THALES

XOMAIL 21

SECURITY TARGET

Edition: **4-public**

08.05.2017

Previous editions:

1	**24 May 2016**
2	**07 Oct 2016**
3	**13 Jan 2017**
4	**02 May 2017**

Author: **CHTE**

Resp.: **ØYJ**

Appr.: **BRK**

All pages in this document shall have the same edition number

Foreword

This document is the Security Target for XOmail 21. The document describes the operating environment and IT product requirements, as well as security functionality implemented in the IT product.

The document was prepared on behalf of

Forsvarsmateriell IKT-kapasiteter
Postboks 800 Postmottak,
2617 Lillehammer
Norway

By:

THALES Norway AS
Postboks 744 Sentrum
0106 Oslo
Norway

Telephone: (+47) 22 63 83 00
Telefax: (+47) 22 63 83 01
E-Mail: mhs.norway@thalesgroup.com
Internet: http://www.thalesgroup.com

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. SCOPE OF DOCUMENT

This document is a Security Target for XOmail Server. The Security Target forms the basis for product security evaluation according to the Common Criteria for IT Security Evaluation (CC).

The document describes the security environment XOmail, including the list of threats met by XOmail and its environment, security objectives for XOmail, security functional requirements, and assurance requirements.

Rationale is provided for each of the identified security objectives, requirements and functions identified.

The assurance level for XOmail is EAL4 augmented with ALC_FLR.3.

2. RELATED DOCUMENTS

[1]	712 27734 AXAA EO	XOmail Installation and Configuration Guide
[2]	739 20529 ABAA EO	XOmail User's Guide
[3]	739 20561 ABAA EO	XOmail Administrator's Guide
[4]	ESD-TR-75-306	Bell & La Padula: Secure Computer Systems: *Unified Exposition and Multics Interpretation*.
[5]	FOR 2001-07-01 nr 744	Forskrift om informasjonssikkerhet, 1 July 2001, updated 1 July 2012. (Norwegian directives on information security).
[6]	CCMB-2012-09-001	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 1 (also known as part 1 of the ISO/IEC 15408 Evaluation Criteria).
[7]	CCMB-2012-09-002	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 2 (also known as part 2 of the ISO/IEC 15408 Evaluation Criteria).
[8]	CCMB-2012-09-003	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 revision 4, Part 3 (also known as part 3 of the ISO/IEC 15408 Evaluation Criteria).
[9]	C-M(2002)49	Security Within the North Atlantic Treaty Organisation (NATO), 17. June 2002.
[10]	LOV 1998-03-20 nr 10	Lov om forebyggende sikkerhetstjeneste (Norwegian Security Act)
[11]	STANAG 4406 Ed. 2	Military Message Handling System Edition 2, NATO C3 Board, 2005
[12]	RFC 2156	MIME Internet X.400 Enhanced Relay, January 1998
[13]	Open Group (X/Open)	API to Electronic Mail (X.400), Issue 3, May 1996
[14]	Open Group (X/Open)	OSI-Abstract-Data Manipulation API (XOM), Issue 3, May 1996
[15]	RFC 6477	Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail, January 2012
[16]	GP OSPP 3.9	Protection Profile for General-Purpose Operating Systems, version 3.9, NIAP and BSI, 15 January 2013.
[17]	GP OSPP 4.1	Protection Profile for General-Purpose Operating Systems, version 4.1, NIAP, 9 March 2016
[18]	NIST FIPS PUB 180-4	Secure Hash Standard (SHS), NIST, March 2012

Table 2-1: Related documents

3. TERMINOLOGY

3.1 Abbreviations and acronyms

ACL	Access Control List
ACP	Allied Communication Publication
ASN.1	Abstract Syntax Notation number One
B&L	Bell & La Padula Security model
CCIS	Command Control Information System
CM	Configuration Management
COTS	Commercial Off The Shelf
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
DAC	Discretionary Access Control
DoS	Denial Of Service
DMP	Direct Message Profile
HCL	Hierarchical Classification Level (e.g. RESTRICTED)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MHS	Message Handling System
MIP	Multilateral Interoperability Programme
ML	Multi-Level
MMHS	Military Message Handling System
MTA	Message Transfer Agent
NATO	North Atlantic Treaty Organization
NHC	Non-Hierarchical Category (e.g. CLEAR)
OS	Operating System
SA	Security Administrator
SFP	Security Functional Policy
SIC	Subject Indicator Code
SL	Single Level
SMTP	Simple Mail Transfer Protocol (RFC 5321)
SP	Security Policy
SS	Secure Storage
ST	Security Target
STANAG	NATO Standardization Agreement
TOE	Target of Evaluation (defined in chapter 4)

TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WAN	Wide Area Network
XOmail	The XOmail MMHS software product family, including Server, MailClient, TSClient, Admin Client, XOmail plugins to other software and supporting software.
XOmail Admin	Covers the XOmail Admin Client and XOmail TS Client. The Admin Client is used for configuring the server, while the TS Client is used by for inspecting and monitoring messaging traffic. The TS Client provides access to classified information related to message traffic, while the Admin Client is concerned with configuration data and audit.
XOmail Client	The XOmail Client provides end users with access to personal and formal message handling and supervision.
XOmail Server	The XOmail Server software

Table 3-1: Abbreviations and Acronyms

Admin Main Object	The main configurable objects of the system. These objects are visible in the top level of the administration client's navigation tree for a given Message Server.
Admin Object	Configurable objects of the system. These objects are identified with leaves in the static parts of the administration client's navigation tree.
Administrator	The least privileged administrator role. Can administer all parts of the TOE, except for the Network Management parts, security parameters and Security Administrator restricted User Templates. Administrator access can be further limited using Command Access parameters in the User Template.
Clearance	Each user is assigned a clearance indicating the maximum security classification of information the user is allowed to access.
Client computer	A computer running the XOmail Client, the XOmail TSClient and/or the XOmail Admin Client. The clients, the operating system and the computer hardware/firmware are not part of the TOE.
Command Access	ACLs for administrative commands. Access to each command can be controlled on a per User Template basis.
FLASH message	Informally: Covers messages with precedence levels FLASH and OVERRIDE. Time-critical military message that must be delivered and handled within defined time limits.
Message precedence	The military precedence level of a message conveys information from the originator to the recipient and is used by the TOE to automatically select the appropriate level of service.

MMHS Server	An MMHS Server is a deployed instance of the TOE, connected to a network. The MMHS Server consists of the TOE, the operating system, and the hardware platform. The XOmail Client, XOmail Admin, or API applications may be co-located on the same hardware, or access the TOE through the network. The MMHS Server may also be a virtual machine running on a hypervisor.
Network Administrator	Administrator with extended privileges compared to the Administrator role. This role has access to administration of Network Management parameters. Other than this, the same limitations are valid as for Administrator.
Normal	The ordinary user role. Users belonging to this role have no administrative access.
OS Root	The primary OS user for the TOE. This is a non-administrative user defined in the operating system as described in XOmail Installation and Configuration Guide [1].
Primary Security Administrator	The most privileged administrator role. Can administer all parts of the TOE. Command access limitations will not be applied.
Security Administrator	The most privileged administrator role. Can administer all parts of the TOE. Command access limitations can however be applied.
Security Attribute	CC definition: Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP. XOmail context: Subject and object HCLs, NHCs and SPs.
Single Level object	Object that is able to handle information at a single security label equal to its own security label.
Social engineering	The use of persuasion and/or deception to gain access to information systems.
Target of Evaluation (TOE)	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
Template	Upon creation all System Units are based on a template. The new System Unit remains associated with a template during its whole lifetime, and some attributes will remain pure template attributes. Templates must be created for Users, Departments, Message Servers and Directory Servers.
Trusted object	Object that is allowed to override security policies.
Trusted subject	Subject that is allowed to override security policies. The subject is allowed to handle information with different security labels.

Table 3-2: Terminology

4. ST INTRODUCTION (ASE_INT)

4.1 ST and TOE identification

ST title:	XOmail 21 Security Target
ST version:	See front page.
ST date:	See front page.
TOE name:	XOmail
TOE version:	XOmail 21.1.1
	Product id 712 27734 AFAA 50
Assurance level:	EAL4 augmented with ALC_FLR.3
CC Identification	Common Criteria for IT Security Evaluation Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

4.2 TOE Overview

XOmail is a family of turn-key products tailored for formal military messaging, information handling and transfer in modern C4ISR solutions.

The TOE is the XOmail Server, the main building block of the XOmail product family. The XOmail Server provides secure message handling, transfer, storage, and administration functionality.

The TOE can be deployed in the configurations below. Multiple configurations may be deployed to a single instance of the TOE.

- **Military Messaging**
  Dedicated to meet specific needs for military message handling in strategic and tactical networks.
- **Afloat**
  Functionality tailored for surface vessels and submarines.
- **Broadcaster**
  Broadcast, Ship-Shore and Maritime Rear Link through STANAG 4406, STANAG 5066 and ACP 127.
- **SMTP Gateway**
  Provides interoperability with MS Exchange and other mail systems.
- **ACP 127 Gateway**
  Automatic gateway between ACP 127 and STANAG 4406.
- **Central Archive**
  Assured automatic storage of all messages.

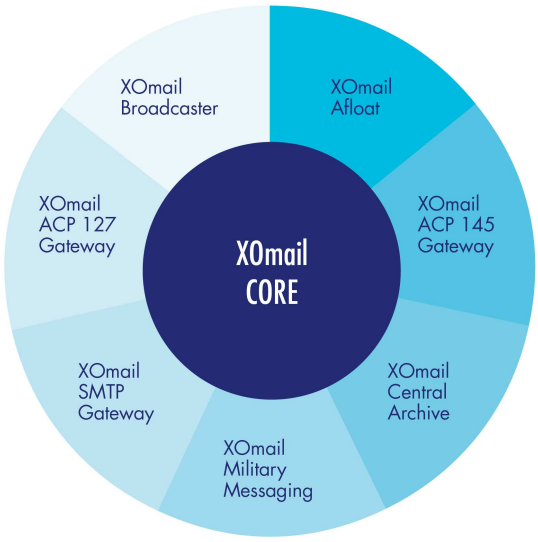

Figure 4-1 XOmail Server configurations, with a common security core.

- **ACP 145 Gateway**
  Implements NATO standard for connecting networks with different security policies and PKI implementations, allowing communication between nations and between national systems and NATO. Unlike the other components, the ACP 145 Gateway must be deployed on a separate instance of the TOE.

XOmail Admin (TOE Environment) is provided for local or remote administration of the XOmail Server (TOE). XOmail Admin provides the Admin Client for configuring the XOmail Server, and the TS Client for traffic monitoring and surveillance.

The XOmail Client (TOE Environment) provides the user interface to the different components of the XOmail Product Family.

4.2.1 Major security features of the TOE

The XOmail Server software (TOE) is built with multi-level security and mandatory access control for all message flows and stored information objects. The TOE provides priority handling for messaging, ensuring flash message traffic is delivered with minimal delay even with heavy traffic or congestion.

The TOE preserves message security through consistent interpretation of security labels across all supported messaging protocols, and supports use of digital signatures to ensure message integrity.

The TOE ensures all users are authenticated, and provides user management functions such as automated logout, lockout, and verification. The TOE provides fine grained access control for messaging operations and administrative commands, with complete accountability of all operations.

4.2.2 Required non-TOE hardware, software and firmware

The TOE runs on standard 64bit PC hardware.

The TOE supports the following operating systems:

Application	Operating systems
XOmail Server	Windows Server 2012 (CC Certified GPOS PP v3.9 [16]) Windows Server 2012 R2 (CC certified GPOS PP v4.1 [17])

Table 4-1: TOE Supported operating systems

Refer to the certification reports and the manufacturer's documentation for additional information.

The XOmail 21 Server software may also run on the following operating systems, but this configuration is not covered by the TOE.

Application	Operating systems
XOmail Server	Windows Server 2008 R2 Solaris 10 (x86-based PC and Sun UltraSPARC)

Table 4-2: Additional operating systems supported by XOmail Server

4.3 TOE Description

XOmail is leading in its ability to be deployed on both strategic as well as tactical low-bandwidth unreliable networks, in army, naval and joint systems, ranging from the troop and vehicle level, up to naval vessels and national and joint headquarters.

The XOmail product family has been developed in close cooperation with military customers in several countries, and has been continuously updated through more than 25 years of operational history.XOmail has been selected by several European NATO member countries for their nationwide messaging service, for NATO missions and NATO systems.

The backbone of XOmail is the implementation of the widely accepted NATO STANAG 4406 messaging standard, as well as seamless integration with legacy ACP 127 systems, tactical network protocols, and Internet Mail (SMTP) based systems.

The XOmail Server provides backbone messaging infrastructure, gateways and message storage. The TOE functionality can be extended through the use of APIs, which allow third-party applications access to the messaging infrastructure.

The TOE is accessed by user and administration clients, which provide user interfaces for messaging and day-to-day management. The clients are not part of the TOE.

4.3.1 The XOmail components

XOmail Server is available in multiple configurations, each of which is deployable as components of the XOmail product family. Each component contains a shared security core provided by the TOE. All components except the ACP 145 Gateway may be configured in parallel on a TOE installation.

4.3.1.1 Core Functionality

The TOE has the following main characteristics and functionality:

- Military messaging system built according to STANAG 4406 Ed. 1 and Ed. 2 military extensions.
- Multi-Level Security and Priority attributes embedded at every level of the system.
- Local and remote administration and supervision.
- A limited ACP133 Ed. D Directory Service and the ability to interact with an external master Directory Service or act as a standalone or intermediate Directory Service. Optimized tactical directory shadowing protocol for low-bandwidth unreliable networks.
- Supports antivirus integration
- Message integrity protection using S/MIME over STANAG 4406 Ed 2 and Internet Mail networks. Integration with third-party Public Key Infrastructures to support certificate validation, including revocation lists and validation of certificate chains.
- Support for automated installation
- Automated printing of messages.
- Clustering support for enhanced availability and reliability.

4.3.1.2 Military Messaging

This is the messaging component of the XOmail product family. It supports military messaging for strategic and tactical systems, with required features for security, military workflow, priority handling, STANAG 4406 Ed. 1 and Ed. 2 communications and gateways to other systems and networks.

Messaging functions are tailored to the needs of large organisations. The system differentiates strictly between official messages (to organisational departments and roles) and personal messages (to individual users).

Additional specialized functions:

- Advanced rule based message distribution mechanisms.
- SIC handling.
- Customer extensible through industry standard Application Program Interfaces, allowing access to the messaging services provided by the TOE.
- Basegram addressing
  Basegram addressing is used to provide an alternative recipient for an addressee that is currently unreachable or with limited bandwidth. A typical use of this function is to allow naval vessels to have low priority traffic delivered to a shore-side mailbox until a high bandwidth channel is available.
- P_mul gateway
  The P_mul protocol is designed for use in tactical limited bandwidth environments. The protocol is defined in STANAG 4406 Annex E. See also Section 4.3.9.4.
- DMP gateway
  DMP is an extremely low overhead protocol for use in tactical communications. The protocol is defined in STANAG 4406 Annex E. See also Section 4.3.9.3.
- MCCIS Gateway
  Support for the MCCIS protocol.
- X.25 protocol support
  The X.25 protocol is used to interface X.25-based networks or radio equipment.

4.3.1.3 XOmail Broadcaster

XOmail Broadcaster provides a modern and flexible solution to maritime messaging, while maintaining the ability to use legacy protocols and operating modes.

XOmail Broadcaster provides functions for handling Broadcast, Ship-Shore and Maritime Rear Link (MRL) circuits. XOmail Broadcaster supports both the modern STANAG 4406/5066 channels and legacy ACP 127 infrastructures.

XOmail Broadcaster is in full operational use in several countries and provides field-proven integration of BRASS and BRASS Enhancement One (EO) functions with national and NATO messaging systems.

The XOmail Broadcaster relays messages between domains connected via maritime communications and procedures. The Broadcaster provides additional system unit types for ACP127 communication, while using the ACP 127 Gateway for low-level communication. An overview of the XOmail Broadcaster is shown in Figure 4-2.

A number of Broadcast Units and Ship-Shore Units can be defined on an XOmail Maritime Gateway.

The Broadcast Unit handles the transmission (broadcast) of messages to ships. The Ship-Shore Unit handles incoming messages from ships. Thus, two-way connectivity requires at least one Broadcast and one Ship-Shore Unit to be defined.

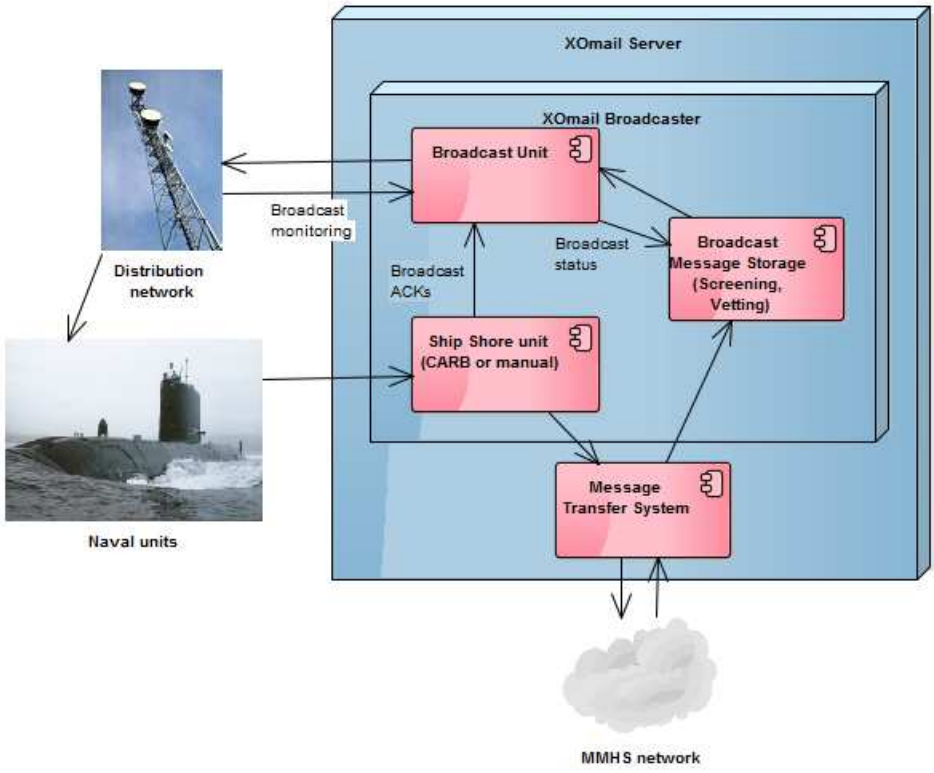

Figure 4-2: XOmail Broadcaster

Broadcast Unit:

The system offers two filtering functions for reducing broadcast load:

- **Screening**
  All messages are subject to automatic screening. Expired messages are discarded and suspected duplicates are halted.

- **Vetting**
  Messages may be stopped for manual review to determine the relevance in the current situation.

Other special Broadcast Unit functions include:

- **Broadcast Schedules**
  Ships may maintain reduced radio watch. A broadcast schedule can be established to ensure that messages are only sent during watch hours. Broadcast schedules can also be used for sharing a broadcaster, e.g. by allowing certain types of traffic (such as NATO only) during certain periods of the day.

- **Automatic Re-runs**
  To ensure that all called stations will receive a message, transmission re-runs can be defined.

