objects based on the *following:*

(a) The user identity associated with a subject; and

(b) The following access control attributes associated with an object: incoming message read permissions and outgoing message read, write, delete and release permissions.

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

Informal Outgoing Message TSP

DAC_OM.1 *Every outgoing message has, at any given time after creation and prior to release, a unique owner user who has sole read-access, write-access and delete-access to the message.*

DAC_OM.2 *Every owner of an outgoing message may forward the message for review to any other user having read clearance for the classification of the message, in which case the owner's access privileges are transferred to the recipient of the outgoing message.*

DAC_OM.3 *For each classification C of outgoing message, there may exist a release authority based on external organizational policy. If defined, only that release authority has release privilege for an outgoing message of the classification C.*

DAC_OM.4 *For each outgoing message, if no release authority is defined, the default release authority is the boss of the current owner of the message.*

DAC_OM.5 *Prior to release, an outgoing message may be re-classified by the current owner of the message to a classification of equal or less sensitivity to the release privilege of the owner.*

Informal Incoming Message TSP

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

DAC_IM.1 *The TSF grants a user read-access to all incoming messages containing a Classification level of equal or less sensitivity to the Classification attribute of that specific user.*

Informal General Message TSP

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects based in the following additional rules:

DAC_GM.1 *Read access to a message is denied to any user whose read clearance is less than the classification of the message.*

5.1.1.2.3 Export Of User Data With Security Attributes (FDP_ETC.2)

FDP_ETC.2.1 The TSF shall enforce the following:

Informal Message Export TSP

EP_OM.1 *Only the release authority having release permission for an outgoing message can transfer release permission for the message to the Supervisor.*

EP_OM.2 *Only the Supervisor can execute the export of an outgoing message.*

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:

EP_OM.3 *After sending of an outgoing message, message classification is time-invariant for all TSF operations*.

5.1.1.2.4 Import Of User Data With Security Attributes (FDP_ITC.2)

FDP_ITC.2.1 The TSF shall enforce the *following:*

IP_IM.1 ***(Informal Message Import TSP)***

The TSF preserves the time-invariance of the Classification and all non security attributes and content of every incoming message imported by the TSF

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: *none*.

5.1.1.2.5 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

5.1.1.3 Identification and Authentication (FIA)

5.1.1.3.1 User Attribute Definition (FIA_ATD.1)

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

(a) *User Name;*

(b) *Role Type;*

(c) *Password*;

(d) *Read Clearance*;

(e) *Release Clearance; and*

(f) *Boss.*

5.1.1.3.2 Verification Of Secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *the following*:

(a) *For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 1,000,000;*

(b) *For multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 100,000; and*

(c) *Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.*

5.1.1.3.3 Timing Of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow *the user identification* 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 the behalf of that user.

5.1.1.3.4 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the user while the authentication is in progress.

5.1.1.3.5 Timing Of Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow no *TSF mediated actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on the behalf of that user.

5.1.1.3.6 User-Subject Binding (FIA_USB.1)

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

(a) The user identity which is associated with auditable events;

(b) The user identity which are used to enforce the Discretionary Access Control Policy;

(c) The user role type used to enforce the Discretionary Access Control Policy;

(d) *The following other user security attributes: user.password, user.read_clearance, user.release_clearance and user.boss used to enforce Discretionary Access Control Policy*

NOTE 1 *The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of a user:*

(e) The TOE Client subject will act on behalf of the User by associating the user, name and user, password with the current TOE Client session.

NOTE 2 *The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of a user:*

(f) *The Administrator Role can change the User / Boss relationship, the User Client Function, enable auto-printing, allocate a mailbox slot, and disable the login.*

5.1.1.4 Security Management (FMT)

5.1.1.4.1 Management Of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the *Discretionary Access Control Policy* to restrict the ability to *modify* the security attributes associated *with a named object* to *the Administrator Role.*

5.1.1.4.2 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the *Discretionary Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the *Discretionary Access Control Policy*.

FMT_MSA.3.2 The TSF shall allow *the Administrator Role* to specify alternative initial values to override the default values when an object or information is created.

5.1.1.4.3 Management of the TSF Data (FMT_MTD.1)

5.1.1.4.3.1 *Management of the Audit Trail* (FMT_MTD.1.1(a))

FMT_MTD.1.1(a) The TSF shall restrict the ability to *create, delete, and clear the audit trail to authorized administrators.*

5.1.1.4.3.2 *Management of Audited Events* (FMT_MTD.1.1(b))

FMT_MTD.1.1(b) The TSF shall restrict the ability to *modify or observe the set of audited events to authorized administrators.*

5.1.1.4.3.3 *Management of User Attributes* (FMT_MTD.1.1(c))

FMT_MTD.1.1(c) The TSF shall restrict the ability to *initialize and modify the user security attributes, other than authentication data, to authorized administrators.*

5.1.1.4.3.4 *Management of Authentication Data* (FMT_MTD.1.1(d)(e))

FMT_MTD.1.1(d) The TSF shall restrict the ability to *initialize the authentication data to authorized administrators.*

FMT_MTD.1.1(e) The TSF shall restrict the ability to *modify the authentication data to the following:*

(a) authorized administrators; and

(b) *users authorized to modify their own authentication data time of the request.*

5.1.1.4.4 Revocation (FMT_REV.1)

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *users* within the TSC to *authorized administrators*.

The TSF shall restrict the ability to revoke security attributes associated with *objects* within the TSC to *users authorized to modify the security attributes by the Discretionary Access Control policy*.

FMT_REV.1.2 The TSF shall enforce the rules*:*

(a) The immediate revocation of security-relevant authorizations;

(b) The access rights associated with an object shall be enforced when an access check is made; and

(c) *[No additional rule]*.

5.1.1.4.5 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles:

(a) authorized administrator;

(b) users authorized by the Discretionary Access Control Policy to modify object security attributes;

(c) users authorized to modify their own authentication data (i.e., password); and

(d) *Supervisor.*

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

5.1.1.5 Protection of the TOE Security Functions (FPT)

5.1.1.5.1 Abstract Machine Testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start up, periodically during normal operation, or at the request of an authorized administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

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

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *Annex B of ACP 127 NATO Supp 3(A) "Message Relay Procedures" message attributes* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *Annex B of ACP 127 NATO Supp 3(A) "Message Relay Procedures" message attributes* when interpreting the TSF data from another trusted IT product.