- **Traffic List generation**
  Broadcast Units log all broadcasted messages in Traffic Lists. The ship side uses these Traffic Lists to determine whether all broadcast messages are received or not.

Ship-Shore Unit:

A Ship-Shore Unit handles incoming messages from ships. In addition, a Ship-Shore Unit provides functionality for automatic and manual aerial switching as well as reception quality assessment and control. A number of Ship-Shore Units can be defined on one XOmail Maritime Gateway.

The ship uses Working Channels for sending messages to the Maritime Gateway. A channel link must be established before a message can be sent. Channel establishment is either performed automatically using CARB procedures, or manually by an operator. In addition, an Aerial Select Channel can be used for directing/controlling the antenna used for receiving messages from ships.

The Maritime Gateway module can be selected during installation of the XOmail Server. The Maritime Gateway does not need to be installed unless the broadcast/ship-shore functionality is required. The base ACP 127 functionality is not affected by this module.

4.3.1.4 XOmail Afloat

XOmail Afloat is a Military Message Handling System (MMHS) tailored for surface and sub-surface (submarine) naval vessels. XOmail Afloat provides Broadcast reception, Ship-Shore transmission, Inter-Ship traffic and re-Broadcast. XOmail Afloat integrates with existing ACP 127 and STANAG 4406 infrastructures.

XOmail Afloat increases overall combat effectiveness through automated message handling and integration with command and control systems.

The Afloat Ship-Shore unit provides detailed control over message transmission and channel utilization on ships.

- **Ship channel handling**
  ACP 127 channel administration, including monitoring of ACP 127 channels for broadcasters, cryptographic device support with communications keying and crypto synchronization. Automated and manual control over message retransmissions.

- **Transmission Pool**
  Afloat messaging often requires strict control over communication means. The transmission pool allows authorized operators detailed control over messages being transmitted.

- **CARB on ships**
  XOmail automates execution of CARB procedures on the ship side when transmitting ACP127 messages from ship to shore, thereby reducing the operator work load.

- **Ship-to-ship communication**
  XOmail provides formal and free text ship-to-ship messaging over ACP 127 channels.

4.3.1.5 XOmail ACP 145 Gateway

XOmail ACP 145 Gateway interconnects both national messaging systems and the NATO messaging system. The Gateway connects networks with different security policies in the strategic domain and in multilateral operations. The XOmail ACP 145 Gateway provides nations with complete flexibility in terms of national messaging implementation. This is achieved by having national-specific gateway functions on one side and ACP 145 specific functions on the other.

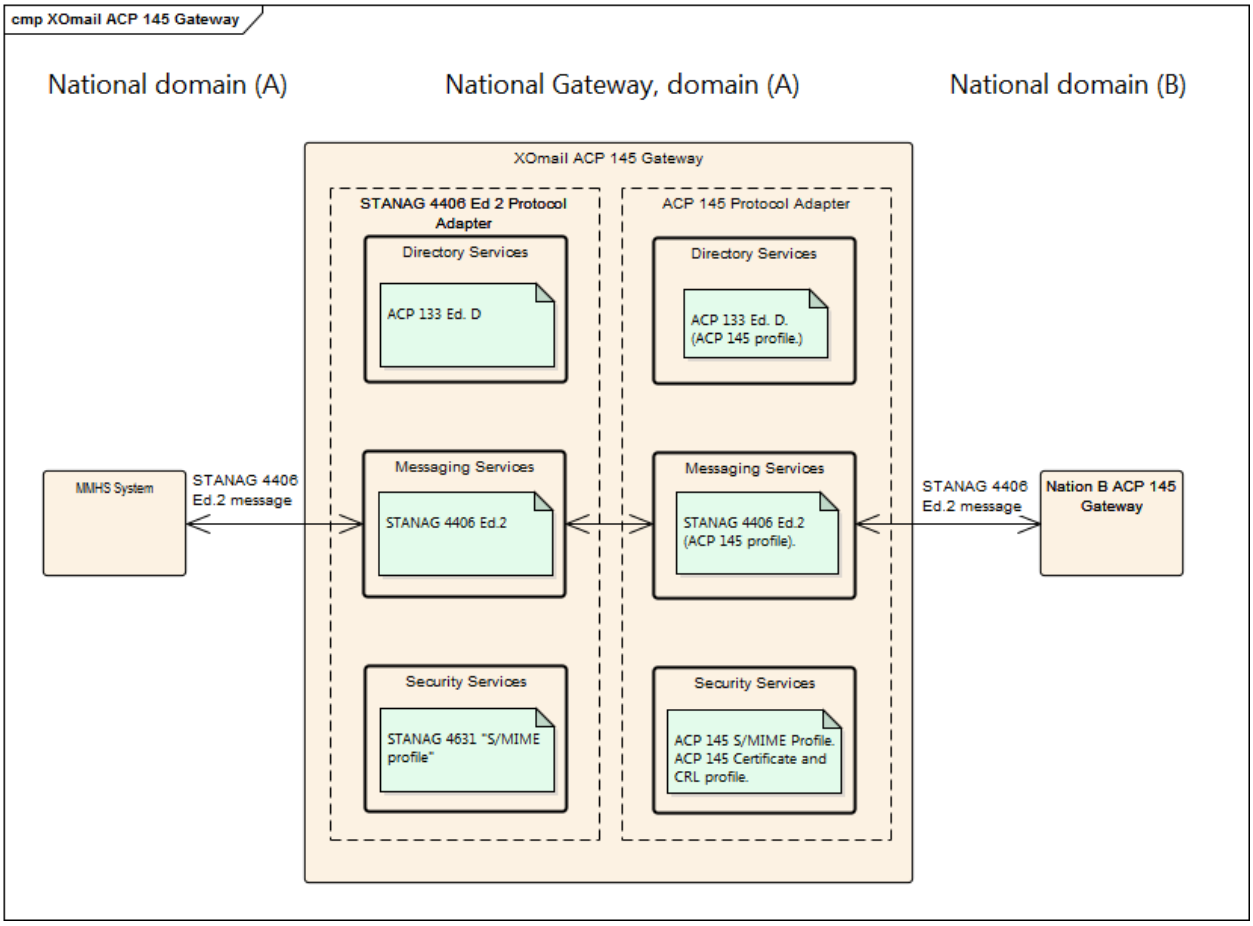

Figure 4-3 XOmail ACP 145 Gateway overview

4.3.1.6 XOmail SMTP Gateway

XOmail SMTP Gateway offers seamless integration of messaging systems and is crucial to effective information flow in modern military and governmental organisations, as well as towards international partners and non-governmental organisations. XOmail SMTP Gateway provides interoperability with modern and legacy military messaging systems as well as Microsoft Exchange and other email systems. The system also provides a bridge between MMHS and military SMTP-based products, like Battle-Force Email.

The SMTP Gateway allows a wide range of SMTP-based messaging applications to be integrated into a military messaging infrastructure. XOmail SMTP Gateway can be configured to map all STANAG 4406 protocol elements into SMTP X-fields. Hence, the gateway can provide alternative routes for military messaging through an SMTP network. See also Section 4.3.9.

The SMTP Gateway also provides a limited IMAP4 server for basic person to person messaging using civilian E-mail clients such as Microsoft Outlook.

4.3.1.7 XOmail ACP 127 Gateway

XOmail ACP 127 Gateway provides interoperability with legacy ACP 127 systems and allows the step-wise deployment of a modern STANAG 4406 system. ACP 127 Gateway is implemented according to

"ACP 127 NATO SUPP-3 (A)" and STANAG 4406 Annex D, extended with automated functions that greatly reduce the need for manual interactions.

The XOmail ACP 127 Gateway is normally configured standalone, on a dedicated installation of XOmail Server, but the ACP 127 Gateway may also be operated with other XOmail components on the same XOmail Server instance.

Detailed features:

- Connects to networks such as AIFS and teleprinters
- Supports use of multiple channels to a single destination to increase throughput.
- Logging of traffic into Channel List logs
- Automated procedures for important Abbreviated SVCs
- Automatic sectioning and de-sectioning of long messages.
- Syntax checking and Security Label conversions.
- Surveillance functions.

4.3.1.8 XOmail Central Archive

XOmail Central Archive provides functionality for storing all messages within a system, in one central location. The archive provides long-term storage of messages and powerful mechanisms that allow authorised users to search and retrieve archived messages. The typical use of the Central Archive is to archive all messages that originate within the system, along with all messages received from external systems via gateways. Optionally, filtering mechanisms can limit the number of messages to be archived.

Metadata for the archived messages are stored in an SQL database for improved search performance. Oracle and PostgreSQL are currently supported. The TOE handles access control for search and retrieval.

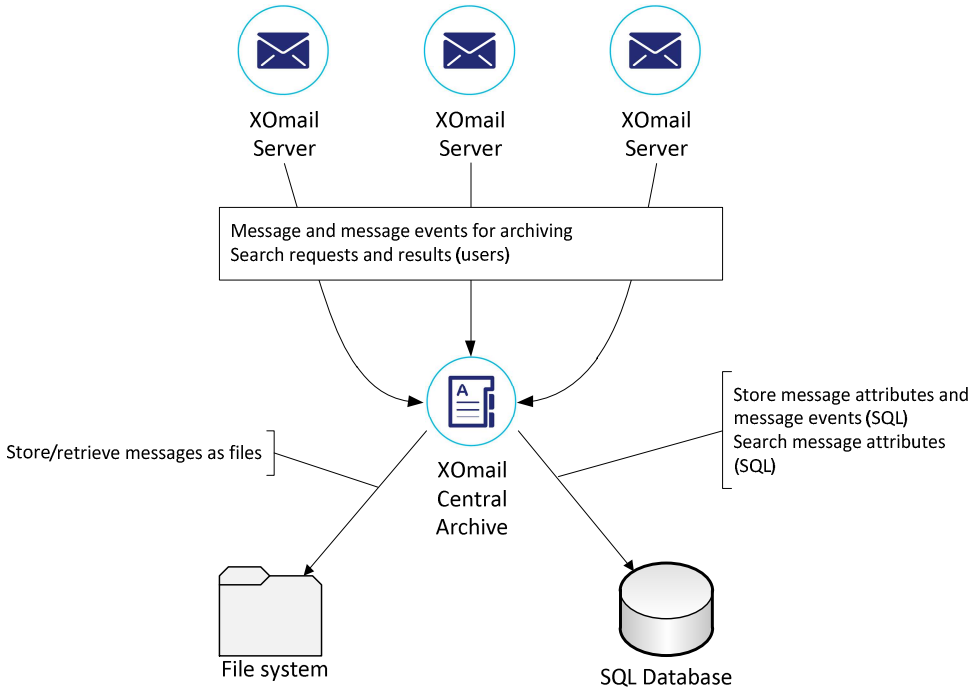

Figure 4-4 Central Archive system context

4.3.2 The XOmail Clients

In addition to the TOE, XOmail provides the clients listed below. The clients are used to access the TOE.

- XOmail Client
  End-user messaging client
- XOmail Admin Client
  Administrative interface
- XOmail Transit Storage Client
  Traffic operator interface

The XOmail Admin Client and XOmail Transit Storage Client may be installed separately or as a single application.

4.3.3 Non-TOE XOmail functionality

The function below is also provided by the XOmail Server, but shall not be used in a certified configuration. The function is contained in a package that must be explicitly enabled during installation.

- POP3 client access
  XOmail provides experimental support for the POP3 protocol.

Also note that the following client is part of the XOmail product family, but is not part of the TOE and only indirectly interfaces the TOE:

- XOmail Sign & Label Add-In for Outlook
  The Sign & Label Add-In for Outlook provides support for STANAG 4406 Ed 2 compatible security labels and S/MIME digital signatures. The Add-In is intended for use in SMTP-based networks that interface MMHS networks via an XOmail SMTP Gateway, and is not directly connected to the XOmail Server.

4.3.4 TOE deployment in a Multi-Level Security configuration

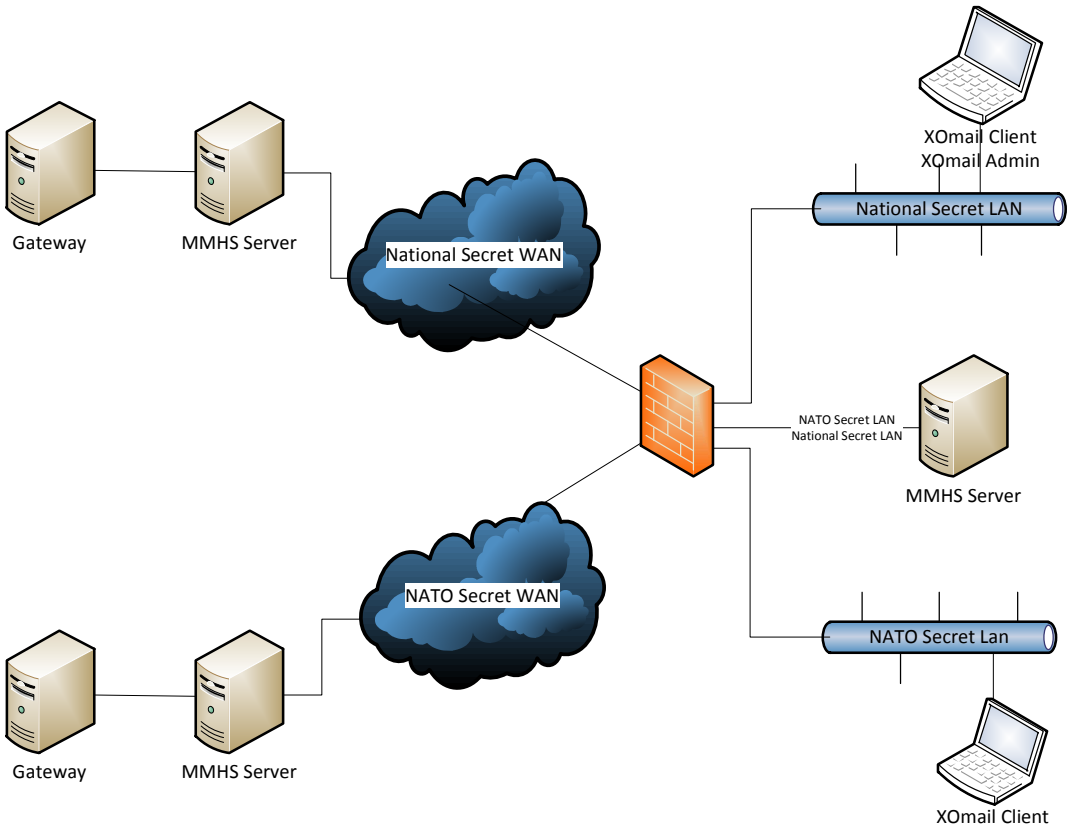

Figure 4-5: MMHS Servers in a Partitioned Operation Mode system

Figure 4-5 shows a general overview of the Partitioned Operation-Mode.

The MMHS Server running XOmail Server may also run XOmail Client, the XOmail TSClient and/or the XOmail Admin Client.

The XOmail Server may serve client logons from both the National Secret LAN and the NATO Secret LAN. In addition it is able to communicate with the MMHS Servers located in the WANs. XOmail Server may also exchange messages with third party MMHS Servers that are present. XOmail Server is able to separate information classified in the different security policies.

In the Figure 4-5 scenario, the firewall has been configured to allow connections to XOmail from both the National Secret LAN and the NATO Secret LAN, and Administrators from the National Secret LAN. XOmail may be configured to allow some users to connect only from the National Secret LAN, while others may connect from both.

Figure 4-6 shows a generalized version of Figure 4-5, with MMHS Servers operating in a multi-level security environment. This scenario shows the XOmail Server in two different roles, as security gateway (the server marked MLS), and as individual MMHS Servers.

The security gateway ensures that only messages labelled *restricted* or lower may pass between the two networks. Messages marked *secret,* or higher, are blocked

- when sent from the *secret* network, and
- when sent from the *restricted* network.

The first rule preserves confidentiality, while the second rule ensures that an attacker cannot inject incorrectly labelled *secret* messages into the *secret* LAN from the less trusted LAN. These rules are configurable.

Messages may be marked with additional categories (caveats), such as *national eyes only*. A *national restricted* LAN may exchange messages with a *NATO restricted* LAN, using the XOmail Server to ensure that *national eyes only* messages do not propagate outside the national network.

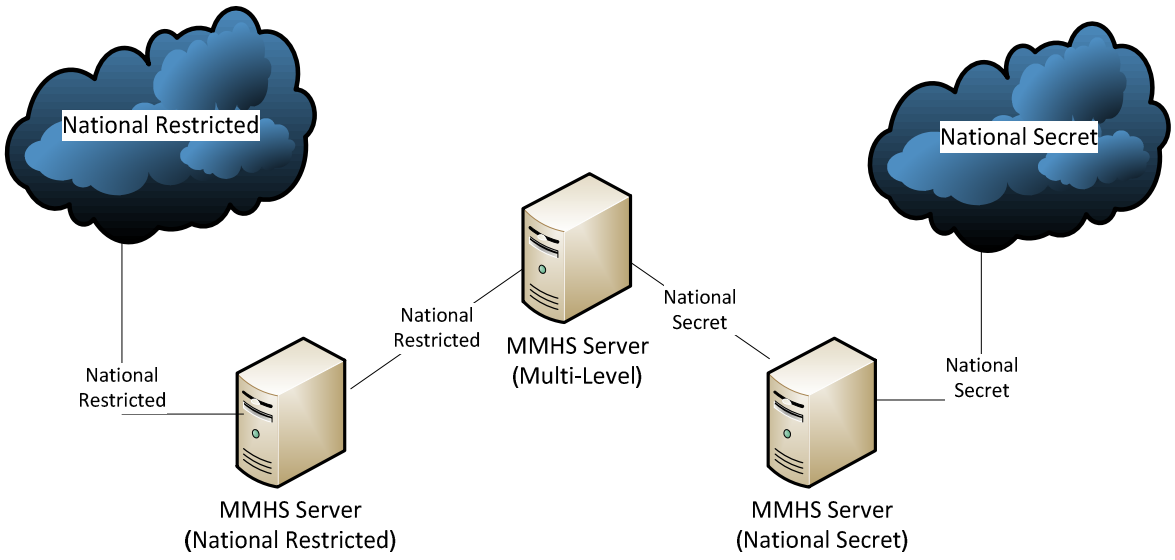

Figure 4-6: XOmail servers in different roles in an MLS environment

XOmail also supports the use of the RELEASABLE TO caveat, allowing specific messages to be marked *releasable to* additional security domains than the originating policy. Typical use is sharing of information to coalition and mission partners. Example: NATO CONFIDENTIAL REL TO SWE.

4.3.5 TOE External Interfaces

The Military Messaging component of the XOmail Server implements a STANAG 4406 compliant MMHS system, compatible with STANAG 4406 Ed1 and STANAG 4406 Ed2 systems.