5.1.2 Security Requirements for the IT Environment

This section contains the security requirements for the IT Environment. The following CC Part 2 Components are referenced, with definitions reproduced verbatim, from the text of the CC or completed where required. Completed definition text (i.e., added text not defined by the CC) is indicated below by *Italics*.

5.1.2.1 Protection of the TOE Security Functions (FPT)

5.1.2.1.1 Non-bypassability of the TSP (FPT_RVM.1)

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

5.1.2.1.2 TSF Domain Separation (FPT_SEP.1)

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.

5.1.2.1.3 Reliable Time Stamps (FPT_STM.1)

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

5.2 Security Assurance Requirements

5.2.1 Statement of Security Assurance Requirements

The following security assurance requirements (SARs) are claimed in accordance with EAL3 requirements, as stated in Part 3 of the CC.

Table 5-2: Security Assurance Requirements

ACM_CAP.3	Authorisation controls
ACM_SCP.1	TOE CM coverage
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance

AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.2.2 Statement of Strength of TOE Security Function

Strength of function, as a CC concept, applies to probabilistic or permutational mechanisms that are non-cryptographic in nature. This ST claims AVA_SOF.1 applicability for the user identification and authentication SFRs: FIA_UID.2 and FIA_UAU.2 through the user password entry function (see ITSF_USER_LOGIN in Section 6.1) and its mechanism.

The minimum strength of function level for the password entry mechanism is SOF-High.

6 TOE SUMMARY SPECIFICATION

6.1 Statement of TOE Security Functions

The TOE IT Security Functions are listed as follows.

ITSF_AUDIT	The TOE performs audit functions by recording all events that pertain to message import, export and reading by a user.
ITSF_DAC	The TOE controls access by an identified and authenticated user to those User Data objects whose Owner attribute is identical to that of the currently authenticated user.
ITSF_USER_LOGIN	The TOE requires the user to identify and authenticate himself/herself by a user login on the client platform. This is a probabilistic mechanism and is rated SOF-High.
ITSF_SERVER_LOGIN	The TOE requires the user to identify and authenticate himself/herself by a user login on the server platform. This is a probabilistic mechanism and is rated SOF-High. The TOE performs a system test on start-up to ensure the secure operation of the TOE.
ITSF_KERNEL	The TOE maintains and separates a security domain for its own execution that protects it from interference and tampering by untrusted subjects. The TOE ensures that all trusted functions properly terminate before invocation of a subsequent function. The TOE also is restricted to the creation, transmission, reception and handling of objects satisfying the ACP 127 message format only.

6.2 Statement of Assurance Measures

The assurance measures that are provided by the TOE are described below.

AM_ACM_CAP	TOE releases are uniquely identified with the version number and model identifier. All Configuration Items that comprise the TOE are under Configuration Management and are included on a Configuration List and uniquely identified by part number.
AM_ACM_SCP	TOE Configuration Management coverage analysis is provided.

AM_ADO_DEL	The TOE delivery procedures ensure that secure delivery of the TOE is achieved.
AM_ADO_IGS	Automated installation procedures are adequate to ensure that the user starts the TOE within a secure configuration.
AM_ADV_FSP	An informal functional specification is supplied for the TOE.
AM_ADV_HLD	The TOE High Level Design documentation addresses the requirements of ADV_HLD.1
AM_ADV_RCR	A representational correspondence is supplied to connect the TOE summary specification to the informal functional specification of TSFs provided, and to connect the informal functional specification to the high level design.
AM_AGD_ADM	The administrator's guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AM_AGD_USR	The User guidance is adequate to provide the user with the required knowledge to correctly perform login procedures and to provide security awareness of the TOE and its policies.
AM_ALC_DVS	Identification of security measures in the life cycle documentation is provided.
AM_ATE_COV	The analysis of coverage for testing is provided to assure completeness of coverage in testing of the TOE.
AM_ATE_DPT	Testing with respect to the High Level Design is provided.
AM_ATE_FUN	Functional testing of all security functions is provided in the referenced test plan (see Section 7.3.2).
AM_ATE_IND	The functional testing was performed by an independent third party.
AM_AVA_MSU	Examination of guidance is provided.
AM_AVA_SOF	The TOE Strength of Function Analysis addresses the requirements of AVA_SOF.1.
AM_AVA_VLA	The TOE vulnerability analysis addresses the requirements of AVA_VLA.1

The developer specific documentation that is offered in evidence for the above assurance measures is described below:

Table 6-1: Developer Specific Documentation Assurance Measures

Assurance Measure	Deliverable Title	Document Number	Description
AM_ACM_CAP	MHS Evaluation Evidence	1165C.01201-EE	List of Configuration Items, description of measures used to perform configuration management, and clearly identifies the evidence that THALES is providing against this assurance requirement
AM_ACM_SCP	MHS Evaluation Evidence	1165C.01201-EE	TOE Configuration Management Configuration
AM_ADO_DEL	MHS Evaluation Evidence	1165C.01201-EE	The delivery procedures to ensure that secure delivery of the TOE is achieved.
AM_ADO_IGS	MHS Installation Instructions	1165C.00903-II	Automated installation procedures are adequate to ensure that the user starts the TOE within a secure configuration.
AM_ADV_FSP	MHS Evaluation Evidence	1165C.01201-EE	An informal functional specification
AM_ADV_HLD	MHS Evaluation Evidence	1165C.01201-EE	Design documents describing the main functional subsystems.
AM_ADV_RCR	MHS Evaluation Evidence	1165C.01201-EE	A representational correspondence to connect the TOE summary specification to the informal functional specification of TSFs provided. Also provides the correspondence between the functional specification and the high-level design of the TSF
AM_AGD_ADM	MHS Administrator Manual	1474P.002-MHS-AM	The administrator's guidance for TOE
AM_AGD_USR	MHS User Manual, MHS Supervisor Manual	1474P.001-MHS-UM, 1474P.003-MHS-SM	The User and Supervisor guidance for TOE
AM_ALC_DVS	MHS Evaluation Evidence	1165C.01201-EE	TOE Life Cycle Document
AM_ATE_COV	MHS Evaluation Evidence	1165C.01201-EE	The analysis/evidence of coverage for testing is provided to assure completeness of coverage in testing of the TOE.
AM_ATE_DPT	MHS Evaluation Evidence	1165C.01201-EE	Mapping of Test document's Test Cases to AM_ADV_HLD