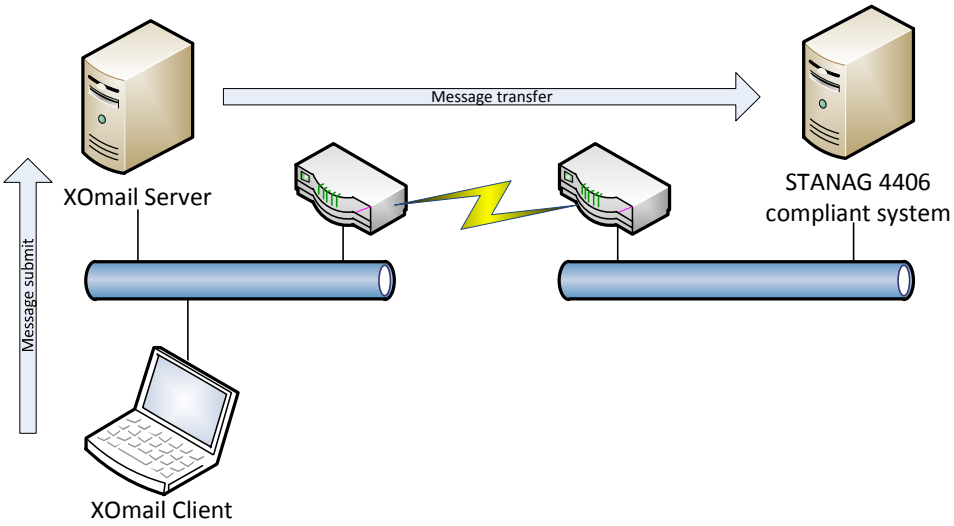

Figure 4-7 STANAG 4406 messaging

The TOE is highly adaptable, and may support a wide range of communication channels, ranging from unreliable tactical HF networks, to gigabit Ethernet.

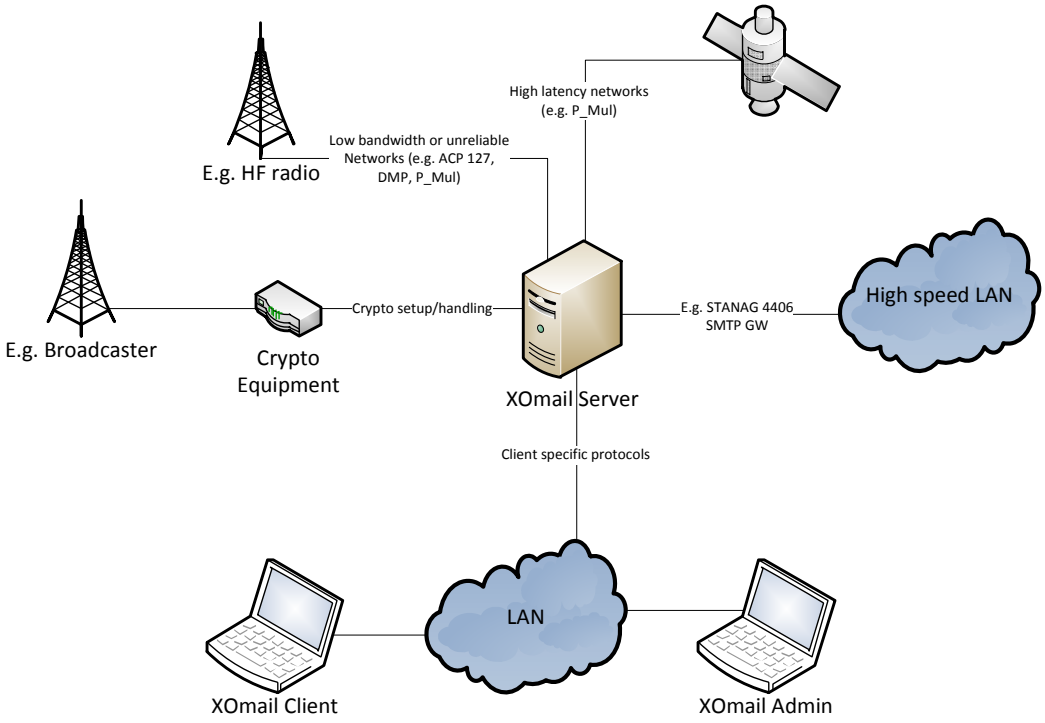

Figure 4-8 XOmail Server supported networks

It is assumed that the TOE Environment provides sufficient protection of the communication channels used by the TOE. This may include physical protection or use of approved cryptographic equipment.

4.3.6 Client interfaces

Logons to be handled by the XOmail Server are Administration Client logons, Transit Storage Client logons and Mail Client logons.

It is possible to configure the server to only allow Mail Client logons from a set of specific hosts, from a set of specific subnets, or from any host.

The XOmail Client is considered a *dumb client* that:

- Is available for all personnel that have user accounts (given that the account has not been locked).
- Is limited to accessing only the information allowed by the server. The server applies Mandatory Access Control and Discretionary Access Control to enforce confidentiality of information, based on the active user's security clearance and storage access. The client presents the security label that is associated with the displayed information.
- Sends requests to the server in order to store, retrieve, delete or create data. The server verifies that the operation is allowed for that user in his/her current environment.

The XOmail Client supports labelling of information upon presentation, but the label is always retrieved from the Server, or from the user that creates the data.

The TSClient is a *thin client* that:

- Is available for all personnel that have appropriate administrative rights (given that the user account has not been locked). See 4.3.6.1 for details on how administrative rights are assigned.
- Is limited to accessing only the information allowed by the server. The server applies Mandatory Access Control and Discretionary Access Control to enforce confidentiality of information, based on the active user's security clearance and storage access.
- Presents both unclassified and classified information. The server always controls the classification as it associates a label with all information that is sent to the TSClient.
- Hides commands the administrator is not authorized to use, based on "command access" and "administrator roles".
- Sends requests to the server in order to retrieve, delete or create data. The server verifies that the operation is allowed for that user in his/her current environment.

The Admin Client is a *thin client* that:

- Is available for all personnel that have appropriate administrative rights (given that the user account has not been locked). See 4.3.6.1 for details on how administrative rights are assigned.
- Presents only the XOmail configuration data that the server allows it to present. The server ensures this by not sending data that the client is not allowed to present.
- Does not present message data.
- Hides commands the administrator is not authorized to use, based on "command access" and "administrator roles".

- Sends requests to the server in order to store, retrieve, delete or create data. The server verifies that the operation is allowed for that user in his/her current environment.

To ensure information integrity and confidentiality, all traffic between the TOE and the clients must be protected from tampering and monitoring. This can be solved using network encryption or physical protection.

Messaging traffic (XOmail Client, XOmail Admin Client) should be separated from administrative traffic (XOmail Admin). This can be solved through physical separation or encryption.

The XOmail Admin Client and XOmail TSClient may optionally be installed as an integrated package. This allows an operator to inspect message traffic and perform configuration from a single application. The choice of configuration should be decided according on local security policy.

4.3.6.1 Administrator access control

There are four administrator roles in XOmail: Administrator, Network Administrator, Security Administrator and Primary Security Administrator. Only administrators have access to the Admin Client and the TSClient.

An administrator's User Template defines the set of commands available to all administrators based on that template. The command ACL grants and denies access to commands available in every command group, e.g. it is possible to grant read only access the "Department Template" command group, while denying access to New, Save and Delete operations.

The maximum command access that is possible to configure for any given User Template is determined from the administrator role that is set for the User Template. E.g. it will only be possible to grant access to network management tasks to Network Administrators and Security Administrators.

Only Security Administrators and the Primary Security Administrator are allowed to modify security parameters, e.g. user clearance and command ACLs.

4.3.7 XOmail Server

Logical interface	Description
MMHS Servers XOmail Client	Messaging operations • Message property mapping. • Encode/decode according to protocol definitions (e.g. STANAG 4406, Internet Mail) • Access control • Label conversion • Association management • Message integrity and authentication
ACP 127 channels	Message transfer • Encode/decode according to channel data definitions • Label conversion
XOmail Admin	Configuration, management and supervision • Encode/decode according to protocol definitions • One-way label conversion
File	Persistent storage of configuration and messaging data and metadata.

	• Label conversion • Encode/decode according to format
ACP 133 channels (Address Directory)	Directory services • Association management • Access control • Encode/decode according to ASN.1 definitions
Printers	Message printing, audit log printing • Encode/decode for printout • Label conversion • Access control
Third party LDAP clients	Directory browsing • Encode/decode according to protocol • Address information only
Third party Internet Mail clients via SMTP+IMAP4 (e.g. Outlook)	Message handling • Encode/decode according to protocol • Label conversion
ICAP (Antivirus)	Transfer messages to an antivirus server. • Encode/decode according to protocol definitions • Decode status codes from antivirus scanner
SCOM Windows Event Log	Audit export • Encode/decode according to protocol
Application Programming Interfaces (ch 4.3.8)	Message transfer, message operations, export from Central Archive • Encode/decode according to API definition • Label conversion • Access control •

Table 4-3: XOmail Server interfaces

Table 4-3 shows the logical interfaces for information flow on the XOmail Server. Each session may use multiple interfaces simultaneously. The figure shows that classified information and possibly other TOE assets may be transported on all these interfaces. It should be noted that there is not a one-to-one relationship between logical interfaces and actual XOmail Server interfaces. The logical interfaces shown in the table are a result of assumed function and the expected use.

The TOE can be configured to trust the security attributes associated with the incoming information. Otherwise, all such information will be classified with a configurable maximum value (system high).

The figure also shows important security functionality that is implemented in the logical interfaces, in addition to the encoding that is most commonly used on the interfaces.

APIs are described in ch 4.3.8.

4.3.7.1 XOmail Server security

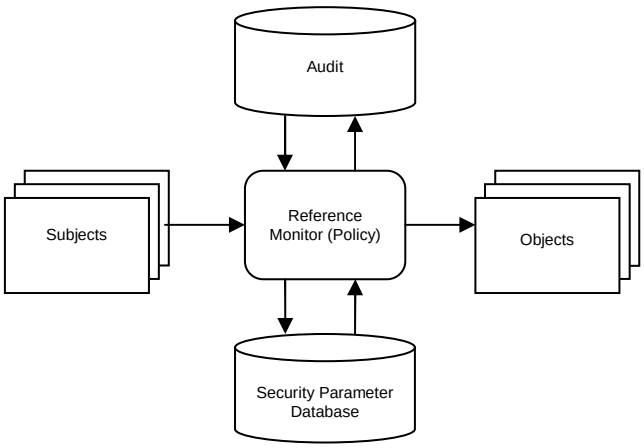

Figure 4-9: XOmail Server Reference Monitor

The core security functions of the XOmail Server are realized in a reference monitor. The reference monitor is tamperproof and it is always invoked when subjects request access to objects. A schematic overview of the reference monitor is shown in Figure 4-9.

All information conveyed between internal TOE components are labelled with a security label and a priority. The security label is used for access control by the reference monitor, based on the Bell & LaPadula multilevel security policy model [4]. The priority attribute ensures that higher priority messages are always given precedence in queues or assigned reserved resources.

Other security mechanisms, as described in Section 10.1, are located in separate software processes. Each security function may be included in several software processes if implemented as a library.

4.3.7.2 OS responsibilities

The TOE relies on authentication mechanisms provided by the Operating System. The responsibility of the TOE is to ensure that authentication is performed before any other operation. The Operating System is responsible for performing the actual authentication and to provide secure storage of the authentication tokens.

The TOE relies on the Operating System to provide an API to the cryptographic functions and Public Key Infrastructure required for S/MIME digital signatures. The TOE depends on the Windows Crypto API (CAPI) standardised interface to third party PKI components:

- X.509 certificate lookup
- X.509 certificate chain validation
- Secure use of cryptographic tokens (private keys).

The TOE does not store cryptographic tokens for S/MIME messaging, but relies on accessing the tokens through the Crypto API. The TOE Environment must ensure appropriate secure storage of cryptographic tokens, e.g. in the CAPI database, on smart cards or HSMs.

4.3.8 API framework

XOmail provides a standard API defined by X/Open for accessing the messaging infrastructure [13-14], i.e. API to Electronic Mail (MA-API).

Additionally, XOmail provides the XOmail Simplified API (XOsapi), based on MA-API, for a simplified, easy-to-use interface to the send and the receive functionality of the XOmail Server.

On computers not running XOmail Server, the XOmail RemoteAccess is installed to provide a low level communication stack which handles communication towards a remote XOmail Server.

The SMTP Gateway may also be used as a messaging API.

XOmail Central Archive supports export of messages in PDF format. This provides seamless export to customer specific archives or communication journals. This is a local API, accessed using a C++ library functions (DLL).

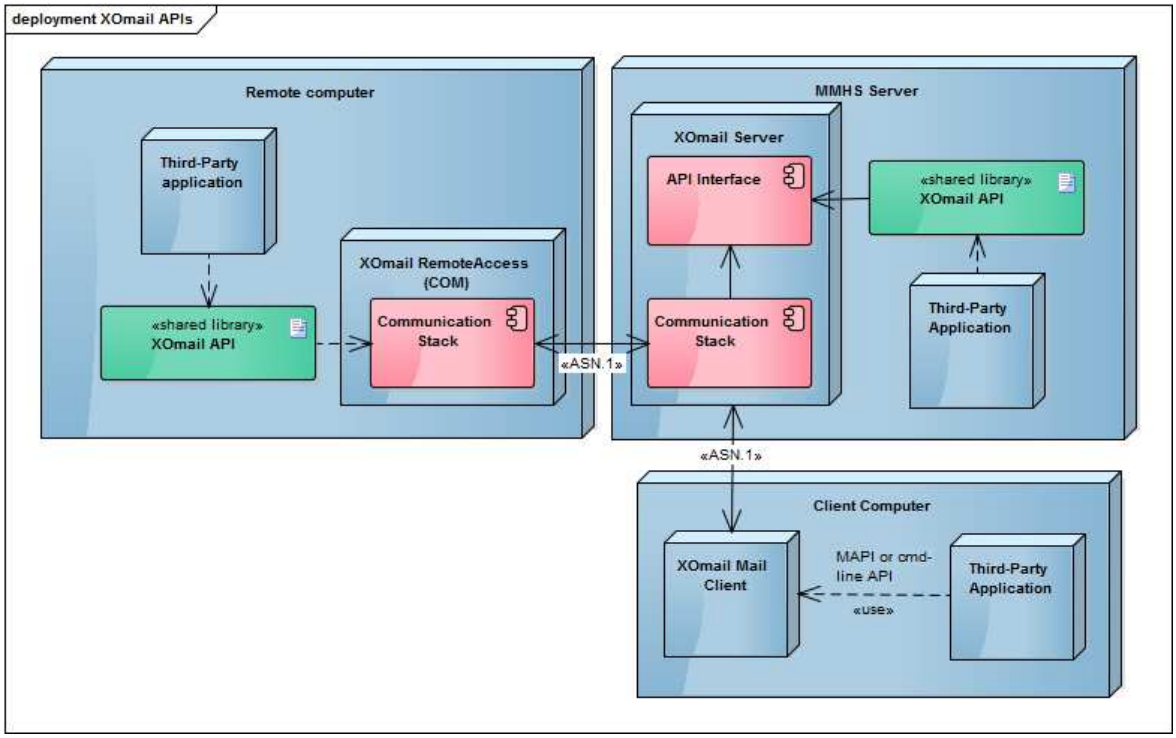

Figure 4-10: XOmail API framework

4.3.9 Gateways

4.3.9.1 SMTP Gateway

The SMTP gateway connects Internet Mail-based systems with MMHS and tactical networks, with conversion according to the MIXER guidelines [12].

The SMTP Gateway can be connected to commercial off the shelf SMTP-based email systems, as well as Battle-Force Email products implementing the SMTP protocol.

The SMTP Gateway also supports the SMTP based MIP Message Exchange Mechanism. MIP messages are received through an SMTP server which accepts messages on the Internet Mail Format with MIP extensions.

To support MMHS functionality inside the SMTP domain, the SMTP gateway implements MMHS attributes as Internet Message Format extensions according to RFC 6477 [15]. The Internet Message Format and SMTP protocol does not have native support for message security labels and other MMHS attributes. No automated handling based on these attributes can be expected, but the information can still be transported across SMTP networks.

MMHS attributes may be exported as a human readable text attachment inside the Internet Message domain, to allow users of standard email clients like Microsoft Outlook and Mozilla Thunderbird the ability to easily access these attributes.

The SMTP gateway must be enabled during installation of the XOmail Server. If the server is not going to communicate with remote servers using the SMTP protocol, or receive message submissions from Internet Email clients, this module does not need to be installed.

4.3.9.2 ACP 127 Gateway

The ACP 127 Gateway is described in 4.3.1.7.

The component is selected during installation of the XOmail Server. If the server is not going to communicate with remote servers using the ACP 127 protocol, this component does not need to be installed.

4.3.9.3 DMP gateway

The DMP gateway allows messages to be sent and received through the DMP protocol defined in STANAG 4406 Annex E. DMP is an ultra-low overhead messaging protocol for use in unreliable, limited and high-latency channels such as HF radio.

To save bandwidth only critical messaging attributes are transported. Other attributes are either reconstructed on the receiving side or discarded.

The module is selected during installation of the XOmail Server. If the server is not going to communicate with remote servers using the DMP protocol, this module does not need to be installed.

4.3.9.4 P_Mul gateway

The P_MUL protocol (ACP 142) provides a connection-less and bandwidth-optimized channel for transporting STANAG 4406 messages. It is designed for unreliable networks (e.g. radio links) with reduced bandwidth and high latency. P_MUL has a higher overhead than the DMP protocol, but supports all of the STANAG 4406 attributes.

P_MUL is defined in STANAG 4406 Annex E.

The module is selected during installation of the XOmail Server. If the server is not going to communicate with remote servers using the P_Mul protocol, this module does not need to be installed.

4.3.10 S/MIME Security Services

The XOmail Server provides the ability to ensure the integrity of MMHS messages transmitted between servers through use of S/MIME digital signatures. These signatures are limited to STANAG 4406 Ed2 messages and messages over the SMTP Gateway.

The XOmail Server relies on the Cryptographic API (CAPI) in Windows to provide cryptographic functions, X.509 certificate validation, certificate path validation and revocation checks.

The TOE does not store or manage cryptographic keys, and does not generate message signatures. The TOE initiates these cryptographic operations through cryptographic APIs provided by the operating system.

The XOmail Server implements cryptographic hash functions to generate the message digests used for S/MIME operations. The TOE Environment operates on message digests rather than the actual message payloads. This reduces the risk for disclosure or modification of classified information.

5. CONFORMANCE CLAIMS (ASE_CCL)

The Security Target and TOE conforms to the Common Criteria for Information Technology Security Evaluation standard, version 3.1 revision 4, dated September 2012, parts 2 and 3.

The Security Target does not claim conformance to a Protection Profile.

Part 2 conformant, with the Security Functional Requirements included below. The Security Target does not declare extended security requirements.

Part 3 conformant to EAL 4 augmented with ALC_FLR.3.

6. SECURITY PROBLEM DEFINITION (ASE_SPD)

In the following sub-chapters the TOE security problem definition will be described.

First, a list of assets and threat agents are described. These lists support identification of the threats to be countered by the TOE. The assets in the system are objects for which the TOE shall ensure confidentiality, integrity and availability, whereas threat agents are the subjects that may perform actions later identified as threats.

Based on the operating environment, the list of threat agents and the TOE itself (including assets), a list of threats can be identified. The identified threats are listed in 6.3. All threats are listed with a description of the threat, the involved threat agents, the affected assets and a description of unwanted outcome from a possible attack. In 6.4, the organisational security policy with which the TOE must comply is described.

Last, a list of assumptions regarding the TOE use and its operating environment is given. It is important to note that the operating environment is essential for ensuring parts of the TOE security functionality. This is further described in each assumption.

6.1 Assets

AS.AUDIT	The log data gathered by the TOE and OS that are part of the audit trail.
AS.AUTH_DATA	Authentication credentials supplied from a subject to the TOE.
AS.CLASSIFIED_INFO	Information classified according to a specific security policy. The information is assigned a hierarchical classification level (HCL) and optionally a set of non-hierarchical categories (NHC).
AS.CONFIG_EXT	TOE configuration data that is stored within the control of the OS. This includes configuration files for which the OS controls the access.
AS.CONFIG_SS	TOE configuration data that is stored in the SS, except that covered by AS.SEC_CFG.
AS.PROPER_OP	Proper operation of the TOE is considered an asset as it is important for authorized users to get access to the system as needed.
AS.SEC_CFG	TOE security configuration. This includes - clearance settings for users and departments, - clearance settings and other security settings for external channels used by the TOE, - labelling of structures within SS, - ACLs for structures within SS,

6.2 Threat agents

TA.ADM	Authenticated authorized administrators of XOmail. These threat agents may unintentionally perform unauthorized actions. Administrators that have not authenticated, or perform actions from applications other than the Admin Client or the TSClient are considered TA.INTERNAL.
TA.DEVELOPER	The TOE developer may unintentionally compromise the TOE security.

TA.EXTERNAL	Personnel with no authorized access to the TOE environment. These threat agents may attempt to gain access to classified information and may have “unlimited” resources supporting them.
TA.INTERNAL	Personnel with authorized access to the TOE environment. These threat agents may try to perform unauthorized actions. Furthermore, such threat agents may be specially trained to perform the unauthorized actions and may have “unlimited” resources supporting them.
TA.SYSTEM_ERROR	Hardware or software failures or transmission errors may cause information to be modified, injected or deleted by accident.
TA.USER	Authenticated authorized users of the TOE. These threat agents may intentionally or unintentionally perform unauthorized actions. Users that have not authenticated, or perform actions from applications other than the MailClient are considered TA.INTERNAL.

6.3 Threats

The threats are divided into two groups based on who meets them. The first group, named TT, is comprised by the threats met by the TOE itself. The second group, named TE, is comprised by the threats met by the TOE environment.

6.3.1 Threats met by the TOE

TT.ADM_ERROR	Improper administration results in a security policy violation.
Threat agents	TA.ADM.
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_SS, AS.SEC_CFG.
Unwanted outcome	Unauthorized personnel get access to, change, or delete classified information because of unintentional improper administration of the TOE.

TT.AUDIT_FAILURE	An attacker may cause audit records to be lost or modified. Attackers may also cause audit overflow, so that important audit records seemingly disappear.
Threat agents	TA.INTERNAL, TA.EXTERNAL
Asset	AS.AUDIT
Unwanted outcome	The TOE is unable to store audit data or provide necessary audit data to the IT environment, or the audit becomes useless because of the inability to separate important audit records from other records. The latter is the case if the audit is overflowed.

TT.COM_INTEGRITY	The integrity of transmitted information may be compromised due to deliberate or accidental insertion or modification. New information may be inserted onto the network, or existing traffic modified in transit. An attacker may modify the security label, priority, recipients, originators or other attributes of the message and its data.
Threat agents	TA.INTERNAL, TA.EXTERNAL, TA.SYSTEM_ERROR
Asset	AS.CLASSIFIED_INFO
Unwanted outcome	Invalid or forged information is mistakenly trusted. Classified information is modified or new information is generated.

TT.DOS	An attacker may cause system resource exhaustion, resulting in delayed message handling or the inability of authorized users to access system resources. Valid message traffic may also cause denial of service conditions when high traffic conditions cause system resources to be exhausted.
Threat agents	TA.USER, TA.INTERNAL, TA.EXTERNAL
Asset	AS.PROPER_OP
Unwanted outcome	Authorized users are prevented from using the system or system performance is degraded. High priority message traffic is queued.

TT.FAULTS	The TOE crashes or deadlocks due to software or hardware errors.
Threat agents	TA.DEVELOPER, TA.SYSTEM_ERROR
Asset	AS.PROPER_OP
Unwanted outcome	Authorized users are prevented from accessing the TOE.

TT.MASQUERADE	An attacker tries to masquerade as a trusted entity in order to by mistake be trusted with classified information.
Threat agents	TA.INTERNAL, TA.EXTERNAL
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_SS, AS.SEC_CFG
Unwanted outcome	Classified information is sent/made available to an entity that is not authorized for the data.

TT.MONITORING	An attacker monitors activities and actions performed on classified information. Such activities and actions include authentication and creating, viewing, modifying and deleting classified information. The monitoring activities can be performed at multiple levels, like screen monitoring or network monitoring.
Threat agents	TA.INTERNAL, TA.EXTERNAL
Asset	AS.CLASSIFIED_INFO, AS.AUTH_DATA
Unwanted outcome	Based on the monitoring activities, attackers can make assumptions of the type of information sent, and possibly even the content of the information sent. Statistical methods can be used to make such assumptions. Also determining normal traffic load, and possible divergence from this can give attackers valuable information. Possibly, the attacker can draw conclusions that would be considered classified information based on traffical patterns.

TT.REPLAY	A malicious process or user gains access by replaying authentication data.
Threat agents	TA.INTERNAL, TA.EXTERNAL
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_SS, AS.SEC_CFG
Unwanted outcome	Unauthorized personnel get access to classified information by replaying the authentication data provided by an authorized user or administrator.

TT.UNATTENDED	A malicious user may gain unauthorized access to an unattended session.
Threat agents	TA.ADM, TA.USER and TA.INTERNAL
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_SS, AS.SEC_CFG
Unwanted outcome	Unauthorized personnel get access to the specified assets.

TT.UNAUTH_ACCESS	Unauthorized access to identified assets may occur. Methods of attack covered by this threat are brute force attacks, session hijacking, authentication data cracking, privilege escalation and social engineering.
Threat agents	TA.ADM, TA.USER, TA.INTERNAL and TA.EXTERNAL
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_SS, AS.SEC_CFG
Unwanted outcome	Unauthorized personnel get access to classified information.

6.3.2 Threats met by the TOE environment

TE.AUDIT_FAILURE An attacker may cause audit records to be lost or modified.

Threat agents	TA.INTERNAL, TA.EXTERNAL
Asset	AS.AUDIT
Unwanted outcome	Audit records are prevented from being recorded, or an attacker is able to alter the information before it is placed in the audit trail.

TE.DELIVERY An attacker may try to replace parts (or the complete) TOE with a malicious version.

Threat agents	TA.INTERNAL, TA.EXTERNAL.
Asset	AS.AUDIT, AS.CLASSIFIED_INFO, AS.CONFIG_EXT, AS.CONFIG_SS, AS.PROPER_OP, AS.SEC_CFG
Unwanted outcome	Unauthorized personnel get unauthorized access to classified information because a compromised version of the TOE is used to maintain the assets.

TE.DOS An attacker block authorized users from system resources via a resource exhaustion denial of service attack.

Threat agents	TA.ADM, TA.USER, TA.INTERNAL, TA.EXTERNAL.
Asset	AS.PROPER_OP.
Unwanted outcome	Authorized users do not get access to necessary information that they have clearance for.

TE.IMPROPER_INST The TOE is installed and/or configured in a manner that undermines security.

Threat agents	TA.ADM, TA.USER, TA.INTERNAL, TA.EXTERNAL.
Asset	AS.CLASSIFIED_INFO, AS.CONFIG_EXT, AS.CONFIG_SS
Unwanted outcome	The TOE is installed in a manner that eases the process of gaining unauthorized access to classified information.

TE.POOR_DESIGN Unintentional or intentional errors in the design of the TOE may exist. Such design flaws includes: inability to adequately separate information based on SP, HCL or NHC and inability to associate correct security attributes with the users.

Threat agents TA.DEVELOPER

Asset AS.AUDIT, AS.AUTH_DATA, AS.CONFIG_EXT, AS.CONFIG_SS, AS.CLASSIFIED_INFO, AS.SEC_CFG.

Unwanted outcome The developer has failed in designing the TOE in a secure manner thereby undermining its ability to protect assets against attacks.

TE.POOR_IMPL The developer has failed in implementing the TOE according to the design or security flaws are present in the TOE.

Threat agents TA.DEVELOPER

Asset AS.AUDIT, AS.AUTH_DATA, AS.CONFIG_EXT, AS.CONFIG_SS, AS.CLASSIFIED_INFO, AS.SEC_CFG.

Unwanted outcome Attackers get access to classified information, audit data or configuration data. Attackers may conceal unauthorized access and other attacks.

TE.UNATTENDED A malicious user may gain unauthorized access to an unattended session.

Threat agents TA.ADM, TA.USER and TA.INTERNAL

Asset AS.AUDIT, AS.CLASSIFIED_INFO, AS.CONFIG_EXT, AS.CONFIG_SS, AS.SEC_CFG.

Unwanted outcome Unauthorized personnel get access to the specified assets.

6.4 Organisational security policy

The TOE is compliant with the applicable parts of:

Norwegian security policy Norwegian Security Act [10] with supplementary Norwegian Information Security Regulations [5].

NATO security policy C-M(2002)49 Security Within the North Atlantic Treaty Organisation (NATO) [9]

The following is a summary of security policy statements from the Norwegian security policy and NATO security policy which are related to the TOE and/or TOE environment.

P.ACCOUNTING

The objective of the policy for accounting is to provide sufficient information to be able to investigate a deliberate or accidental disclosure, loss or modification of classified information and to support determination of implications of a security breach.

Norwegian security policy

Norwegian Information Security Regulations [5]: §4-11, §4-12, §4-14, §4-16, §5-3 e.

NATO security policy

NATO security policy [9]:

- Enclosure B: §16
- Enclosure E: §§14-16, §§17-23
- Enclosure F: §11, §12.i

P.CLASSIFICATION

The objective of the policy for classification of information is to determine who is responsible for security classification of information, which security classifications to be used, handling of re-classification, and time-limitations of classifications.

Norwegian security policy

Norwegian Security Act [10]: §11

Norwegian Information Security Regulations [5]: §2-1, §2-3, §2-9-§2-13,

NATO security policy

NATO security policy [9]:

- Enclosure B: §§16-19
- Enclosure E: §3, §5

P.CLEAR

Under exceptional operational circumstances, classified information may be transmitted in clear text provided each occasion is properly authorised.

NATO security policy

NATO security policy [9]:

- Enclosure F: §21

P.DAC

A discretionary access control policy based on identity and need-to-know of the user, process and/or groups to which they belong, shall be enforced.

Norwegian security policy

Norwegian Information Security Regulations [5]: §3-3, §5-3 a-b

NATO security policy

NATO security policy [9]:

- Enclosure B: §9.b, §11, §16, §20

- Enclosure C
- Enclosure F : §12.a, §12.b

P.INTEGRITY Classified information shall be protected against alteration and introduction of false information.

Norwegian security policy: Norwegian Information Security Regulations [5]: §5-3 c

NATO security policy: NATO security policy [9]:

- Enclosure B: §2
- Enclosure F: §§3-4, §12.c, §12.d

P.INTERFACE_CONTROL Different information systems can be connected on the following conditions:

1. It shall only be used services and protocols, and administration of these, which are necessary to fulfil the functional requirements of the system.
2. Each of the connected information systems shall have a protection against other information systems, and the security in each of the systems shall be based on mechanisms in that system.
3. Security measures shall be implemented on different levels in the system, to avoid that the protection is based on only one component.
4. Access according to need-to-know shall be implemented mutually between the connected systems.

Norwegian security policy: Norwegian Information Security Regulations [5]: §5-5, §5-7, §5-8

NATO security policy: NATO security policy [9]:

- Enclosure F: §12.f

P.MAC		A mandatory access control policy based on hierarchical classification levels and non-hierarchical categories shall be enforced. Information shall not be allowed to flow from a higher security level to a lower security level or between non-comparable security levels. All individuals, civilian and military, who require access to, or whose duties or functions may afford access to information classified CONFIDENTIAL / KONFIDENSIELT or above, shall be appropriately cleared and briefed before such access is authorised.
	Norwegian security policy	Norwegian Security Act [10]: §§19-26 Norwegian Information Security Regulations [5]: §3-3, §5-3 b,
	NATO security policy	NATO security policy [9]: • Enclosure A: Article 3 • Enclosure B : §9.b, §11, §12 • Enclosure C. • Enclosure F: §7
P.MARKING		The objective of the policy for marking of classified information is to determine who is responsible for the marking, and details on how the marking shall be done.
	Norwegian security policy	Norwegian Security Act [10]: §§11-16 Norwegian Information Security Regulations [5]: §2-2 - §2-7, §4-1 - §4-3, §4-7, §4-8
	NATO security policy	NATO security policy [9]: • Enclosure B: §19 • Enclosure E: §3, §7, §§10-12, §13
P.PROTECTION		Classified information, stored or transmitted, shall be protected against loss of confidentiality, integrity or availability. A balanced set of security measures (physical, personnel, security of information and INFOSEC) shall be implemented. Protective measures and procedures to prevent, detect, and recover from the loss or compromise of information shall be enforced.
	Norwegian security policy	Norwegian Information Security Regulations [5]: §5-1 – §5-5, §6-1

NATO security policy	NATO security policy [9]: • Enclosure B: §2, §16, §22 • Enclosure D. • Enclosure E: §§1-2, §5 • Enclosure F : §§3-4, §8, §12.f, §12.h, §16-20

6.5 Assumptions

The following assumptions must be ensured by the TOE environment.

6.5.1 Physical aspects of the operational environment

A.PHYSICAL	The hardware on which XOmail runs is protected from unauthorized physical modification.
A.PHYSICAL_LOC	The hardware on which XOmail runs is located where only authorized personnel have access.

6.5.2 Personnel aspects of the operational environment

A.ADM_TRAINING	All administrators know how to administrate the TOE in a secure manner. Administration of the TOE in a secure manner means that each administrator must know all consequences of all administrative tasks that are performed. Furthermore, each administrator knows all his/her responsibilities with regards to TOE administration. Administrator training shall be based on XOmail Administrator's Guide [3].
A.AUDIT_REVIEW	Administrator personnel review audit logs on a regular basis.
A.CONFIDENCE	Administrators or developers will not intentionally compromise the TOE security.
A.INVALIDATE	Proper disposal of authentication data and associated privileges is performed after access is removed (job termination, change in responsibility). Proper disposal means that the authentication data cannot be used to authenticate towards any part of the TOE.
A.NOTIFY	Administrators and users notify the proper authority of any security issues that impact their systems. This will minimize the potential for loss or compromise of data.
A.USR_TRAINING	All users know how to use the TOE in a secure manner. To use the TOE in a secure manner each user must know the consequences of each available operation. It is also assumed that the user training ensures that the user always labels information correctly. User training shall be based on XOmail User's Guide [2].

6.5.3 Assumptions for the IT-environment

A.ARCHIVE_DB	The TOE Environment ensures the database used for the Central Archive is configured as required by the TOE guidance documentation, and protected appropriately for the sensitivity level of the stored information.
A.NETWORK	The network connections used between separate parts of the TOE and for external communication are protected from unauthorized disclosure and modification.
A.OS	The TOE runs on an operating system evaluated at an appropriate level for the organizational policies of the TOE Environment.. The OS protects the TOE from unauthorized modifications and provide vital security mechanisms like auditing.

7. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

No extended components are defined.

8. SECURITY OBJECTIVES (ASE_OBJ)

8.1 Security objectives for the TOE

O.ACCESS_HIST	The TOE maintains information related to previous attempts for a user to establish a session. This information is displayable to authorized administrators.
O.AUDIT	The TOE uses its internal secure database (SS), as well as OS audit mechanisms to record security related information. When OS audit mechanisms are used, the TOE provides the OS with all necessary information, including the identity of the user that caused the event. The audit trail shall contain information that is sufficient to reconstruct sequences of events, i.e. the event shall include the event time, the event type, who was responsible for the event, and the outcome of the event.
O.AUTO_LOGOUT	The TOE provides an automatic logout mechanism for the MailClient. The mechanism terminates client sessions after a configurable period of inactivity.
O.CMD_ACL	The TOE provides means for restricting access to administrative commands for each user or group of users. This can be used to restrict the administrative right given to the role that the users belong to.
O.CMD_LOG	The TOE provides means for recording administrative commands.
O.DAC	The TOE ensures Discretionary Access Control by controlling access to resources based on the identity of users and groups of users.
O.FLASH	The TOE reserves resources to ensure delivery of STANAG 4406 FLASH messages within prescribed time limits.
O.ID_AUTH	A user is identified and authenticated before given access to classified information. Authentication mechanisms include verification of the provided username and password.
O.LABELLING	The TOE ensures that information is labelled with the correct human-readable label when exported out of TSC.
O.LOCK	The TOE provides a locking mechanism that makes it possible to prevent users from logging on, even if they have a valid account. The locking mechanism works on accounts, and can be activated both manually and automatically. Automatic locking is activated when the user has provided a configurable number of invalid authentication tokens.
O.MANAGE	The TOE allows administrators to effectively, accurately and securely manage the TOE and its security functions.
O.MAC	The TOE ensures Mandatory Access Control by controlling access to resources based on security clearance of users and resources.
O.MAC_INTEGRITY	The TOE allows authorized security administrators to specify the security clearance of users and resources.

O.MESSAGING	The TOE provides secure messaging functions. This implies that messages with incorrect security marks will be rejected, while correctly formatted messages are accepted. The TOE will furthermore be able to convert security marks to and from all supported security mark representations.
O.MSG_INTEGRITY	The TOE provides means for ensuring the integrity of STANAG 4406 Ed 2 messages sent between the TOE and other STANAG 4406 Ed 2 compliant MMHS systems. The TOE provides means for ensuring the integrity of Internet Mail (SMTP) messages sent between the TOE and other compliant Internet Mail systems.
O.RECOVER	The TOE will ensure preservation of a secure state in the event of a secure component failure. Upon restart after an abnormal termination, the state may not be a secure state, and the TOE shall use the current state to recover to a secure state.
O.REUSE	The TOE ensures secure reuse of resources. Secure reuse implies that it is not possible to retrieve information stored during a previous use of the resource by other subjects or by the same subject at a different security label.
O.ROLE_MNG	When template “Permit” flag is set, only administrators with the same, or a more privileged level can associate users with that template. However, for templates where the Permit flag is not set, only *Security Administrators* can associate other users with that template, thereby prohibiting use of that template for non-“Security Administrators”.
O.ROLES	The TOE assigns each user to a specific role. The TOE will define roles named *Normal*, *Administrator, Network Administrator, Security Administrator* and *Primary Security Adminstrator*. The role *Normal* has no administrative rights, while the role *Administrator* and *Network Administrator* have administrative rights except security settings. The roles *Security Administrator* and *Primary Security Adminstrator* have all administrative rights. For all roles it is possible to limit the privileges, except for the user assigned *Primary Security Adminstrator* role which will always have all privileges. Furthermore, all defined users are associated with one of the defined roles above.
O.SCHEDULING	The TOE queues and processes information according to its associated priority.
O.SELF_TEST	The TOE database performs a self-test during start-up. The system will not be operable before the database consistency check passes.