Assurance Measure	Deliverable Title	Document Number	Description
AM_ATE_FUN	MHS Evaluation Evidence	1165C.01201-EE	Functional testing of all security functions. This includes test procedures (with expected results) and observed test results.
AM_ATE_IND	External document supplied by Evaluation Laboratory	N/A	The functional testing performed by an independent third party.
AM_AVA_MSU	External document supplied by Evaluation Laboratory	N/A	The vulnerability analysis documented by an independent third party.
AM_AVA_SOF	MHS Evaluation Evidence	1165C.01201-EE	Strength of Function Analysis addresses the requirements of AVA_SOF.1 for functions claimed in the ST
AM_AVA_VLA	MHS Evaluation Evidence	1165C.01201-EE	Vulnerability analysis addresses the requirements of AVA_VLA.1. Vulnerability tests were derived from this analysis

7 RATIONALE

7.1 Security Objectives Rationale and Traceability

The purpose of this section is to show that the security objectives of the TOE are appropriate to the security problem defined in the security environment section (see Section 1.3). This is accomplished through a set of tables that cross-reference threats, security policies and assumptions against the security objectives that address them. Each threat, policy or assumption is addressed by one or more security objective. Each security objective of the TOE (described in Section 4.1) addresses at least one threat, policy or assumption. An informal argument is provided to show, for each threat, policy or assumption, why the identified security objective provides an effective countermeasure that prevents an attack or mitigates risk to acceptable levels.

7.1.1 Security Objectives Rationale for Environmental Assumptions

The following table shows the mapping for each of the security objectives for the non-IT environment to the environmental assumptions.

Table 7-1: Mapping for Each of the Security Objectives

Security Objectives / Environmental Assumptions	O.INSTALL	O.PHYSICAL	O.CREDEN	O.TIME_CHANGE	O.AUTHENTICATION	O.COMMS	O.INTERNAL_CHANNEL
A.MANAGE	X						
A.NO_EVIL_ADM	X						
A.LOCATE		X					
A.PROTECT		X					
A.CONNECT		X					
A.INTERNAL_CHANNEL							X
A.CHANNEL						X	
A.COOP			X				
A.AUTHENTICATION					X		
A.TIME_CHANGE				X			

The security objectives appear on the left for each row, and corresponding assumptions are indicated by an 'X' in the appropriate column.

It is clear from the above representation that each environmental security objective addresses at least one environmental assumption and that each environmental assumption is addressed by at least one environmental security objective.

The rationale for the environmental assumptions against the environmental security objectives is given in the table below. For each assumption a list of security objectives of the environment is given, followed by an argument stating how each security objective enforces the assumption in question.

Table 7-2: Environmental Assumptions Against the Environmental Security Objective

Assumption	Security Objective	Rationale
A.MANAGE	O.INSTALL	O.INSTALL ensures that the secure state of the system is achieved on initialization and that management of the system can proceed from a secure state.
A.NO_EVIL_ADM	O.INSTALL	O.INSTALL ensures that those responsible for the system will ensure the installation and management and operation are consistent with IT security objectives. This precludes the actions of a hostile administrator or supervisor.
A.LOCATE	O.PHYSICAL	O.PHYSICAL provides for the requirements of A.LOCATE by ensuring that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives through sitting in an adequately protected location.
A.PROTECT	O.PHYSICAL	O.PHYSICAL directly addresses A.PROTECT by ensuring that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.CONNECT	O.PHYSICAL	O.PHYSICAL directly addresses A.CONNECT by ensuring that all connections to peripheral devices reside within the controlled access facilities, and that internal communication paths to access points such as terminals are protected by their physical location.

Assumption	Security Objective	Rationale
A.INTERNAL_CHANNEL	O.INTERNAL_CHANNEL	O.INTERNAL_CHANNEL addresses A.INTERNAL_CHANNEL by ensuring that the LAN connectivity services between the TOE Server and Client platforms are physically isolated from external communication channels, provide assured identification of their end points and protect the channel data from modification or disclosure.
A.CHANNEL	O.COMMS	O.COMMS addresses A.CHANNEL by providing that communication channels between the TOE and authorized remote messaging systems that are logically distinct from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure.
A.COOP	O.CREDEN	O.CREDEN addresses A.COOP by ensuring that authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment. This includes the requirement that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives.
A.AUTHENTICATION	O.AUTHENTICATION	O.AUTHENTICATION directly provides for the requirements of A.AUTHENTICATION by ensuring that users will be procedurally authenticated and logged on physical entry to the zone in which the TOE operates through a sign-in procedure
A.TIME_CHANGE	O.TIME_CHANGE	O.TIME_CHANGE directly provides for the requirements of A.TIME_CHANGE by ensuring that the Supervisor will make an entry into the system log on each change or resetting of the server clock or system time.

7.1.2 TOE Security Objectives Rationale for Threats

The mapping between the threats addressed by the TOE and the TOE Security Objectives is shown in the table below. The threats appear on the left for each row, and corresponding Security Objectives are indicated by an ‘X’ in the appropriate column.

Table 7-3: Corresponding Security Objectives

Security Objectives / Threats	O.IMPORT	O.EXPORT	O.READ_ACCESS	O.WRITE_ACCESS	O.MODIFY_ACCESS
T.IMPORT	X				
T.EXPORT		X			
T.READ_ACCESS			X		
T.WRITE_ACCESS				X	
T.MODIFY_ACCESS					X

The rationale for the threats against the security objectives is given in the table below. For each threat a list of security objectives of the TOE is given, followed by an argument stating how each TOE security objective counters the threat in question.