8.2 IT Security objectives for the TOE environment

OE.ACCOUNTABLE	Those responsible for the TOE will ensure that the product is configured such that only the group of users for which the system was accredited may access the system, and furthermore that each individual user is assigned a unique user identification.
OE.AUDIT	The OS will perform auditing as specified in GPOSPP and as required by organizational policies. The audit shall contain information that is sufficient to reconstruct sequences of events, i.e. the event shall include the event time, the

	event type, who was responsible for the event, and the outcome of the event. The OS is able to receive audit events from XOmail through its defined logging and management interfaces. Audit events from XOmail may be considered classified information. The operating system will protect the audit data according to the relevant organizational policies.
OE.ID_AUTH	A user is identified and authenticated before given access to the OS that the TOE runs on.
OE.NETWORK	Those responsible for the TOE will ensure that networks that are used for communication between separate parts of the TOE and for external communication are protected. The protection is implemented by means of data encryption or physical protection.
OE.PLATFORM	Those responsible for the TOE will ensure that the Operating System and third party applications used with the TOE are securely installed and managed. In particular, this includes the database server required by Central Archive, PKI services, third party applications accessing the TOE API, and network management services (e.g. MS SCOM).
OE.PKI	The TOE environment will provide mechanisms for management and protection of cryptographic keys, signing and verifying digests, as well as certificate distribution and validation.
OE.TRAF_SEPARATION	The TOE environment will ensure that TOE administrative network traffic can be separated from other TOE network traffic.

8.3 Non-IT Security objectives for the TOE environment

NOE.ADM_TRUST	Those responsible for the TOE will ensure that administrators of the system are trustworthy.
NOE.INSTALL	Those responsible for the TOE will ensure that the TOE is installed, managed and operated according to the TOE guidance documentation. This requires users and administrators to be properly trained.
NOE.PHYSICAL	Those responsible for the TOE will ensure that security relevant components of the TOE are protected from physical attack that might compromise the IT-security.

9. SECURITY REQUIREMENTS (ASE_REQ)

The IT security requirements are standard CC requirements, with minor adaptations. Any deviations from the CC standard requirements have been marked with *blue and italic text*.

9.1 TOE security requirements

9.1.1 TOE security functional requirements

The following subchapters present the security functional requirements for the TOE. Among the assurance requirements, AVA_SOF.1 is included. Therefore a SOF claim must be made for security functions realised using probabilistic or permutational mechanisms. The SOF claim made for TOE security functions is SOF-Medium. Further details each of the security functions can be found in 10.1.

9.1.1.1 Class FAU: Security audit

FAU_ARP.1
Security alarms.

FAU_ARP.1.1
The TSF shall take *the following actions* upon detection of a potential security violation:

a) Warm start on selected events

b) Cold start on selected events

FAU_GEN.1
Audit data generation.

FAU_GEN.1.1
The TOE shall be able to generate audit records of the following auditable events:

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

b) All auditable events for the *basic* level of audit*, as listed in* Table 9-1.

c) Message operations on the offline journal are not audited.

FAU_GEN.1.2
The TOE 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;

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, *message identifier for selected audit event types.*

FAU_GEN.2
User identity association

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

TOE Requirement	Event	Note
FAU_ARP.1	Actions taken due to imminent security violations	
FAU_GEN.1	N/A	
FAU_GEN.2	N/A	
FAU_SAA.1	An alarm is raised when alarm events for a given alarm type occurs more than once within the given period.	
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	
FAU_STG.1	N/A	
FAU_STG.3	An alarm is raised when the available disk space falls below a given limit.	
FAU_STG.4	N/A	When the disk is full, it is not possible to store auditable events.
FDP_ACC.2	N/A	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	
FDP_ETC.2	All attempts to export information.	
FDP_IFC.2	N/A	
FDP_IFF.2	All decisions on requests for information flow.	
FDP_ITC.2	All attempts to import user data, including any security attributes.	
FDP_RIP.2	N/A	
FDP_UIT.1	The identity of any user or subject using the data exchange mechanisms. The identity of any user or subject attempting to use the user data exchange mechanisms, but who are unauthorised to do so. A reference to the names or other indexing	

TOE Requirement	Event	Note
	information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a user) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a user).	
FIA_ATD.1	N/A	
FIA_UAU.2	All use of the authentication mechanism.	
FIA_UAU.5	The result of each activated mechanism together with the final decision.	
FIA_UAU.6	All reauthentication attempts.	
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	Unknown user names are not logged, in order to protect passwords from inadvertent disclosure.
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	This operation is performed in conjunction with the login process, and is not logged separately.
FMT_MSA.1	All modifications of the values of security attributes.	
FMT_MSA.3	a) Modifications of the default setting of permissive or restrictive rules; b) All modifications of the initial values of security attributes.	
FMT_MTD.1	All modifications to the values of TSF data.	
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role.	
FPT_FLS.1	Failure of the TSF.	
FPT_RCV.1	a) The fact that a failure or service discontinuity occurred.	Auditing may not be available in this event (audit storage is full). Startup is guaranteed to be logged via FPT_RCV.2.
FPT_RCV.2	a) The fact that a failure or service discontinuity occurred; b) Resumption of the regular operation;	

TOE Requirement	Event	Note
	c) Type of failure or service discontinuity	
FPT_RCV.4	a) If possible, the inability to return to a secure state after failure of a security function; b) If possible, the detection of a failure of a security function.	
FPT_TDC.1	a) Use of the TSF data consistency mechanisms. b) Identification of which TSF data have been interpreted. c) Detection of modified TSF data.	This requirement defines "TSF data" as "object security labels" a) The mechanisms cannot be bypassed. Specific logging is not considered to be informative. b) The TSF data is invariant (security labels), and are always included in log data. c) Any invalid security labels are specifically handled. The IT environment protective measures are used to ensure TSF data integrity.
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	
FRU_FLT.2	Any failure detected by the TSF.	
FRU_PRS.1	Priority level of each transmitted message. Reception of FLASH messages. Unhandled FLASH messages.	The guidance for FRU_PRS.1 suggests that invocation of the scheduling security function may be audited. This is both infeasible and unnecessary in the TOE, as priority is an integral low-level part of the implementation.
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	
FTA_TSE.1	All attempts at establishment of a user session.	

Table 9-1: Auditable Events

FAU_SAA.1

Potential violation analysis

FAU_SAA.1.1
The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2
The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of *alarms* known to indicate a potential security violation;

b) None

FAU_SAR.1
Audit review

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

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

FAU_SAR.2
Restricted audit review

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.

FAU_STG.1
Protected audit trail storage

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* unauthorized modifications to the audit records in the audit trail.

FAU_STG.3
Action in case of possible audit data loss

FAU_STG.3.1
The TSF shall *generate an alarm* if the audit trail *storage* exceeds *80% utilization or a configurable limit*.

FAU_STG.4
Prevention of audit data loss

FAU_STG.4.1
The TSF shall *shut down the system* if the audit trail is full.

9.1.1.2 Class FCO: Communication

FCO_NRO.1
Selective proof of origin

FCO_NRO.1.1
The TSF shall be able to generate evidence of origin for transmitted *STANAG 4406 and Internet Mail messages* at the request of *none (disabled), the message releaser (optional), or at all times (required)*.

FCS_NRO.1.2
The TSF shall be able to relate the *subject name and address* of the originator of the information, and the *message's S/MIME SignedAttributes and the message payload (STANAG 4406: P2 content, Internet Mail: Message bodyparts.)* of the information to which the evidence applies.

FCO_NRO.1.3
The TSF shall provide a capability to verify the evidence of origin of information to *the message releaser and recipient* given *that a message signature is present*.

FCO_NRR.1
Non-repudiation of receipt

FCO_NRR.1.1
The TOE shall be able to generate evidence of receipt for r*eceived STANAG 4406 and Internet Mail messages* at the request of the *message releaser*.

FCO_NRR.1.2
The TSF shall be able to relate the *subject name and address* of the originator of the information, and the *message's S/MIME SignedAttributes and the message payload (STANAG 4406: P2 content, Internet Mail: Message bodyparts)* of the information to which the evidence applies.

FCO_NRR.1.3
The TSF shall provide a capability to verify the evidence of receipt of information to *message releaser and recipient* given *that a signed recieipt has been generated.*

9.1.1.3 Class FCS: Cryptographic support

FCS_COP.1
Cryptographic operation

FCS_COP.1.1
The TSF shall ~~perform~~ *generate message digests* in accordance with a specified cryptographic algorithm *SHA-1 or SHA-2* and ~~cryptographic key sizes~~ *hash function lengths 128 bits or 256 bits* that meet the following: *NIST FIPS PUB 180-4 Secure Hash Standard [18]*

9.1.1.4 Class FDP: User data protection

FDP_ACC.2
Complete access control

FDP_ACC.2.1
The TSF shall enforce the *DAC* on *all user created data in the internal database* 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 controlled by the TSF and any object controlled by the TSF are covered by an access control TSF.

FDP_ACF.1
Access control functions

FDP_ACF.1.1
The TSF shall enforce the *DAC* to objects based on the following: *subject identifier, object ownership*.

FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Use of Command ACLs and Storage ACL.*

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

a) *XOMAIL_SA*
If the subject is connected as the Primary Security Administrator user, all XOmail administrative access is allowed.

Note: This applies only to the Primary Security Administrator user, not to all users with SA role.

b) *OS_ROOT*
If the subject is the OS Root, user access to all database objects is allowed.

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

FDP_ETC.2
Export of user data with security attributes

FDP_ETC.2.1
The TSF shall enforce the *DAC and the MAC* 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:

a) *Convert security label from internal representation into the representation required by the export medium.*

FDP_IFC.2
Complete information flow control

FDP_IFC.2.1
The TSF shall enforce the *MAC as stated in B&L [4] on all subjects, all information*, and all operations that cause that information to flow to and from non-trusted subjects covered by the SFP.

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

FDP_IFF.2
Hierarchical security attributes

FDP_IFF.2.1
The TSF shall enforce the *MAC as stated in B&L [4]* based on the following types of subject and information security attributes: *subject security clearance (max HCL, NHC, SP), object hierarchical classification level (HCL), object non-hierarchical categories (NHC) and object security policy (SP).*

FDP_IFF.2.2
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold:

a) Read operation: Subject clearance must dominate object label (S >= O).

b) Write operation: Object label must dominate subject clearance (O >= S).

c) RW operation: Subject clearance must be equal to object label (S == O).

FDP_IFF.2.3
The TSF shall enforce the *following additional flow control SFP rules: none*.

FDP_IFF.2.4
The TSF shall provide the following *additional SFP capabilities: none*.

FDP_IFF.2.5
The TSF shall explicitly authorise an information flow based on the following rules:

a) *The Non-Hierarchical category CLEAR shall allow communication of classified information via unsecured communication channels. Information shall be marked CLEAR (according to the interface protocol used), and the original label shall not be transmitted. On reception, CLEAR info shall be marked with a hierarchical security label corresponding to Confidential, and the non-hierarchical security category CLEAR.*

b) *Trusted subjects are allowed to bypass the MAC rules of FDP_IFF.2.2.*

FDP_IFF.2.6
The TSF shall explicitly deny information flow based on the following rules: *none*.

FDP_IFF.2.7
The TSF shall enforce the following relationships for any two valid information flow control security attributes:

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the two security attributes are incomparable; and

b) There exists a ”least upper bound” in the set of security attributes, such that, given any two security attributes, there is a valid security attribute that is greater than or equal to the two

valid security attributes; and

c) There exists a ”greatest lower bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

FDP_ITC.2
Import of user data with security attributes

FDP_ITC.2.1
The TSF shall enforce the *DAC and the MAC* 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:

a) *If no label is present:*
ACP: The message shall be trapped.
Other channels: The message shall be set to the highest label of the channel.

b) *If the label is invalid:*
ACP: The message shall be trapped.
Other channels: The message shall be discarded and alarm shall be generated.

c) *If the channel is tagged as “System-High”, the label shall be set to the highest allowed, and the original label shall be kept as an informative label.*

d) *If the label exceeds the bounds defined for the channel, the message shall be rejected, and an alarm shall be generated.*

e) *If Security Review & Release is activated for the channel, an authorized user shall specify the resulting security label.*

Note: ACP127 message traffic is handled differently because ACP communication channels may be unreliable and message corruption is common. Messages containing errors are trapped for manual inspection by a designated traffic operator.

FDP_RIP.2
Full residual information protection

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.

FDP_UIT.1
Data exchange integrity

FDP_UIT.1.1
The TSF shall enforce the *DAC* to *transmit* user data in a manner protected from *modification and insertion* errors.

FDP_UIT.1.2
The TSF shall be able to determine on receipt of user data, whether *modification or insertion* has occurred.

9.1.1.5 Class FIA: Identification and authentication

FIA_AFL.1
Authentication failure handling

FIA_AFL.1.1
The TSF shall detect when *an administrator configurable positive integer within 0 and 999999* unsuccessful authentication attempts occur related to *client logons for all users*.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall *lock the user account, e.g. the user shall not be able to authenticate until an administrator unlocks the user account.*

FIA_ATD.1
User attribute definition

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

a) *User identifier*

b) *User clearance*

c) *User template (group)*
Each user belongs to a user template. The following security attributes are determined by the user template:

1) *User command access*

2) *Administrator role.*

3) *Command ACLs*

d) *Message storage access lists.*

FIA_UAU.2
Timing of authentication

FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5
Multiple authentication mechanisms

FIA_UAU.5.1
The TSF shall provide *verification of username and password* to support user authentication.

FIA_UAU.5.2
The TSF shall authenticate any user's claimed identify according to the *following rules:*

a) *Use OS password verification mechanisms to verify the username and password.*

b) *Use Kerberos to authenticate user using a Kerberos ticket provided by the OS.*

FIA_UAU.6
Re-authenticating

FIA_UAU.6.1
The TSF shall reauthenticate the user under the conditions:

a) *when requested by an administrator*

b) *when an administrator triggers an administrative command that requires reauthentication to be performed.*

FIA_UID.2
Timing of identification

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

FIA_USB.1
User-subject binding

FIA_USB.1.1
The TSF shall associate the following user security attributes with subjects acting on behalf of that user: *User identifier, User Clearance, User Command Access*.

FIA_USB.1.2
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

a) *Initial User identifier shall be identical to OS user identifier with the same username*

b) *Initial User Clearance shall be set from the User Template that the user creation is based on*

FIA_USB.1.3
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

a) *Users shall be logged out when User Clearance has been changed*

b) *Users shall be logged out when User Command Access has been changed*.

9.1.1.6 Class FMT: Security management

FMT_MSA.1
Management of security attributes

FMT_MSA.1.1
The TSF shall enforce the *MAC and the DAC* to restrict the ability to *change_default, query, modify or delete* the security attributes:

a) *Subject security clearance,*

b) *Subject administrator access levels,*

c) *Subject and object ACLs (e.g. command access),*

d) *Template Permit flag.*

to *the Security Administrator role.*

The following exceptions exist:

a) *The Administrator role may query and modify department ACLs if sufficient command access is available for the user.*

b) *A user may grant other users read access to objects owned by the user (the user's own storage).*

FMT_MSA.3
Static attribute initialization

FMT_MSA.3.1
The TSF shall enforce the *MAC and DAC* to provide *configurable* default values for security attributes that are used to enforce the SFP.

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

FMT_MTD.1
Management of TSF data

FMT_MTD.1.1
The TSF shall restrict the ability to *query, modify, and delete* the *system configuration* to *the Administrator, Network Administrator and Security Administrator roles*.

FMT_SMF.1
Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following security management functions: *TOE security data maintenance*.

FMT_SMR.1
Security roles

FMT_SMR.1.1
The TSF shall maintain the roles *User, Administrator, Network Administrator and Security Administrator.*

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

9.1.1.7 Class FPT: Protection of the TSF

FPT_FLS.1
Fail secure

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: *all*.

FPT_RCV.1
Manual Recovery

FPT_RCV.1.1
After *audit storage has been exhausted* the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2
Automated recovery

FPT_RCV.2.1
When automated recovery from *abnormal termination* is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2
For *all failures except abnormal termination*, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.4
Function recovery

FPT_RCV.4.1
The TSF shall ensure that *all SFs* have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

FPT_TDC.1
Inter-TSF basic TSF data consistency

FPT_TDC.1.1
The TSF shall provide the capability to consistently interpret *object security labels* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2
The TSF shall use *the rules defined for the communication channel* when interpreting the TSF data from another trusted IT product.

Note 1: The interpretation will depend on which protocol is used by the originator.

FPT_TST.1
TSF testing

FPT_TST.1.1
The TSF shall run a suite of self-tests *during initial start-up* to demonstrate the correct operation of the TSF.

FPT_TST.1.2
The TSF shall provide authorized users with a capability to verify the integrity of *TSF data*.

FPT_TST.1.3
The TSF shall provide authorized users with the capability to verify the integrity of *stored TSF executable code, including installed patches*.

9.1.1.8 Class FRU: Resource utilisation

FRU_FLT.2
Limited fault tolerance

FRU_FLT.2.1
The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur:

a) Abnormal termination of a TOE software module

FRU_PRS.1
Limited priority of service

FRU_PRS.1.1
The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2
The TSF shall ensure that each access to the following resources shall be mediated on the basis of the subjects' assigned priority:

- Secure DBMS
- Inter-Process Communication handled by the reference monitor.
- Message processing resources specifically reserved for FLASH traffic.

9.1.1.9 Class FTA: TOE access

FTA_SSL.3
TSF-initiated termination

FTA_SSL.3.1
The TSF shall terminate an interactive session after a *configurable period of user inactivity*.

FTA_TSE.1
TOE session establishment

FTA_TSE.1.1
The TSF shall be able to deny session establishment based on *the following attributes:*
- the lock attribute for users and administrators,
- the ip address, subnet address or hostname of the client
- the authentication tokens provided

9.2 TOE security assurance requirements

The security assurance requirements for the TOE are selected according to EAL4 augmented with ALC_FLR.3 (systematic flaw remediation).

From CC Part 3:

EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and **complete** interface specification, guidance documentation, **a** description of the **basic modular** design of the TOE, **and a subset of the implementation,** to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, **implementation representation, security architecture description** and guidance evidence provided) demonstrating resistance to penetration attackers with **an Enhanced-Basic** attack potential.

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

EAL4 is considered appropriate for the TOE when placed in an operational environment with the properties and policies described by the security problem definition in Chapter 6. The security problem definition has been selected according to operational environments for classified networked information systems in military organizations.

The ALC_FLR.3 component has been included to provide assurance for the developer's procedures for handling and patching security flaws discovered in the TOE.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_FLR.3 Systematic flaw remediation ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 9-2: EAL4 augmented with ALC_FLR.3

10. TOE SUMMARY SPECIFICATION (ASE_TSS)

This describes the security functions provided by the TOE to meet the security functional requirements specified. Furthermore a statement of assurance measures specifies the assurance measures of the TOE that are claimed to satisfy the stated assurance requirements.

10.1 TOE security functions

10.1.1 SF.AUDIT

Audit data is stored in the TOE secure database (SS) and through OS auditing mechanisms.

The following operator-initiated operations are auditable:

1) Message operations performed by users.
   - Show
   - Print
   - Delete
   - Change
     Does not apply to Draft messages
   - Accept
   - Send
   - Refuse
   - Change Label
   - Release from Security Review
   - Release from Vetting
   - Reroute
   - Resend
   - Copy
   - Forward
   - Reply
   - Export message
   - Export attachment
   - Import message
   - Create from message
   - Restore deleted message
   - Result from message signature validation

2) Message reception and transmission.

3) Message signed, validated, or re-signed by a traffic operator or gateway

4) Reception of files from centralized management.

5) FLASH message reception and transmission.

6) All administrator commands.

7) Whether each operation or command succeeded or was denied.

8) User login attempts, both successful and failed, and logout.

9) User lockout after a number of unsuccessful logins.

10) All changes to a user's command access.

11) System failures.

12) Self-tests and self-test results.

13) Start-up and shutdown of the XOmail Server.
Note that the audit functions cannot be disabled,
and are started before any auditable events can be performed.

The TOE associates a user identity with all records where applicable.

It is possible for the Security Administrators and Primary Security Administrator to configure alarm descriptors for each alarm type. The alarm descriptors include e.g. alarm severity level, and whether successive alarm events in a configurable period shall raise the corresponding alarm.

Additionally, Security Administrators and Primary Security Administrator may configure specific auditable events to be reported to the operating system or via SNMP, in addition to the secure database. Alarms may also be configured to be stored on the file system. External files and databases are protected by OS DAC. MAC is enforced when printing alarms.

The XOmail audit logs are stored in the XOmail database and protected by SF.DAC and SF.MAC. DAC is evaluated for each audit log (e.g. system log), and MAC is evaluated for each record. A user must pass both mechanisms to gain access to audit records.

It is possible to add audit records until the hard disk is full. An alarm will be issued when disk utilization exceeds a configurable limit. When the hard disk is full, XOmail will shut down. The TOE can be started manually after sufficient disk space has been made available in the TOE environment. If an error occurred during shutdown, recovery is handled by SF.DB_SELF_TEST.

When the TOE has initiated the auditing via an OS system call, the responsibility for correct audit handling is transferred to the OS.

10.1.2 SF.AUTHENTICATION

The SF ensures that only authenticated users get access to TOE services and data held within the TOE. If correct authentication tokens can be provided, the SF associates a role and a security clearance with the user. The TOE supports both user-password authentication and single sign-on mechanisms such as Kerberos.

10.1.3 SF.AUTO_LOGOUT

The SF ensures that sessions can be terminated after a period of inactivity. The length of the period of inactivity is configurable.

10.1.4 SF.CLEAR

A CLEAR policy offers the opportunity for (authorized) users, forcibly and deliberately, to initiate the transmission of classified messages over a communication channel, despite its rejection by the basic Communication Policy ("Sending Sufficiency").

The CLEAR policy has three major components:

- The CLEAR-MARKING policy which enables the marking of a message in order for the Communication policy to recognize it

- The CLEAR-SENDING policy, which recognizes a CLEAR message, and allows its transmission. This policy is essentially a part of the Communication Policy (“Sending Exception”)
- The CLEAR-RECEPTION policy which recognizes a cleared message upon reception, and enforces that such a message is hierarchically labelled as “CONFIDENTIAL”, and non-hierarchically labelled as “Clear”

10.1.5 SF.COMMAND_ACCESS

Administrative access is configurable on a User Template basis. For every operation on an Admin Main Object or Admin Object it is possible to grant or deny access for users based on the User Template currently edited. Role assignments furthermore apply some restrictions on how command access can be configured.

10.1.6 SF.COMMUNICATION_SECURITY

The interfaces to external channels perform the following security functions:

- Correct labelling of incoming and outgoing messages.

- Evaluate needs for Secure Associations
  The TOE ensures that classified information is sent on secure lines only. It is the responsibility of system administrators to define which lines are secure. See XOmail Administrator’s Guide[3] for details. Note that SF.CLEAR provides a controlled override of this policy.

- Provision of a Secure Association Service based on network status and/or manual settings by Security Administrators.

10.1.7 SF.DAC

The Discretionary Access Control (DAC) is always invoked when a subject requests access to tables. If an ACL is defined for the table, that ACL is used for identifying the allowable types of access. If an ACL does not exist, only the table owner is allowed to access the table and its content.

Every user must furthermore be explicitly authorized before being given access to the MailClient, the TSClient or the Admin Client. Authorization is accomplished by requiring users to log on to the applications they use. The Discretionary Access Control (DAC) is inhibited for the OS Root.

Finally, SF.DAC enforces access control for message storage access and traffic operator commands.

A subject must pass both MAC and DAC to access an object.

10.1.8 SF.DB_SELF_TEST

During XOmail start-up, the system database performs a self-test. The test includes a check for whether the database was cleanly shut down, or not. If the database was not cleanly shut down, an internal check for consistency is performed. The check is algorithmic, i.e. for each field it is evaluated whether the value is correct or incorrect. The function also corrects incorrect values, and ensures that XOmail enters a secure state upon startup.

10.1.9 SF.EXECUTION_DOMAINS

The TOE will ensure that execution domains are separated, by using both TSF and OS mechanisms. The OS is responsible for keeping processes separated, and for zeroing memory for processes when created and disk space when allocated. The TOE explicitly classifies processes as trusted or untrusted.

Communication between the two classes is brokered by a reference monitor. The TOE will prevent inadvertent disclosure of information by zeroing new database objects.

10.1.10 SF.MESSAGE_INTEGRITY

The TOE supports S/MIME digital signatures in STANAG 4406 Ed 2. By digitally signing STANAG 4406 Ed 2 messages, the TOE provides server to server message integrity protection, non-repudiation of origin, and non-repudiation of receipt.

Incoming digitally signed messages are verified by the TOE when delivered to recipient storages, or in gateway operations. Outgoing military messages may be digitally signed before transmission depending on the system's configured security policy.

The TOE also supports re-signing messages when conversions or traffic operator handling invalidates the message signature.

When requested by an originator, the TOE will generate a delivery report or read receipt. If required by configuration, these will be signed, ensuring non-repudiation of receipt.

The TOE can be configured to interface external systems or use protocols without support for digital signatures. The TOE will verify signatures before transmission of messages on these channels, and will sign incoming messages.

The security function is configurable and optional, and applies to the STANAG 4406 Ed 2 protocol and the SMTP Gateway

10.1.11 SF.LABEL_TRANSFORM

During their lifetime messages may be converted between different format representations. Within XOmail four different formats exists, i.e. a human-readable format, the ACP127 format, the STANAG 4406 format and the XOmail internal storage format. The value set for security classification need not be the same for the four different format representations.

There exists a predefined and unambiguous way to transform the security label between these four representations. This transformation is performed by a trusted function. The transformation handles cases with syntactical or semantic errors in a security label, and cases where a security label cannot be represented in the target format. These result in the transformation not taking place with a subsequent failure in processing.

10.1.12 SF.LABELLING

On the ACP127-interface and STANAG 4406 interface, messages may arrive without labelling or with a label that is not possible to determine. In these cases the messages shall be trapped (ACP), discarded (STANAG 4406, invalid label) or labelled with maximum label for the current channel (STANAG 4406, without label).

10.1.13 SF.LOCK

All user accounts can be locked. The TSF supports both manual and automatic locking. A user with the Administrator, Network Administrator or Security Administrator role initiates the manual locking. The automatic locking is initiated by a succession of unsuccessful logon attempts.

This function is a separate function from the locking mechanism implemented in the operating system, and allows for users to be locked out from the TOE while still being allowed to use the operation system in the TOE environment.

10.1.14 SF.MAC

The Mandatory Access Control (MAC) implements access rights according to hierarchical classification level (HCL), non-hierarchical category (NHC) and security policy (SP). For MAC evaluation, SP is handled in the same way as the NHC. A subject must pass both MAC and DAC to access an object.

10.1.15 SF.PRIORITY

The TOE integrates support for priority across all levels of its implementation, to ensure timely delivery of messages according to their precedence. Priority attributes are embedded in communication between modules within the TOE (including the secure DBMS) and in all messages sent onto the network, including to the Mail Client. Non-message processing (e.g. administrator sessions) is given a default (low or normal) priority in the TOE

The TOE reference monitor queues and processes internal communication according to priority.

FLASH messages are handled specially by the TOE, with reserved resources to ensure immediate processing of STANAG 4406 messages even under heavy load.

10.1.16 SF.ROLES

TOE users are assigned a role designating the type of administrative access. There are four defined roles: *User* (no administrator access), *Administrator*, *Network Administrator* and *Security Administrator*. Every authenticated used is associated with a role during logon.

An additional role, the *Primary Security Administrator* is provided as a built in role for initial configuration. The *Primary Security Administrator* may be locked after initial configuration (SF.LOCK).

An administrator role is required to access the Admin Client and TSClient. Additionally, the user must be explicitly granted access to commands. The role defines the set of commands that may be enabled for the user.

10.1.17 SF.SECURE_STATE_RECOVERY

Security functions of the XOmail system are designed so that they either succeed and lead to a new secure state, or fail and then return to the previous secure state.

When a software fault is detected, the TOE restores operation by restarting the affected software module, the entire TOE or the operating system.

Upon fatal failure of the XOmail system, the system is automatically shut down and the current state is preserved for later use. The secure state is restored via the SF.DB_SELF_TEST security function.

10.1.18 SF.SUBNET_RESTRICTION

XOmail Client logon may be restricted to be from a specific IP address, a specific hostname, or specific IP subnets only. These restrictions can be configured on a per-storage and per-user basis. That is, a user may have access to storages according to ACLs, but SF.SUBNET_RESTRICTION restricts the locations from which the storage can be accessed.

10.1.19 SF.VALIDATE

The validate security function provides the ability to verify the integrity of both TSF data and TSF executable code. The validation mechanism produces checksums that must be compared with the

developer provided checksums. SF.VALIDATE also validates the signature of core configuration files, such as the security policy definitions (part of TSF data).

11. RATIONALE

The rationale demonstrates that threats, assumptions and policies form a basis for the definition of security objectives. Likewise, it is demonstrated that the chosen security requirements cover all security objectives, and that security functions in the TOE or its environment fully cover the security requirements.

11.1 Security objectives rationale

In the following subsections every security objective is correlated with identified threats and assumptions. It is furthermore shown that all identified threats are covered by a security objective.

The following three tables (Table 11-1, Table 11-3 and Table 11-4) demonstrate that all threats, assumption and policies are covered by a security objective. Some threats are fully covered by a single security objective, while others need more than one security objective to be fully covered.

Threats / Security objectives	TT.ADM_ERROR	TT.AUDIT_FAILURE	TT.COM_INTEGRITY	TT.DOS	TT.FAULTS	TT.MASQUERADE	TT.MONITORING	TT.REPLAY	TT.UNATTENDED	TT.UNAUTH_ACCESS
O.ACCESS_HIST		X				X		X		X
O.AUDIT	X	X		X		X		X		X
O.AUTO_LOGOUT									X	
O.CMD_ACL	X									X
O.CMD_LOG	X	X		X		X		X		X
O.DAC	X									X
O.FLASH				X						
O.ID_AUTH						X		X	X	X
O.LABELLING										X
O.LOCK										X
O.MAC	X									X
O.MAC_INTEGRITY										X
O.MANAGE	X									
O.MESSAGING										X
O.MSG_INTEGRITY			X							
O.RECOVER				X	X					X
O.REUSE						X		X		
O.ROLE_MNG	X									X
O.ROLES	X									X
O.SCHEDULING				X						
O.SELF_TEST				X						X
OE.ACCOUNTABLE	X									
OE.AUDIT	X									X
OE.ID_AUTH										
OE.NETWORK			X	X			X	X		X
OE.PKI			X							
OE.PLATFORM										X
OE.TRAF_SEPARATION							X			

Threats / Security objectives	TT.ADM_ERROR	TT.AUDIT_FAILURE	TT.COM_INTEGRITY	TT.DOS	TT.FAULTS	TT.MASQUERADE	TT.MONITORING	TT.REPLAY	TT.UNATTENDED	TT.UNAUTH_ACCESS
NOE.ADM_TRUST	X									
NOE.INSTALL	X									
NOE.PHYSICAL			X	X			X	X		X

Table 11-1: TOE threats coverage

Threats / Security objectives	TE.AUDIT_FAILURE	TE.DELIVERY	TE.DOS	TE.IMPROPER_INST	TE.POOR_DESIGN	TE.POOR_IMPL	TE.UNATTENDED
O.ACCESS_HIST							
O.AUDIT							
O.AUTO_LOGOUT							
O.CMD_ACL							
O.CMD_LOG							
O.DAC							
O.FLASH							
O.ID_AUTH							
O.LABELLING							
O.LOCK							
O.MAC							
O.MAC_INTEGRITY							
O.MANAGE							
O.MESSAGING							
O.MSG_INTEGRITY							
O.RECOVER			X			X	
O.REUSE							
O.ROLE_MNG							
O.ROLES							
O.SCHEDULING							
O.SELF_TEST							
OE.ACCOUNTABLE							
OE.AUDIT	X		X				X
OE.ID_AUTH							
OE.NETWORK			X		X	X	
OE.PKI							
OE.PLATFORM							
OE.TRAF_SEPARATION					X	X	
NOE.ADM_TRUST				X			

Threats / Security objectives	TE.AUDIT_FAILURE	TE.DELIVERY	TE.DOS	TE.IMPROPER_INST	TE.POOR_DESIGN	TE.POOR_IMPL	TE.UNATTENDED
NOE.INSTALL		X		X			
NOE.PHYSICAL			X		X	X	X

Table 11-2: TOE Environment threats coverage

Assuptions and policies / Security objectives	A.ADM_TRAINING	A.ARCHIVE_DB	A.AUDIT_REVIEW	A.CONFIDENCE	A.INVALIDATE	A.NETWORK	A.NOTIFY	A.PHYSICAL	A.PHYSICAL_LOC	A.OS	A.USR_TRAINING
O.ACCESS_HIST											
O.AUDIT											
O.AUTO_LOGOUT											
O.CMD_ACL											
O.CMD_LOG											
O.DAC											
O.FLASH											
O.ID_AUTH										X	
O.LABELLING											
O.LOCK											
O.MANAGE											
O.MAC											
O.MAC_INTEGRITY											
O.MESSAGING											
O.MSG_INTEGRITY											
O.RECOVER											
O.REUSE											
O.ROLE_MNG											
O.ROLES											
O.SCHEDULING											
O.SELF_TEST											
OE.ACCOUNTABLE	X		X								X
OE.AUDIT										X	
OE.ID_AUTH										X	
OE.NETWORK		X				X				X	
OE.PKI											
OE.PLATFORM		X								X	
OE.TRAF_SEPARATION						X					

Assumptions and policies / Security objectives	A.ADM_TRAINING	A.ARCHIVE_DB	A.AUDIT_REVIEW	A.CONFIDENCE	A.INVALIDATE	A.NETWORK	A.NOTIFY	A.PHYSICAL	A.PHYSICAL_LOC	A.OS	A.USR_TRAINING
NOE.ADM_TRUST				X	X						
NOE.INSTALL	X		X		X		X				X
NOE.PHYSICAL								X	X		

Table 11-3: Assumptions coverage

Assumptions and policies / Security objectives	P.ACCOUNTING	P.CLASSIFICATION	P.CLEAR	P.DAC	P.INTEGRITY	P.INTERFACE_CONTROL	P.MAC	P.MARKING	P.PROTECTION
O.ACCESS_HIST	X								
O.AUDIT	X								
O.AUTO_LOGOUT									
O.CMD_ACL									
O.CMD_LOG	X								
O.DAC				X					
O.FLASH									
O.ID_AUTH	X								
O.LABELLING								X	
O.LOCK									
O.MANAGE									
O.MAC		X	X				X		
O.MAC_INTEGRITY							X		
O.MESSAGING									
O.MSG_INTEGRITY					X				
O.RECOVER									
O.REUSE									
O.ROLE_MNG									
O.ROLES							X		
O.SCHEDULING									
O.SELF_TEST									
OE.ACCOUNTABLE	X								
OE.AUDIT	X								
OE.ID_AUTH									
OE.NETWORK					X				X
OE.PKI					X				
OE.PLATFORM									X
OE.TRAF_SEPARATION									
NOE.ADM_TRUST									
NOE.INSTALL						X			X

Assuptions and policies / Security objectives	P.ACCOUNTING	P.CLASSIFICATION	P.CLEAR	P.DAC	P.INTEGRITY	P.INTERFACE_CONTROL	P.MAC	P.MARKING	P.PROTECTION
NOE.PHYSICAL									X

Table 11-4: Policies coverage

11.1.1 Threats met by the TOE

TT.ADM_ERROR

Objectives covering this threat:

- O.AUDIT, O.CMD_LOG, OE.AUDIT
  Knowing that security relevant actions are audited makes this a less likely occurrence, as administrators know that they can be held accountable for their actions. The intention is that administrators perhaps will think twice/double check before initiating a command when knowing that the command is audited. Auditing will also make it possible to identify and correct unwanted operations.

- O.CMD_ACL
  Command ACLs allows administrative access to be tailored for each administrative role. Restricting access to commands reduces the risk of administrative errors.

- O.DAC
  Restricting access to objects reduces the probability of and effect of administrative errors.

- O.MAC
  Restricting access to objects reduces the probability of and effect of administrative errors.

- O.MANAGE
  Means for an effective management of the TOE reduces the possibility of unintentional administrator errors.

- O.ROLE_MNG
  Managing role associations makes it possible to avoid wrong role associations.

- O.ROLES
  Roles categorizes administrative responsibilities. Well-defined responsibilities reduce the possibility of administrative errors.

- OE.ACCOUNTABLE
  Those responsible for the TOE will ensure that administrative privileges are granted only to those users who are authorized. The scope of administrative privileges are limited to the user's actual needs. This limits the probability and impact of administrative errors.

- NOE.ADM_TRUST
  Ensuring that administrators are trustworthy is an essential countermeasure for unintentional administrative errors. Trustworthy personnel improve the quality of the work performed.

- NOE.INSTALL
  Administrator training and organizational procedures ensure that the TOE is administered according to the TOE guidance documentation.

TT.AUDIT_FAILURE

Objectives covering this threat:

- O.ACCESS_HIST
  Access history is useful when audit failure already has occurred. It can help determining from where and by whom a possible attack was performed. Other reasons for audit failure may also be determined from the access history.

- O.AUDIT
  The objective shall prevent audit failures. Audit failures include audit overflow, erroneous audit data and missing audit records.

- O.CMD_LOG
  Logging administrative commands will ensure that it is possible to detect actions that may lead to audit failure.

TT.COM_INTEGRITY

Objectives covering this threat:

- O.MSG_INTEGRITY
  The objective ensures integrity of message content, and discovery of integrity violations.

- OE.NETWORK
  The objective ensures integrity of messages transmitted over the network.

- OE.PKI
  The objective supports the operation of O.MSG_INTEGRITY.

- NOE.PHYSICAL
  The objective ensures integrity by restricting physical access.

TT.DOS

Objectives covering this threat:

- O.AUDIT
  Audit logs can be used to detect possible DOS attacks so that proper measures can be applied in an early stage of an attack.

- O.CMD_LOG
  The command log can in certain situations reveal by whom and from where a DOS attack was launched. Having identified by whom and from where the attack is coming, it is considerably easier to assign countermeasures.

- O.FLASH
  FLASH message traffic is given priority over other traffic, even when the server experiences heavy load or network congestion.

- O.RECOVER
  The objective covers recovery from possible DOS attacks.

- O.SELF_TEST.
  Ensuring that a database self-test is being performed during start-up reduces the chances of the TOE entering an unknown state after a DoS attack.

- O.SCHEDULING
  The TOE queues and processes messages in an order according to priority. This ensures that higher priority traffic is given precedence during network congestion and heavy load.

- OE.NETWORK.
  The objective reduces the possibility of DoS attacks against the TOE as it becomes considerably more difficult for attackers to gain access to the network the TOE resides in. The network protection will also to a certain degree prevent external subjects from accessing the computer equipment hosting the TOE.