Table 7-4: Security Objective

Threat	Security Objective	Rationale
T.IMPORT	**O.IMPORT**	O.IMPORT prevents the possibility of T.IMPORT by enforcing all message objects imported to the TOE to preserve the security label information bound to the message object and retain the binding between message object and security label internally within the TOE. No change of message sensitivity is therefore possible.
T.EXPORT	**O.EXPORT**	**O.EXPORT** prevents the possibility of T.EXPORT by enforcing all message objects exported from the TOE to export the security label information internally bound to the message object and export the binding relationship between message object and security label through the uniform interpretation of ACP 127 message formats.

Threat	Security Objective	Rationale
T.READ_ACCESS	**O.READ_ACCESS**	**O.READ_ACCESS** prevents the possibility of T.READ_ACCESS by preventing all subjects within the TSF to execute read access if the subject is of lower security sensitivity to a message object of higher security sensitivity.
T.WRITE_ACCESS	**O.WRITE_ACCESS**	**O.WRITE_ACCESS** prevents the possibility of T.WRITE_ACCESS by preventing all subjects within the TSC to execute write access to the attribute of any queued message, including the classification of the message.
T.MODIFY_ACCESS	**O.MODIFY_ACCESS**	**O.MODIFY_ACCESS** prevents threat agents from changing the security label information bound to a message object after release and transmission, and ensures that all such attempts are audited.

7.1.3 Organizational Policy Rationale

The mapping between the Organizational policies enforced in the TOE Environment and the Organizational Security Objectives is shown in the table below. The policies appear on the left for each row, and corresponding Security Objectives are indicated by an 'X' in the appropriate column.

Table 7-5: Organizational Policy Rationale

Security Objectives / Policies	O.AUTHORIZATION	O.MANAGE	O.ENFORCEMENT	O.DISCRETIONARY_ACCESS	O.RESIDUAL_INFORMATION	O.AUDITING
P.AUTHORIZED_USERS	X	X	X			
P.NEED_TO_KNOW		X	X	X	X	
P.ACCOUNTABILITY		X	X			X

The rationale for the policies against the security objectives is given in the table below. For each policy a list of security objectives of the TOE Environment is given, followed by an argument stating how each security objective satisfies the policy in question.

Table 7-6: Organizational Policy

Organizational Policy	Security Objective	Rationale
P.AUTHORIZED_USERS	**O.AUTHORIZATION** **O.MANAGE** **O.ENFORCEMENT**	P.AUTHORIZED_USERS states that only those users authorized to access the information assets of the system may access the system. The policy is implemented by O.AUTHORIZATION, and supported by O.MANAGE by requiring authorized administrators to be able to manage the functions. O.ENFORCEMENT ensures that the functions are invoked and operational.
P.NEED_TO_KNOW	**O.MANAGE** **O.ENFORCEMENT** **O.DISCRETIONARY_ACCESS** **O.RESIDUAL_INFORMATION**	P.NEED_TO_KNOW states that access to the read, modification and destruction of information access must be limited to authorized users having need-to-know. O.DISCRETIONARY_ACCESS implements this policy. O.MANAGE supports the policy by requiring authorized administrators to manage the functions. O.ENFORCEMENT ensures that the functions are always invoked and operational. O.RESIDUAL_INFORMATION enforces the restrictions on resources defined by authorized users by ensuring that information is not left behind in a resource that may have different restrictions placed upon it.
P.ACCOUNTABILITY	**O.MANAGE** **O.ENFORCEMENT** **O.AUDIT**	P.ACCOUNTABILITY requires users of the system to be held accountable for their actions in the system. This policy is implemented by O.AUDIT in requiring the recording of actions in an audit trail. O.MANAGE supports this by requiring the secure management of the audit trail, and O.ENFORCEMENT ensures that functions are always invoked and operational.

7.2 Security Requirements Rationale

7.2.1 Security Functional Requirements (SFRs) Rationale

The mapping between the SFRs and the Security Objectives is shown in the table below. The SFRs appear on the left for each row, and corresponding Security Objectives are indicated by an 'X' in the appropriate column.

Table 7-7: Security Functional Requirements

SFR	Description	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS	O.AUDITING	O.RESIDUAL_INFORMATION	O.MANAGE	O.ENFORCEMENT	O.IMPORT	O.EXPORT	O.WRITE_ACCESS	O.READ_ACCESS	O.MODIFY_ACCESS
FAU_GEN.1	Audit Data Generation			X								X
FAU_GEN.2	User Identity Association			X								X
FAU_SAR.1	Audit Review			X								X
FAU_SAR.2	Restricted Audit Review			X								
FAU_SAR.3	Selectable Audit Review			X		X						
FAU_SEL.1	Selective Audit			X		X						
FAU_STG.1	Protected audit trail storage			X								
FDP_ACC.2	Complete Access Control		X							X	X	X
FDP_ACF.1	Security Attribute Based Access Control		X									
FDP_ETC.2	Export of user data with security attributes								X			X
FDP_ITC.2	Import of user data with security attributes							X				
FDP_RIP.2	Full Residual Information Protection				X							
FIA_ATD.1	User Attribute Definition	X	X									
FIA_SOS.1	Verification Of Secrets	X										
FIA_UAU.1	Timing Of Authentication	X										

SFR	Description	O.AUTHORIZATION	O.DISCRETIONARY_ACCESS	O.AUDITING	O.RESIDUAL_INFORMATION	O.MANAGE	O.ENFORCEMENT	O.IMPORT	O.EXPORT	O.WRITE_ACCESS	O.READ_ACCESS	O.MODIFY_ACCESS
FIA_UAU.7	Protected Authentication Feedback	X										
FIA_UID.1	Timing Of Identification	X										
FIA_USB.1	User-Subject Binding		X									
FMT_MSA.1	Management of Object Security Attributes		X									
FMT_MSA.3	Static Attribute Initialization		X									
FMT_MTD.1(a)	Management of the Audit Trail			X		X						
FMT_MTD.1(b)	Management of Audited Events			X		X						
FMT_MTD.1(c)	Management of User Attributes					X						
FMT_MTD.1(d)(e)	Management of Authentication Data	X				X						
FMT_REV.1	Revocation		X			X						
FMT_SMR.1	Security Roles					X						
FPT_AMT.1	Abstract Machine Testing						X					
FPT_RVM.1	Non-bypassability of the TSP						X					
FPT_SEP.1	TSF Domain Separation						X					
FPT_TDC.1	Inter-TSF basic TSF data consistency							X				

The rationale for the SFRs against the security objectives of the TOE and its IT environment is given in the table below. For each security objective of the TOE, a list of assigned SFRs is given, followed by an argument stating how each SFR addresses or satisfies the security objective in question.