- NOE.PHYSICAL
  The objective reduces the possibility for DOS attacks met by the TOE as it becomes considerably more difficult to send data resulting in TOE resource exhaustion. The physical protection prevents unauthorized sources from accessing computer equipment hosting the TOE, thereby complicating the DoS attack. Other channels than physical access to the TOE must be used.

TT.FAULTS

- O.RECOVER
  The TOE is able to recover from software faults by restarting failed modules, the entire TOE, or the operating system of the MMHS Server.

TT.MASQUERADE

Objectives covering this threat:

- O.ACCESS_HIST
  The objective will provide means for detection of entity masquerading. The objective itself is not to detect masquerading, but to provide evidence of access that can be used in forensic analysis.

- O.AUDIT
  Auditing operations issued during a masquerade attack can help both in determining from where and by whom the attack was launched. It may also to a certain degree help in reversing actions performed as part of the attack.

- O.CMD_LOG
  Logging commands issued during a masquerade attack can help both in determining from where and by whom the attack was launched. It may also to a certain degree help in reversing actions performed as part of the attack.

- O.ID_AUTH
  Authentication mechanisms complicates a masquerade attack.

- O.REUSE.
  Managed reuse of resources prevents attackers from being able to retrieve information that later can be used in a masquerade attack.

TT.MONITORING

Objectives covering this threat:

- OE.NETWORK
  Monitoring by intercepting the network traffic between two distinct TOE locations is prevented through cryptographic protection or physical barriers.

- OE.TRAF_SEPARATION
  Monitoring of administrative traffic is significantly more difficult when traffic separation is implemented, as only administrators will have access through the administrative network.

- NOE.PHYSICAL
  Monitoring the physical assets of the TOE are prevented through physical access restrictions.

TT.REPLAY

Objectives covering this threat:

- O.ACCESS_HIST
  The objective will ease the detection of successful replayed authentication attempts. The objective itself does not perform detection of authentication replays; it only provides evidence for access. This evidence must be crosschecked with authorized user.

- O.AUDIT
  Auditing operations issued during a replay attack can help both in determining from where and by whom the attack was launched. It may also to a certain degree help in reversing actions performed as part of the attack.

- O.CMD_LOG
  Command log can be used to detect replay of administrative commands. Once detected it is considerably easier to assign countermeasures for an attack.

- O.ID_AUTH
  Because users need to be identified and authorized to perform security relevant action within the TOE replaying information is made more difficult.

- O.REUSE
  Proper reuse of resources prevents attackers from being able to retrieve information that can be replayed.

- OE.NETWORK
  Network protection measures prevents attackers from retrieving or injecting information.

- NOE.PHYSICAL
  Physical protection of the TOE prevents attackers from being able to retrieving or injecting information.

TT.UNATTENDED

Objectives covering this threat:

- O.AUTO_LOGOUT
  The objective provides means for minimizing the probability of someone finding an unattended session as sessions are terminated automatically after a configurable period of user inactivity.

- O.ID_AUTH
  Together with O.AUTO_LOGOUT this objective ensures that unattended sessions can be made unavailable to unauthorized personnel.

TT.UNAUTH_ACCESS

Objectives covering this threat:

- O.ACCESS_HIST
  The access history can help determining that unauthorized access has occurred. It can furthermore be used to determine from where and by whom the unauthorized access was obtained.

- O.AUDIT
  Audit logs can help determining that unauthorized access has occurred. It can furthermore be used to determine from where and by whom the unauthorized access was obtained.

- O.CMD_ACL
  Command ACLs provide means for restricting each user's access to perform administrative actions. Unauthorized access can be obtained by performing administrative actions that in turn provide access to the system. Restricting access to administrative tasks reduces the likelihood for unauthorized administrators gaining access to the TOE via intentional malicious TOE administration. Roles provide default command ACLs.

- O.CMD_LOG
  The command log can help determining that unauthorized access has occurred. It can furthermore be used to determine from where and by whom the unauthorized access was obtained.

- O.DAC
  The objective is to perform DAC in order to avoid unauthorized access. DAC is performed for access to all database records. Initially this ensures that only the owner has access to records stored within the table. It is furthermore possible to add an ACL to the table definition so that access for other entities can be controlled.

- O.ID_AUTH
  Requiring users to identify themselves and provide valid authentication tokens before being allowed access to TOE assets prevents (in combination with O.DAC) unauthorized access to that information.

- O.LABELLING
  The objective ensures that information is labelled, so that it can be handled according to its classification. Improper handling of classified information may result in unauthorized access.

- O.LOCK
  Locking the user account after a given number of logon attempts reduces the chances of a successful brute force attack. The TOE will lock accounts after a configurable number of unsuccessful logon attempts.

- O.MAC
  The objective shall enforce the separation of data based on HCL, and NHC and SP. MAC is performed whenever access to subjects and object is requested.

- O.MAC_INTEGRITY
  In order to dynamically change clearance and sensitivity label, there must be functions to maintain this information. Dynamic change of clearance and sensitivity labels is necessary because the authenticated resources (e.g. users) change over time, and objects do not necessary have the same sensitivity label over time. This security objective covers the need for functions to maintain the integrity of data used in MAC so that unauthorized access based on old clearance/classification data is not given.

- O.MESSAGING
  To ensure unambiguous and correct information security labelling the TOE rejects all security marks that cannot be unambiguously converted into internal representation. Furthermore, the TOE rejects messages that have security marks outside the restrictions set by the system configuration, which in turn ensures that the system can only store information that it has clearance for.

- O.RECOVER
  The objective is to preserve a state in case of a system failure, so that XOmail can perform secure recovery and thereby avoid entering an insecure state allowing unauthorized access to TOE assets upon start-up.

- O.ROLE_MNG
  The objective shall ensure that roles and role-belongings can be managed so that role assignments can be performed on an as-needed basis, and changed according to changing needs.

- O.ROLES
  The roles contain predefined access restrictions for administrative tasks, thereby providing a default set of available administrative commands. This reduces the chance of an attacker to successfully perform an unauthorized administrative task, thereby allowing the attacker or a third party access to TOE assets.

- O.SELF_TEST
  Performing a database self-test ensures that corrupt ownership, ACLs and security parameters do not lead to unauthorized access to TOE assets.

- OE.AUDIT
  The audit can help determining that unauthorized access has occurred. It can furthermore be used to determine from where and by whom the unauthorized access was obtained.

- OE.PLATFORM
  By securing systems and applications that are tightly connected to the TOE, the risk of unauthorized access to TOE information is reduced. In particular, the Central Archive platform and services needs to be secured in order to protect archived messages from being disclosed.

- OE.NETWORK
  The network protection prevents external sources from accessing the network connected to the TOE. This in turn complicates the process of gaining unauthorized access to the TOE equipment and TOE’s assets.

- NOE.PHYSICAL
  The physical protection prevents external sources from accessing the computer equipment hosting the TOE. This in turn complicates the process of gaining access to the TOE’s assets.

11.1.2 Threats met by the TOE Environment

TE.AUDIT_FAILURE

Objectives covering this threat:

- OE.AUDIT
  The objective is to prevent audit records from being lost or modified.

TE.DELIVERY

Objectives covering this threat:

- NOE.INSTALL
  Secure delivery routines can prevent attackers from compromising the TOE with viruses and other malicious software. Secure operation of the TOE cannot be ensured if the TOE is tampered with before being installed in a controlled environment.

TE.DOS

Objectives covering this threat:

- O.RECOVER
  The objective covers recovery from an abnormal termination due to denial of service attacks on the OS that the TOE runs on. It is ensured that the TOE does not enter an unsecure state upon startup.

- OE.AUDIT
  The audit can be used to detect possible DOS attacks so that proper measures can be applied in an early stage of the attack.

- OE.NETWORK
  The objective reduces the possibility for DOS attacks met by the TOE host as it becomes more difficult to send data to the host. The network protection will to a certain degree prevent external sources from accessing the computer equipment hosting the TOE.

- NOE.PHYSICAL
  The objective reduces the possibility for DOS attacks met by the TOE environment as it becomes more difficult to send data resulting in TOE environment resource exhaustion. The physical protection will to a certain degree prevent unauthorized sources from accessing the computer equipment hosting the TOE, thereby complicating the DOS attack. Channels other that physical attack must be used.

TE.IMPROPER_INST

Objectives covering this threat:

- NOE.ADM_TRUST
  The administrator must be trusted to install the TOE correctly. The objective addresses the need for administrators that in a correct and secure manner performs proper installation of the TOE.

- NOE.INSTALL
  The objective seeks to eliminate improper installation and improper initial configuration of the TOE.

TE.POOR_DESIGN

Objectives covering this threat:

- OE.NETWORK
  The objective ensures that only trusted personnel have access to the TOE, thereby reducing the set of possible threat agents.

- OE.TRAF_SEPARATION
  Separating different types of network traffic reduces the set of threat agents being able to exploit potential flaws.

- NOE.PHYSICAL
  The objective ensures that only trusted personnel have access to the TOE, thereby reducing the set of possible threat agents.

TE.POOR_IMPL

Objectives covering this threat:

- O.RECOVER
  The objective covers recovery from an abnormal termination due to implementation errors in the TOE. It is ensured that the TOE does not enter an insecure state upon start-up.

- OE.NETWORK
  The objective ensures that only trusted personnel have access to the TOE, thereby reducing the set of possible threat agents.

- OE.TRAF_SEPARATION
  Separating different types of network traffic reduces the set of threat agents being able to exploit potential flaws.

- NOE.PHYSICAL
  The objective ensures that only trusted personnel have access to the TOE, thereby reducing the set of possible threat agents.

TE.UNATTENDED

Objectives covering this threat:

- OE.AUDIT
  The audit can help determining that access via unattended sessions has occurred. It can furthermore be used to determine from where and by whom the access was obtained.

- NOE.PHYSICAL
  The objective addresses the need for the physical protection of the TOE environment to avoid exploitation of an unattended session.

11.1.3 Assumptions

A.ADM_TRAINING

Objectives covering this assumption:

- OE.ACCOUNTABLE
  All administrator shall be aware that they are accountable for their actions. Consequently the administrators must bear in mind his/her responsibilities at all time during administration of the TOE.

- NOE.INSTALL
  Secure installation, management and operation of the TOE require administrators to be properly trained.

A.ARCHIVE_DB

Objectives covering this assumption:

- OE.NETWORK
  The objective ensures security for information transmitted between the TOE and the Central Archive Database Server when these are not located on the same physical hardware.

- OE.PLATFORM
  The objective ensures that the Central Archive database is securely configured and managed.

A.AUDIT_REVIEW

Objectives covering this assumption:

- OE.ACCOUNTABLE
  Holding users of the TOE accountable for their actions means that the audit must be regularly, reviewed to detect inconsistencies or abnormal patterns and traces.

- NOE.INSTALL
  Administrators perform audit reviews.

A.CONFIDENCE

Objectives covering this assumption:

- NOE.ADM_TRUST
  The objective ensures trustworthy administrators which results in confidence that the system will not intentionally be misconfigured.

A.INVALIDATE

Objectives covering this assumption:

- NOE.ADM_TRUST
  Trust in administrative personnel is essential to ensure proper invalidation of authentication data.

- NOE.INSTALL
  Keeping user access updated is an integral part of the secure management of the TOE.

A.NETWORK

Objectives covering this assumption:

- OE.NETWORK
  The objective ensures that protection of the network that TOE use for communication, is pointed out as a responsibility of the TOE owners.

- OE.TRAF_SEPARATION
  The objective provides additional protection for TOE management traffic.

A.NOTIFY

Objectives covering this assumption:

- NOE.INSTALL
  Handling security issues are required for the secure management and operation of the TOE.

A.PHYSICAL

Objectives covering this assumption:

- NOE.PHYSICAL
  The TOE owners are responsible for implementing and maintaining sufficient physical protection for the system.

A.PHYSICAL_LOC

Objectives covering this assumption:

- NOE.PHYSICAL
  The TOE owners are responsible for restricting access to the areas where XOmail is used.

A.OS

Objectives covering this assumption:

- O.ID_AUTH
  The identification and authentication mechanisms of the TOE rely on basic mechanisms in the OS. Authentication tokens are only defined and protected by the OS, and the TOE shall not be able to maintain identities that do not exist in the OS.

- OE.AUDIT
  The objective describes use of OS audit mechanisms to store auditable events performed by the TOE.

- OE.ID_AUTH
  The objective identifies the need for user identification and authentication in the OS that the TOE runs on. The assumption A.OS covers this, as the OS need to be evaluated.

- OE.NETWORK
  The objective identifies the need for protection of network communication. The OS may provide lower layer protocol security mechanisms.

- OE.PLATFORM
  The objective identifies the need for securely configuring and managing the platform the TOE runs on.

A.USR_TRAINING

Objectives covering this assumption:

- OE.ACCOUNTABLE
  All users shall be aware that they are accountable for their actions. Consequently the users must bear in mind their responsibilities at all time during administration of the TOE.

- NOE.INSTALL
  The secure management and operation of the TOE requires users to be properly trained.

11.1.4 Policies

P.ACCOUNTING

The objective of the policy for accounting is to provide sufficient information to be able to investigate a deliberate or accidental compromise of accountable information and assess the damage arising from the compromise. This calls for a unique identification of the users (O.ID_AUTH, OE.ACCOUNTABLE) and logging of sensitive events (O.ACCESS_HIST, O.AUDIT, O.CMD_LOG, OE.AUDIT). The user identification will appear in the log records.

P.CLASSIFICATION

The classification of information is done by the originator (O.MAC).

P.CLEAR

The CLEAR procedures allows exceptions in the mandatory access control mechanisms (O.MAC) for authorised users to send classified messages in clear on unsecure lines.

P.DAC

The TOE ensures Discretionary Access Control (O.DAC) by controlling access to resources based on the identity of users and groups of users.

P.INTEGRITY

The TOE shall be able to ensure integrity of message data (O.MSG_INTEGRITY, OE.NETWORK, OE.PKI).

P.INTERFACE_CONTROL

The TOE, the host computer and computer network must be installed and configured in accordance with the policy for the system (NOE.INSTALL).

P.MAC

The TOE ensures Mandatory Access Control (O.MAC) based on user clearances and object security classifications.

The TOE allows authorized security administrators (O.ROLES) to specify the security clearance of users and resources (O.MAC_INTEGRITY).

P.MARKING

The TOE ensures that information is labelled with the correct human-readable label (O.LABELLING).

P.PROTECTION

Those responsible for the TOE will ensure that the TOE is installed, managed and operated in a manner that maintains security (NOE.INSTALL, NOE.PHYSICAL), that network communication to/from the TOE is protected (OE.NETWORK), and that the operating system and services tightly connected to the TOE is appropriately protected (OE.PLATFORM).

11.2 Security requirements rationale

11.2.1 Requirements are appropriate

The following table (Table 11-5) show that requirements are appropriate to cover TOE security objectives.

Objective / Req.	O.ACCESS_HIST	O.AUDIT	O.AUTO_LOGOUT	O.CMD_ACL	O.CMD_LOG	O.DAC	O.FLASH	O.ID_AUTH	O.LABELLING	O.LOCK	O.MAC	O.MAC_INTEGRITY	O.MANAGE	O.MESSAGING	O.MSG_INTEGRITY	O.RECOVER	O.REUSE	O.ROLE_MNG	O.ROLES	O.SELF_TEST	O.SCHEDULING
FAU_ARP.1										X						X					
FAU_GEN.1	X	X																			
FAU_GEN.2	X	X																			
FAU_SAA.1		X																			
FAU_SAR.1		X																			
FAU_SAR.2		X																			
FAU_STG.1		X																			
FAU_STG.3		X																			
FAU_STG.4		X																			
FCO_NRO.1															X						
FCO_NRR.1															X						
FCS_COP.1															X						
FDP_ACC.2						X								X							
FDP_ACF.1				X		X								X							
FDP_ETC.2						X			X		X										
FDP_IFC.2											X			X							
FDP_IFF.2											X			X							
FDP_ITC.2						X					X										
FDP_RIP.2																	X				
FDP_UIT.1															X						
FIA_AFL.1										X											
FIA_ATD.1						X					X								X		
FIA_UAU.2				X	X			X													
FIA_UAU.5								X													
FIA_UAU.6								X					X								

Objective / Req.	O.ACCESS_HIST	O.AUDIT	O.AUTO_LOGOUT	O.CMD_ACL	O.CMD_LOG	O.DAC	O.FLASH	O.ID_AUTH	O.LABELLING	O.LOCK	O.MAC	O.MAC_INTEGRITY	O.MANAGE	O.MESSAGING	O.MSG_INTEGRITY	O.RECOVER	O.REUSE	O.ROLE_MNG	O.ROLES	O.SELF_TEST	O.SCHEDULING
FIA_UID.2				X	X			X													
FIA_USB.1			X	X	X																
FMT_MSA.1				X								X	X								
FMT_MSA.3												X									
FMT_MTD.1													X								
FMT_SMF.1												X	X								
FMT_SMR.1																		X	X		
FPT_FLS.1																X					
FPT_RCV.1		X																			
FPT_RCV.2																X				X	
FPT_RCV.4																X					
FPT_TDC.1											X			X							
FPT_TST.1																				X	
FRU_FLT.2																X					
FRU_PRS.1							X														X
FTA_SSL.3			X																		
FTA_TSE.1						X				X											

Table 11-5: Security objectives satisfaction

11.2.1.1 O.ACCESS_HIST

Requirements covering this objective:

- FAU_GEN.1
  The TOE is required to maintain an access history list i.e. a list of successful and unsuccessful session establishment attempts. Authorized administrators may access this list.

- FAU_GEN.2
  The TOE associates user identities for the events.

  Note: If the username is unknown to the system, it should not be logged in order to prevent unintentional logging of user password.

11.2.1.2 O.AUDIT

Requirements covering this objective:

- FAU_GEN.1
  The TOE is responsible for recording audit data or initiating OS audit system calls when auditable events occur within the TSC.

- FAU_GEN.2
  The TOE provides user identities for events. The user identity for each event conforms to the owner of the software process that caused the event. When TOE audit mechanisms are initiated, the user identity must be specified by the TOE.

- FAU_SAA.1
  The audit records are required by the TSF self-monitoring introduced by this requirement.

- FAU_SAR.1
  The TOE audit must be possible to read and interpret for the authorized TOE administrators.

- FAU_SAR.2
  It must be possible to restrict access to the audit so that only authorized TOE administrators are allowed access.

- FAU_STG.1
  The audit must be protected against unauthorized deletion or modification.

- FAU_STG.3
  The TOE issues alarms to ensure that administrators are warned before the audit storage is exhausted.

- FAU_STG.4
  The TOE implements means to ensure that auditing is always available as long as the system is running.

- FPT_RCV.1
  If the audit trail storage is exhausted, the TOE will shut down to preserve a secure state.

11.2.1.3 O.AUTO_LOGOUT

Requirements covering this objective:

- FTA_SSL.3.
  The TOE is responsible for providing mechanisms that are capable of automatically terminate sessions after a configurable period of user inactivity.

- FIA_USB.1
  The TOE is responsible for automatic logout of the user when the user clearance or user command access has been changed.

11.2.1.4 O.CMD_ACL

Requirements covering this objective:

- FDP_ACF.1.
  For the TOE to be able to restrict access to commands based on user identity, the DAC mechanisms must be implemented.

- FIA_UAU.2.
  For the TOE to be able to restrict access to administrative commands, it must require all users to identify and authenticate themselves before access to administrative functions can be given. The FIA_UAU.2 ensures that authentication is performed before users are given access to administrative commands.