Table 7-8: SFR Security Objective

Security Objective	SFR	Rationale
O.AUTHORIZATION	FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.7 FIA_UID.1 FMT_MTD.1(d) FMT_MTD.1(e)	FIA_ATD.1 provides that the TSF maintain the user identifiers, role types, passwords that enable identification and authentication of users. FIA_SOS.1 provides that the strength of the password function is of SOS_HIGH level. FIA_UAU.1 allows only the user identification on behalf of the user to be performed before the user is authenticated. FIA_UAU.7 prevents the disclosure of user password information during login. FIA_UID.1 allows no other actions to be taken by the user prior to user identification. These requirements collectively ensure that only authorized users gain access to the TOE and its resources. FMT_MTD.1(d) ensures only authorized Administrators can initially assign a password to a user account. FMT_MTD.1(e) ensures only authorized Administrators and the user corresponding to the password can change a password.
O.DISCRETIONARY_ACCESS	FDP_ACC.2 FDP_ACF.1 FIA_ATD.1 FIA_USB.1 FMT_MSA.1 FMT_MSA.3 FMT_REV.1	FDP_ACC.2 provides that the TOE Discretionary Access Control Policy is enforced and allow for authorized users to forward message objects to other authorized users, and thereby provide discretionary access and ownership transfer between users. FDP_ACF.1 provides that a) each user identity is associated with a subject; and b) The following access control attributes are associated with an object: incoming message read permissions and outgoing message read, write, delete and release permissions. This supports the enforcement of DAC policy expressed by FDP_ACF.1. FIA_ATD.1 provides that the TSF shall maintain the following list of security attributes belonging to individual users: a) User Name; b) Role Type; c) Password, d) Read Clearance; e) Release Clearance; f) Boss, that collectively determine the security attributes of the user subject engaged in discretionary access events. FIA_USB.1 associates the above user security attributes with subjects acting on the behalf of that user. FMT_MSA.1 provides that the TSF shall restrict the ability to initialize and modify the user security attributes, other than authentication data, to authorized administrators. Also, the TSF shall restrict the ability to initialize the authentication data to authorized administrators. Furthermore, the TSF shall restrict the ability to modify the authentication data to the following a) authorized administrators; and b) users authorized to modify

Security Objective	SFR	Rationale
		their own authentication data time of the request. This provides for the secrecy of user authentication data required for effective implementation of DAC policy. FMT_MSA.3 provides each message object with restrictive default Discretionary Access Control values, namely, exclusive read-access through ownership by the user creating the message object. FMT_REV.1 provides that the TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to authorized administrators.
O.AUDITING	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FMT_MTD.1(a) FMT_MTD.1(b)	FAU_GEN.1 and FAU_GEN.2 provide that audit records will be generated for selected events and that the TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_SAR.1 provides that the TSF shall provide authorized administrators with the capability to read all audit information from the audit records and that the audit records will be presented in a manner suitable for the user to interpret the information. FAU_SAR.2 provides that the TSF will restrict users from having read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.3 provides that the TSF shall provide the ability to perform searches of specified types on the audit records. FAU_SEL.1 provides that the TSF shall be able to include or exclude auditable events from the set of audited events based on the specified attributes. FAU_STG.1 provides that the TSF shall protect the stored audit records from unauthorized deletion, and to prevent modifications to the audit records. Thus the integrity of audit records is guaranteed. FMT_MTD.1(a) provides that the TSF shall allow management of the Audit Trail and restrict the ability to create, delete, and clear the audit trail to authorized administrators. Furthermore FMT_MTD.1(b) provides that the TSF restrict the ability to modify or observe the set of audited events to authorized administrators.
O.RESIDUAL_ INFORMATION	FDP_RIP.2	FDP_RIP.2 provides that the TSF will prevent access to residual information by ensuring that no such information is released when the resource is recycled.
O.MANAGE	FAU_SAR.3 FAU_SEL.1 FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c) FMT_MTD.1(d) FMT_MTD.1(e) FMT_REV.1 FMT_SMR.1	FAU_SAR.3 provides that the TSF shall provide the ability to perform searches of specified types on the audit records. FAU_SEL.1 provides that the TSF shall be able to include or exclude auditable events from the set of audited events based on the specified attributes FMT_MTD.1(a) provides that the TSF restrict the ability to create, delete, and clear the audit trail to authorized administrators. FMT_MTD.1(b) provides that the TSF restrict the ability to

Security Objective	SFR	Rationale
		modify or observe the set of audited events to authorized administrators. FMT_MTD.1(c) provides that the TSF restrict the ability to initialize and modify the user security attributes, other than authentication data, to authorized administrators. FMT_MTD.1(d) provides that the TSF restrict the ability to initialize the authentication data to authorized administrators. FMT_MTD.1(e) provides that the TSF restrict the ability to modify the authentication data to authorized administrators and users authorized to modify their own authentication data time of the request. FMT_REV.1 provides that the TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to authorized administrators, and that revocations be effective immediately. FMT_SMR.1 provides that the TSF maintain role types and that the role types can be associated by the TSF with users
O.ENFORCEMENT	FPT_AMT.1 FPT_RVM.1 FPT_SEP.1	FPT_AMT.1 provides that the TSF run a suite of tests during initial start-up to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_RVM.1 provides that the TSF ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_SEP.1 provides that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and that the TSF shall enforce separation between the security domains of subjects in the TSC.
O.IMPORT	FDP_ITC.2 FPT_TDC.1	FDP_ITC.2 provides that the TSF enforce import policy IP_IM.1, stating the time-invariance of the Classification, all non-security attributes and content of every incoming message imported by the TSF. FPT_TDC.1 provides that the TSF provide the capability to consistently interpret and use NATO ACP 127 message attributes when shared between the TSF and another trusted IT product.
O.EXPORT	FDP_ETC.2	FDP_ETC.2 provides that the TSF enforce export policy IP_EM.1, stating the conditions for release of a message exported by the TSF.
O.READ_ACCESS	FDP_ACC.2	FDP_ACC.2 provides that the TOE Discretionary Access Control Policy is enforced for all operations among subjects and objects covered by the DAC policy, including read operations.
O.WRITE_ACCESS	FDP_ACC.2	FDP_ACC.2 provides that the TOE Discretionary Access Control Policy is enforced for all operations among subjects and objects covered by the DAC policy, including write operations.

Security Objective	SFR	Rationale
O.MODIFY_ACCESS	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FDP_ACC.2 FDP_ETC.2	FAU_GEN.1, FAU_GEN.2 and FAU_SAR.1 ensure that changes to the security label information bound to a message object are audited and can be viewed by authorized personnel to determine the user responsible. FDP_ACC.2 provides that the permissive TOE Discretionary Access Control Policy is enforced for all operations among subjects and objects covered by the DAC policy. The proscriptive policy EP_OM.3 that denies changes to the classification of a message after export is enforced in FDP_ETC.2.

The coverage of the above table against the SFRs satisfies the following properties:

- for every security objective of the TOE, there is at least one SFR that satisfies it;
- for every SFR, there is at least one security objective of the TOE that it addresses; and
- for every security objective of the TOE, an informal argument as to why the identified SFRs are sufficient to meet it is provided.

7.2.2 Functional Claims Rationale

The selected functionality for this ST is consistent with and appropriate for the security objectives for the TOE. There are 4 main categories of security service that the TOE provides:

- User Identification and Authentication must precede all other access to protected information, providing binding between the user and the client session;
- Import of message objects;
- Export of message objects; and
- Controlled access to message objects during the creation and release process.

These security services embody the security objectives of the TOE and its IT environment are consistent with the level of capability and motivation that a threat agent would be expected to possess, given the assumptions regarding data sensitivity of information assets and sophistication of threat agent. Elimination of all potential threat agents clearly requires environmental support, procedural security and training. The latter safeguards are complementary security objectives that the environment is expected to

supplement the TOE functional properties with in order to obtain an overall acceptable level of risk. They do not constitute weaknesses or omissions in the TOE, as the majority of the environmental security objectives are beyond the scope of any conceivable software solution. In addition, not all may represent serious risk to the average system in which the TOE is deployed.

7.2.3 SFR Dependency Rationale

The following table shows the dependency analysis of the claimed SFRs for the TOE and its IT environment. The traceability of an SFR dependency is confirmed by selecting an SFR from the left-hand column and noting the columns in which an 'X' appears. Each such column determines an SFR that should be included in the claims of Section 5 by way of a dependency rule specified in the CC, Part 2. In the case where an alternative is specified in the CC, at least one of the alternative SFRs has been chosen. In the case of those SFRs that depend on FDP_ACC.1 (i.e., FDA_ACF.1, FDP_ETC.2, FDP_ITC.2 and FMT_MSU.1), the refinement FDP_ACC.2 is claimed. Note that FPT_STM.1 is a SFR for the IT Environment that satisfies the dependency requirement of FAU_GEN.1

By confirming that each column SFR is also a row SFR in the matrix, the property of closure under dependencies is established for Section 5 (with the exception of the unsupported dependencies FTP_ITC.1 and FTP_TRP.1, as explained below in Section 7.2.4).

Table 7-9: SFR Dependency Rationale

SFR	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.2	FDP_ACF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_STM.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FAU_GEN.1													X			
FAU_GEN.2	X							X								
FAU_SAR.1	X															
FAU_SAR.2		X														
FAU_SAR.3		X														
FAU_SEL.1	X										X					
FAU_STG.1	X															
FDP_ACC.2					X											

SFR	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.2	FDP_ACF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_STM.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ACF.1				X						X						
FDP_ETC.2				X												
FDP_ITC.2				X										X	[X]	O
FDP_RIP.2																
FIA_ATD.1																
FIA_SOS.1																
FIA_UAU.1								X								
FIA_UAU.7							X									
FIA_UID.1																
FIA_USB.1						X										
FMT_MSA.1				X								X				
FMT_MSA.3									X			X				
FMT_MTD.1												X				
FMT_REV.1												X				
FMT_SMR.1								X								
FPT_AMT.1																
FPT_RVM.1																
FPT_SEP.1																
FPT_STM.1																
FPT_TDC.1																
FTP_ITC.1	NOT SUPPORTED															
FTP_TRP.1	NOT SUPPORTED															

7.2.4 Rationale for Unsupported Dependencies

FTP_ITC.1 is a dependency of FDP_ITC.2. The notation '[X]' in the table indicates that this requirement is not met directly by the TOE, but rather by the environmental assumptions A.CHANNEL and A.INTERNAL_CHANNEL. This is justified by the fact that all external communications between the TOE and external communications channels and off-ship message handling systems are the responsibility of the ship environment and its command. Furthermore, such protections are mandated by military security policy to specialized cryptographic and communications systems that must necessarily lie outside the TSC and TOE boundary.

The only other potential alternative dependency of FDP_ITC.2 provided by the CC, Part 2, is FTP_TRP.1. This is represented by the notation 'O' in the table. If applicable, it could replace the requirement for FTP_ITC.1. In the context of FDP_ITC.2 however, the use of a trusted path could only be relevant if the import of the message object were directly from the user, or possibly from some device or storage medium under direct monitoring control of the user. This is clearly not the case, as all imported message objects originate from an external off-ship ACP 127 system, and must be transmitted under the provisions of A.CHANNEL. By definition, a trusted path cannot fulfil these requirements.

Similarly, the LAN, which uniquely provides the channel connecting the TOE Client and Server components, is assumed to have sufficient isolation and protection properties to provide the assurance that TOE communications between these two components is not disclosed or modified in an unauthorized fashion. This is stated in A.INTERNAL_CHANNEL. The LAN entity is outside the TSC. Thus the requirements of FTP_TRP.1 are fulfilled through the environment by A.INTERNAL_CHANNEL.

No claim for TOE conformity is therefore relevant regarding either FTP_ITC.1 or FTP_TRP.1. This is indicated by the shaded rows for FTP_ITC.1 and FTP_TRP.1 at the bottom of the table. The intended functionality of both is captured in A.CHANNEL and A.INTERNAL_CHANNEL.

7.2.5 Security Assurance Requirements Rationale (SARs)

Given the statement of security environment and security objectives contained in this ST, an assurance level of EAL3 is appropriate to capture the moderate level of independently assured protection provided by the TOE. For environments that have an adequate security policy and set of security procedures that address the issues raised in the environmental assumptions (see Section 3.1), the services of the TOE will provide secure discretionary access control and audit services.

The vulnerability analysis required by AVA_VLA.1 and strength of function analysis required by AVA_SOF.1 are appropriate for the level of protection claimed by this TOE, and is provided, as referenced in Section 6.2 (see also Section 5.2.2 for claim).

7.2.6 Strength of Function Rationale

The TOE minimum strength of function of SOF-High is selected as required by our customers. The explicit strength of function claim for the authentication mechanism described in FIA_SOS.1 and FIA_UAU.1 of guessing a password is strong and is in turn consistent with the security objectives described in Section 7.2.1.

The SOF-High strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST, specifically given the assumption A.COOP (Authorized users possess the necessary authorization to access at least some of the information management by the TOE and are expected to act in a cooperating manner in a benign environment.)

7.3 TOE Summary Specification Rationale

7.3.1 IT Security Functions Rationale (SFRs)

The mapping between the IT security functions and the SFRs is shown in the table on the next page.

Table 7-10: IT Security Functions Rationale

SFR	ITSF_AUDIT	ITSF_DAC	ITSF_USER_LOGIN	ITSF_SERVER_LOGIN	ITSF_KERNEL
FAU_GEN.1	**X**				
FAU_GEN.2	**X**				
FAU_SAR.1	**X**				
FAU_SAR.2	**X**				

SFR	ITSF_AUDIT	ITSF_DAC	ITSF_USER_LOGIN	ITSF_SERVER_LOGIN	ITSF_KERNEL
FAU_SAR.3	**X**				
FAU_SEL.1	**X**				
FAU_STG.1	**X**				
FDP_ACC.2		**X**			
FDP_ACF.1		**X**			
FDP_ETC.2		**X**			
FDP_ITC.2		**X**			
FDP_RIP.2		**X**			
FIA_ATD.1		**X**			
FIA_SOS.1			**X**		
FIA_UAU.1			**X**		
FIA_UAU.7			**X**		
FIA_UID.1			**X**		
FIA_USB.1			**X**		
FMT_MSA.1		**X**			
FMT_MSA.3		**X**			
FMT_MTD.1	**X**	**X**			
FMT_REV.1		**X**			
FMT_SMR.1		**X**			
FPT_AMT.1				**X**	
FPT_TDC.1					**X**

The IT security functions appear on the left for each row, and corresponding SFRs are indicated by an ‘X’ in the appropriate column.

The detailed traceability of the TSF to the Security Function Requirements follows. The TOE IT Security Functions are referenced to the list of SFRs, described in Section 5, that are provided by the defined IT Security Function. Specifications of IT Security Functions are provided in Section 6.1. A Coverage Mapping is included to describe how the IT Security Functions covers the referenced SFR.

Table 7-11: IT Security Functions

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FAU_GEN.1	ITSF_AUDIT	ITSF_AUDIT creates audit records satisfying the FAU_GEN.1 requirements for auditable events.
FAU_GEN.2	ITSF_AUDIT	ITSF_AUDIT creates audit records satisfying the FAU_GEN.1 requirements for association of auditable events with user name.
FAU_SAR.1	ITSF_AUDIT	ITSF_AUDIT provides administrators with the capability of reading all audit records and presents the records in a manner suitable for the supervisor to interpret.
FAU_SAR.2	ITSF_AUDIT	ITSF_AUDIT prohibits all users from read access to the audit trail with the exception of the supervisor.
FAU_SAR.3	ITSF_AUDIT	ITSF_AUDIT provides the ability to perform searches for audit events satisfying specified user identity, subject, severity (outcome) and/or date information.
FAU_SEL.1	ITSF_AUDIT	ITSF_AUDIT allows the inclusion or exclusion of events in the audit trail based on specified user identity, subject, severity (outcome) and/or date information.
FAU_STG.1	ITSF_AUDIT	ITSF_AUDIT protects audit records from deletion and modification.
FDP_ACC.2	ITSF_DAC	ITSF_DAC provides the TOE DAC policy on all user subjects, message objects and operations between subjects and objects.
FDP_ACF.1	ITSF_DAC	ITSF_DAC enforces the DAC policies specified in FDP_ACF.1.
FDP_ETC.2	ITSF_DAC	ITSF_DAC enforces the DAC export policies specified in FDP_ETC.2.
FDP_ITC.2	ITSF_DAC	ITSF_DAC enforces the DAC import policies specified in FDP_ITC.2.
FDP_RIP.2	ITSF_DAC	ITSF_DAC includes protection against object reuse attacks, and prevents the leakage of residual information. In doing so, it meets the requirements of FDP_RIP.2

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FIA_ATD.1	ITSF_DAC	ITSF_DAC maintains the required user attributes necessary to correctly mediate all DAC policies.
FIA_SOS.1	ITSF_USER_LOGIN	ITSF_USER_LOGIN uses a strong password mechanism that prevents a random attempt at password guessing from success by reducing the probability to 1/1,000,000.
FIA_UAU.1	ITSF_USER_LOGIN	ITSF_USER_LOGIN does not permit user actions other than user identification to be performed prior to user authentication.
FIA_UAU.7	ITSF_USER_LOGIN	ITSF_USER_LOGIN does not provide explicit feedback to the user while authentication is in progress. This satisfies the requirements of FIA_UAU.7.
FIA_UID.1	ITSF_USER_LOGIN	ITSF_USER_LOGIN does not permit user actions prior to authentication with the exception of user identification. This satisfies the requirements of FIA_UID.1
FIA_USB.1	ITSF_USER_LOGIN	ITSF_USER_LOGIN provides a binding between user name and auditable events and DAC mediations. This satisfies the requirements of FIA_USB.1
FMT_MSA.1	ITSF_DAC	ITSF_DAC restricts the ability to modify the DAC control attributes associate with a named object to the administrator. This satisfies the requirements of FMT_MSA.1
FMT_MSA.3	ITSF_DAC	ITSF_DAC enforces DAC to provide restrictive default values for users on creation (no read permissions). This satisfies the requirements of FMT_MSA.3
FMT_MTD.1.1 (a)	ITSF_AUDIT ITSF_DAC	ITSF_AUDIT provides ability to create, delete or clear the audit trail to the administrator. ITSF_DAC restricts the ability to create, delete or clear the audit trail to the supervisor. This satisfies the requirements of FMT_MTD.1
FMT_MTD.1.1 (b)	ITSF_DAC	ITSF_DAC restricts the ability to modify or observe audit events to the supervisor. This satisfies the requirements of FMT_MTD.1
FMT_MTD.1.1 (c)	ITSF_DAC	ITSF_DAC restrict the ability to initialize and modify the user security attributes, other than authentication data, to authorized administrators. This satisfies the requirements of FMT_MTD.1
FMT_MTD.1.1 (d)	ITSF_DAC	ITSF_DAC restrict the ability to initialize the authentication data to authorized administrators. This satisfies the requirements of FMT_MTD.1

Security Functional Requirement	IT Security Function	IT Security Function to SFR Coverage Mapping
FMT_MTD.1.1 (e)	ITSF_DAC	ITSF_DAC restrict the ability to modify the authentication data to authorized administrators and users authorized to modify their own authentication data time of the request. This satisfies the requirements of FMT_MTD.1
FMT_REV.1	ITSF_DAC	ITSF_DAC allows only the administrator to revoke a user' security attributes. This satisfies the requirements of FMT_REV.1
FMT_SMR.1	ITSF_DAC	ITSF_DAC enforces the security role types: a) user; b) administrator; c) supervisor.
FPT_AMT.1	ITSF_SERVER_LOGIN	ITSF_SERVER_LOGIN performs system testing on start-up.
FPT_TDC.1	ITSF_KERNEL	ITSF_KERNEL ensures that all local and inter-TSF message traffic adheres to ACP 127 standard message format and therefore ensures TSF data consistency.

The combined aggregate of the TOE security functions satisfies the set of identified TOE SFRs as shown above. Provided the configuration and maintenance of the TOE is carried out in accordance with organizational policy, environmental assumptions, and following vendor recommendations, the TOE security functional claims are valid.

7.3.2 Assurance Measures Rationale

The compliance of the TOE with the required assurance measures is established in the table below.

Table 7-12: Assurance Measures Rationale

Assurance Components	Description	Assurance Measures	Compliance
ACM_CAP.3	Authorisation controls	AM_ACM_CAP	TOE releases are adequately identified with the version number. All Configuration Items that comprise the TOE are under Configuration Management and are included on a Configuration List.
ACM_SCP.1	TOE CM coverage	AM_ACM_SCP	The coverage of the Configuration Management System includes tracking of source code changes, documentation (including the CM Plan), and provides information on any tools comprising the CM System and development support. Security flaws are tracked.
ADO_DEL.1	Delivery procedures	AM_ADO_DEL	The TOE delivery procedures ensure that secure delivery of the TOE is achieved.

Assurance Components	Description	Assurance Measures	Compliance
ADO_IGS.1	Installation, generation, and start-up procedures	AM_ADO_IGS	Automated installation procedures are adequate to ensure that the user starts the TOE within a secure configuration.
ADV_FSP.1	Informal functional specification	AM_ADV_FSP	An informal functional specification is supplied for the TOE.
ADV_HLD.2	Security enforcing high-level design	AM_ADV_HLD	High level design documentation supplied describes the informal TOE design, its subsystems, and the security functionality provided by the subsystems.
ADV_RCR.1	Informal correspondence demonstration	AM_ADV_RCR	A representational correspondence is supplied to connect the TOE summary specification to the informal functional specification of TSFs provided and to link the informal functional specification to the high-level design.
AGD_ADM.1	Administrator guidance	AM_AGD_ADM	The administrator's guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AGD_USR.1	User guidance	AM_AGD_USR	The User guidance is adequate to provide the user with the required knowledge to correctly perform login procedures and to provide security awareness of the TOE and its policies.
ALC_DVS.1	Identification of security measures	AM_ALC_DVS	The development environment is a secure facility, and its security documentation describe physical, procedural, personnel and network security measures that protect the integrity and confidentiality of the TOE design and implementation.
ATE_COV.2	Analysis of coverage	AM_ATE_COV	The analysis of coverage for testing is provided to assure completeness of coverage in testing of the TOE.
ATE_DPT.1	Testing: high-level design	AM_ATE_DPT	The depth of functional testing is analyzed and it is demonstrated that the TSF operates in accordance with its high-level design.
ATE_FUN.1	Functional testing	AM_ATE_FUN	Functional testing of all security functions, including identification and authentication, discretionary access control and audit components, is provided.
ATE_IND.2	Independent testing - sample	AM_ATE_IND	The functional testing was performed by an independent third party.
AVA_MSU.1	Examination of guidance	AM_AVA_MSU	Guidance documentation is analyzed for completeness, and the presence of misleading, conflicting and unreasonable guidance is addressed. Insecure states are clearly identified.

Assurance Components	Description	Assurance Measures	Compliance
AVA_SOF.1	Strength of TOE security function evaluation	AM_AVA_SOF	The TOE Strength of Function Analysis addresses the requirements of AVA_SOF.1 by providing analysis supporting a claim of SOF-High for the TOE password mechanism implemented in function ITSF_USER_LOGIN.
AVA_VLA.1	Developer vulnerability analysis	AM_AVA_VLA	The TOE vulnerability analysis addresses the requirements of AVA_VLA.1

8 REFERENCES

CC Common Criteria for Information Technology Security Evaluation, August 1999, Version 2.1, CCIMB-99-032

CEM Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation Methodology, Version 1.0, August 1999

ACP 127 ACP 127 NATO SUPP-3 (A) "Message Relay Procedures" "NATO Unclassified"