- FIA_UID.2.
  For the TOE to be able to enforce the ACL for administrative commands, each administrator must be identified before performing any other action. The identification is used to determine whether the user is allowed to perform the command.

- FIA_USB.1
  Command access restrictions rely heavily on the TOE's ability to associate user identity with subjects acting on behalf of users. Accordingly, FIA_USB.1 is necessary for correct command access restriction functionality.

- FMT_MSA.1
  The requirement restricts access to the management of command ACLs. Only security administrators are allowed to change the command ACLs of user templates.

11.2.1.5 O.CMD_LOG

Requirements covering this objective:

- FIA_UAU.2.
  In order to perform recording of administrative commands and associate user identification with each of the records, all users must identify and authenticate. The FIA_UAU.2 ensures authentication of all users before administrative commands can be performed.

- FIA_UID.2.
  Each entry in the command log must be associated with the user that caused the command. Therefore it is necessary for administrators to identify themselves before any other action is performed.

- FIA_USB.1.
  Command log functionality relies heavily on the TOE's ability to associate user identity with subjects acting on behalf of users. Accordingly, FIA_USB.1 is necessary for correct command log functionality.

11.2.1.6 O.DAC

Requirements covering this objective:

- FDP_ACC.2.
  Requires DAC to be performed on database objects and database subjects.

- FDP_ACF.1.
  Specifies how DAC shall be applied on database objects and database subjects.

- FDP_ETC.2.
  Requires the TOE to perform DAC during export to outside the TSC.

- FDP_ITC.2.
  Requires the TOE to perform DAC during import from outside the TSC.

- FIA_ATD.1.
  Requires security attributes to be maintained for each individual user. Some of the security attributes are necessary for DAC operation.

- FTA_TSE.1
  Requires the TOE to perform DAC based on the client host address, and authentication tokens.

11.2.1.7 O.FLASH

Requirements covering this objective:

- FRU_PRS.1.
  Ensures that FLASH messages are given priority above other message traffic.

11.2.1.8 O.ID_AUTH

Requirements covering this objective:

- FIA_UAU.2.
  Ensures that unauthorized users are not given access to the TOE's assets.

- FIA_UAU.5.
  Specifies authentication methods that shall be present in the TOE.

- FIA_UAU.6.
  Requires administrators to reauthenticate themselves if this is required to perform an administrative command. Allows administrators to force any user or administrator to reauthenticate.

- FIA_UID.2.
  FIA_UID.2 allows the user to receive an error message upon failed identification before being successfully identified. The error message reveals no assets, nor will it give assistance in finding a correct identification.

11.2.1.9 O.LABELLING

Requirements covering this objective:

- FDP_ETC.2.
  Upon export outside TSC information is labelled with a human-readable label representation of internal information label.

11.2.1.10 O.LOCK

Requirements covering this objective:

- FAU_ARP.1
  The requirement implements automatic lockout of users upon selected potential security violations.

- FIA_AFL.1.
  Describes the conditions for automatic locking of user accounts (setting of the lock-attribute).

- FTA_TSE.1.
  The TOE is required to be able to deny users access based on a lock-attribute.

11.2.1.11 O.MAC

Requirements covering this objective:

- FDP_ETC.2.
  Requires the TOE to perform MAC during export to outside the TSC.

- FDP_IFC.2.
  Requires MAC to be performed on all non-trusted subjects and all information.

- FDP_IFF.2.
  Describes how MAC and MAC support-functions shall be realized. The TOE is required to ensure that access to resources is given based on clear rules for clearance and label comparison.

- FDP_ITC.2.
  Requires the TOE to perform MAC during import from outside the TSC.

- FIA_ATD.1.
  Requires security attributes to be maintained for each individual user. Some of the security attributes are necessary for MAC operation.

- FPT_TDC.1.
  The TOE's ability to perform MAC correctly relies on its ability to assign object label and subject clearance upon importing data from other trusted IT products. FPT_TDC.1 addresses the requirements that ensure TSF data consistency.

11.2.1.12 O.MAC_INTEGRITY

Requirements covering this objective:

- FMT_MSA.1.
  The TOE is required to enforce MAC and DAC to restrict the ability to read or write object and subject security attributes. This in turn ensures that unauthorized personnel cannot violate the integrity of the MAC security attributes.

- FMT_MSA.3.
  The TOE is required to provide default values for security attributes and additionally let *Security*

Administrators override the default settings. This allows *Security Administrator* to maintain integrity of MAC security attributes.

- FMT_SMF.1.
  Management functions that ensure integrity of MAC security attributes must be well defined.

11.2.1.13 O.MANAGE

Requirements covering this objective:

- FIA_UAU.6
  Specifies that administrators may be required to reauthenticate to perform specific administrative commands when required by the configured security policy.

- FMT_MSA.1.
  Enforcing MAC and DAC to restrict ability to modify security attributes support secure and error free management.

- FMT_MTD.1.
  Being able to allow only administrators to read or write TOE configuration data minimises the effort necessary for TOE owners to accomplish secure and effective management of the TOE.

- FMT_SMF.1.
  Management functions that ensure secure, efficient and accurate management of the TOE must be well defined.

11.2.1.14 O.MESSAGING

Requirements covering this objective:

- FDP_ACC.2.
  Enforcing DAC ensures that message can be created, viewed, modified or deleted only by those explicitly granted access to the TOE.

- FDP_ACF.1.
  The DAC mechanisms must be implemented as specified in this requirement in order to have it applied to the message handling.

- FDP_IFC.2.
  Enforcing MAC ensures that message can be created, viewed, modified or deleted only by those explicitly granted clearance for that type of information.

- FDP_IFF.2.
  The MAC mechanisms must be implemented as specified in this requirement in order to have it applied to the message handling.

- FPT_TDC.1.
  The requirements in FPT_TDC.1 ensure that the TOE must reject all messages that do not have a valid security mark that can be verified against internal rules.

11.2.1.15 O.MSG_INTEGRITY

Requirements covering this objective:

- FDP_UIT.1
  The TOE is able to digitally sign messages to allow separate instances of the TOE or third party MMHS implementations to verify the integrity of the transmitted messages. The TOE is able to verify the integrity of digitally signed messages exchanged between separate TOEs or the TOE and other MMHS products.

- FCO_NRO.1
  The TOE is able to generate proof of origin through the use of digital signatures.

- FCO_NRR.1
  The TOE is able to generate proof of receipt through the use of digital signatures.

- FCS_COP.1
  The TOE generates message digests to support the above SFRs.

11.2.1.16 O.RECOVER

Requirements covering this objective:

- FAU_ARP.1
  The TOE performs automated recovery actions upon detection of potential security violations.

- FPT_FLS.1.
  The TOE is required to preserve a secure state in the case of any failure. The preserved secure state can later be used to recover from the failure.

- FPT_RCV.2
  This requirement ensures that automated recovery is performed, and that the TOE does not start in an insecure state.

- FPT_RCV.4
  This requirement ensures that TSF shall either succeed and enter a new secure state, or fail and return to another secure state.

- FRU_FLT.2
  The TOE is able to recover from software faults.

11.2.1.17 O.REUSE

Requirements covering this objective:

- FDP_RIP.2
  Ensures that all informational content of a resource is unrecoverable upon reuse of that resource.

11.2.1.18 O.ROLE_MNG

Requirements covering this objective:

- FMT_SMR.1
  Defines requirements to the TOE on how the roles shall be managed.

11.2.1.19 O.ROLES

Requirements covering this objective:

- FIA_ATD.1
  Requires the TOE to use roles.

- FMT_SMR.1
  Defines the roles that the TOE shall maintain and associate users with.

11.2.1.20 O.SELF_TEST

Requirements covering this objective:

- FPT_RCV.2
  The TOE is required to evaluate the need for, and if needed perform an automated recovery upon start-up.

- FPT_TST.1.
  The TOE is required to run a database integrity check during start-up.

11.2.1.21 O.SCHEDULING

- FRU_PRS.1.
  The TOE associates priority attributes with all TOE internal communication, based on message precedence levels to ensure correct scheduling according to priority.

11.2.2 Functional security requirements dependencies

The table shows each component's direct dependencies to other components. This demonstrates that the set of security requirements form a mutually supportive and consistent whole.

TOE Requirement	Dependency	Included
FAU_ARP.1	FAU_SAA.1	Yes
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1 (via FIA_UID.2)	Yes

TOE Requirement	Dependency	Included
FAU_SAA.1	FAU_GEN.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3	FAU_STG.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FDP_ACC.2	FDP_ACF.1	Yes
FDP_ACF.1.	FDP_ACC.1, FMT_MSA.3	Yes
FDP_ETC.2	FDP_ACC.1, FDP_IFC.1	Yes
FDP_IFC.2	FDP_IFF.1	Yes
FDP_IFF.2	FDP_IFC.1, FMT_MSA.3	Yes
FDP_ITC.2	FDP_ACC.1, FDP_IFC.1, FPT_TDC.1, (*FTP_ITC.1* or *FTP_TRP.1*)	No
FDP_RIP.2		N/A
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1 (both included) FTP_ITC.1 is not included, as the trusted channel is the responsibility of the TOE Environment (OE.NETWORK).	Partial
FIA_AFL.1	FIA_UAU.2	Yes
FIA_ATD.1		N/A
FIA_UAU.2	FIA_UID.1 (via FIA_UID.2)	Yes
FIA_UAU.5		N/A
FIA_UAU.6		N/A
FIA_UID.2		N/A
FIA_USB.1	FIA_ATD.1	Yes
FMT_MSA.1	FDP_ACC.1, FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	Yes
FMT_SMF.1		Yes
FMT_SMR.1	FIA_UID.1 (via FIA_UID.2)	Yes
FPT_FLS.1	ADV_SPM.1	Yes
FPT_RCV.1	AGD_OPE.1	Yes
FPT_RCV.2	AGD_OPE.1	Yes
FPT_RCV.4		N/A
FPT_TDC.1		N/A
FPT_TST.1	(*FPT_AMT.1*)	No
FRU_FLT.2	FPT_FLS.1	Yes
FRU_PRS.1		N/A
FTA_SSL.3		N/A
FTA_TSE.1		N/A

Table 11-6: Functional requirements dependency check

Dependencies are met with three exceptions:

FDP_ITC.2 specifies that either FTP_ITC.1 or FTP_TRP.1 must be present. Given that only OS-authenticated users can perform import, the physical protection of the TOE environment, and the integrity protection of the network, none of these requirements are considered necessary for secure operation.

FPT_TST.1 specifies that FPT_AMT.1 must be present. This dependency is not considered necessary to fulfil as the OS provides an abstract machine that can be used. The OS performs abstract machine testing.

11.2.3 TOE Security Assurance Requirements rationale

The TOE meets the assurance requirements for EAL4 augmented by ALC_FLR.3.

The TOE stresses assurance from best practice development practices. Through review of vendor-supplied evidence and independent testing the Assurance Requirements confirm the implementation of these practices.

The selected assurance level ensures the TOE fulfills national requirements for use in military and governmental networks, handling and separating information as specified in the TOE Overview and TOE Description. In particular, mediation of information flow between national, international and inter-organizational security domains operating at equal or similar sensitivity levels, such as national SECRET, NATO SECRET and Mission SECRET.

11.3 TOE summary specification rationale

11.3.1 TOE security functional requirements satisfaction

This chapter demonstrates that the TOE Security Functions completely implement the TOE Security Functional Requirements.

Table 11-7 shows that each Security Functional Requirement is covered by at least one TOE Security Function and vice versa.

The table is followed by a rationale demonstrating that each SFR is completely implemented by one or more TSFs.

Security function / Req.	SF.AUDIT	SF.AUTHENTICATION	SF.AUTO_LOGOUT	SF.CLEAR	SF.COMMAND_ACCESS	SF.COMMUNICATION_SECURIT	SF.DAC	SF.DB_SELF_TEST	SF.EXECUTION_DOMAIN	SF.MESSAGE_INTEGRITY	SF.LABELLING	SF.LABEL_TRANSFORM	SF.LOCK	SF.MAC	SF.PRIORITY	SF.ROLES	SF.SECURE_STATE_RECOVER	SF.SUBNET_RESTRICTION	SF.VALIDATE
FAU_ARP.1																	X		
FAU_GEN.1	X																		
FAU_GEN.2	X																		
FAU_SAA.1	X																		
FAU_SAR.1	X						X							X					
FAU_SAR.2	X						X							X					
FAU_STG.1	X						X							X					
FAU_STG.3	X																		
FAU_STG.4	X																		
FCO.NRO.1										X									
FCO_NRR.1										X									
FCS_COP.1										X									
FDP_ACC.2							X												
FDP_ACF.1							X												
FDP_ETC.2							X					X		X					
FDP_IFC.2														X					
FDP_IFF.2				X										X					
FDP_ITC.2							X				X	X		X					
FDP_RIP.2									X										
FDP_UIT.1	X									X									
FIA_AFL.1													X						
FIA_ATD.1		X																	
FIA_UAU.2		X																	
FIA_UAU.5		X																	
FIA_UAU.6		X			X														
FIA_UID.2		X																	
FIA_USB.1							X							X					
FMT_MSA.1					X		X							X					
FMT_MSA.3							X							X					
FMT_MTD.1																X			
FMT_SMF.1	X																		
FMT_SMR.1																X			
FPT_FLS.1																	X		
FPT_RCV.1	X																X		
FPT_RCV.2								X											
FPT_RCV.4																	X		
FPT_TDC.1						X						X							
FPT_TST.1								X											X

Security function / Req.	SF.AUDIT	SF.AUTHENTICATION	SF.AUTO_LOGOUT	SF.CLEAR	SF.COMMAND_ACCESS	SF.COMMUNICATION_SECURIT	SF.DAC	SF.DB_SELF_TEST	SF.EXECUTION_DOMAIN	SF.MESSAGE_INTEGRITY	SF.LABELLING	SF.LABEL_TRANSFORM	SF.LOCK	SF.MAC	SF.PRIORITY	SF.ROLES	SF.SECURE_STATE_RECOVER	SF.SUBNET_RESTRICTION	SF.VALIDATE
FRU_FLT.2																	X		
FRU_PRS.1															X				
FTA_SSL.3			X																
FTA_TSE.1						X							X					X	

Table 11-7: Functional requirements satisfaction

11.3.1.1 FAU_ARP.1

This requirement is enforced by the following security functions:

- SF.SECURE_STATE_RECOVERY
  The TOE performs recovery actions upon detection of potential security violations.

11.3.1.2 FAU_GEN.1

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE audit trail satisfies the FAU_GEN.1 list of auditable events.

11.3.1.3 FAU_GEN.2

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE is required to associate a user identity with all audit records where applicable.

11.3.1.4 FAU_SAA.1

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE can be configured for each alarm type to raise an alarm when successive alarm events occur in a configurable period.

11.3.1.5 FAU_SAR.1

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE allows the audit information to be read by authorized and sufficiently cleared administrators.

- SF.DAC
  The audit logs stored in the XOmail database is protected by DAC. This will enable authorised users to read audit records.

- SF.MAC
  The audit logs stored in the XOmail database is protected by MAC. This will enable authorised users to read audit records for which the user has proper clearance.

11.3.1.6 FAU_SAR.2

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE restricts audit information to authorized administrators.

- SF.DAC
  The audit logs stored in the XOmail database is protected by DAC. This will ensure that only authorised users get read access to audit records.

- SF.MAC
  The audit logs stored in the XOmail database is protected by MAC. This will ensure that users only get read access according to the users clearance and the audit records security classification.

11.3.1.7 FAU_STG.1

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE protects audit records from modification and unauthorized deletion.

- SF.DAC
  The audit logs stored in the XOmail database is protected by DAC. This will ensure that only authorised users get delete access to audit records.

- SF.MAC
  The audit logs stored in the XOmail database is protected by MAC. This will ensure that users only get delete access according to the users clearance and the audit records security classification.

11.3.1.8 FAU_STG.3

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE will issue alarms to warn the system administrators when the audit storage nears exhaustion.

11.3.1.9 FAU_STG.4

This requirement is enforced by the following security functions:

- SF.AUDIT
  The TOE will suspend the operation when audit trail is full i.e. the hard disk is full.

11.3.1.10 FCO_NRO.1

- SF.MESSAGE_INTEGRITY
  The TOE supports non-repudiation of origin for the specified messaging protocols.

11.3.1.11 FCO_NRR.1

- SF.MESSAGE_INTEGRITY
  The TOE supports non-repudiation of receipt for the specified messaging protocols.

11.3.1.12 FCS_COP.1

This requirement is enforced by the following security functions:

- SF.MESSAGE_INTEGRITY
  The TOE generates message digests using the specified algorithms.

11.3.1.13 FDP_ACC.2

This requirement is enforced by the following security functions:

- SF.DAC
  The TOE is required to apply DAC within the TSC.

11.3.1.14 FDP_ACF.1

This requirement is enforced by the following security functions:

- SF.DAC
  The requirement describes how DAC shall be applied.

11.3.1.15 FDP_ETC.2

This requirement is enforced by the following security functions:

- SF.DAC
  The TOE is required to apply DAC during export of information from the TSC.

- SF.LABEL_TRANSFORM
  The TOE is required to convert internal label representation to a representation that unambiguously can be associated with the exported data. The exported representation is defined by the export medium.

- SF.MAC
  The TOE is required to apply MAC during export of information from the TSC.

11.3.1.16 FDP_IFC.2

This requirement is enforced by the following security functions:

- SF.MAC
  The TOE is required to apply MAC within the TSC.

11.3.1.17 FDP_IFF.2

This requirement is enforced by the following security functions:

- SF.CLEAR
  Requires the TOE to allow CLEAR-marking of information. The requirements of FDP_IFF.2 specify how to handle CLEAR-marked information.

- SF.MAC
  The requirements specify how MAC shall be applied.

11.3.1.18 FDP_ITC.2

This requirement is enforced by the following security functions:

- SF.DAC
  The TOE is required to apply DAC during import of information into the TSC.

- SF.LABELLING
  The TOE is required to assign a label during import of information into the TSC if correct label cannot be determined. This security function covers cases where either label is not readable, or where label does not exist.

- SF.LABEL_TRANSFORM
  The TOE is required to ensure that interpretation of security label information is as intended by the source of the user data. This covers potentially converting the label information into the internal representation.

- SF.MAC
  The TOE is required to apply MAC during import of information into the TSC.

11.3.1.19 FDP_RIP.2

This requirement is enforced by the following security functions:

- SF.EXECUTION_DOMAINS.
  Different execution domains may over time reuse system resources. It is therefore necessary that information is made unavailable upon allocation of all new system resources. FDP_RIP.2 specifies such requirements for the TOE.

11.3.1.20 FDP_UIT.1

This requirement is enforced by the following security functions:

- SF.AUDIT.
  The security function performs auditing of message traffic (i.e. “use of the data exchange mechanism”).

- SF.MESSAGE_INTEGRITY.
  The security function provides integrity verification of specific message types and generates the necessary verification data for sent messages.

11.3.1.21 FIA_AFL.1

This requirement is enforced by the following security functions:

- SF.LOCK.
  Requirements for account locking are specified in the FIA_AFL.1.

11.3.1.22 FIA_ATD.1

This requirement is enforced by the following security functions:

- SF.AUTHENTICATION.
  The authentication mechanism shall assign security attributes to the user's subjects. FIA_ATD.1 specifies the security attributes available to the authentication mechanism.

11.3.1.23 FIA_UAU.2

This requirement is enforced by the following security functions:

- SF.AUTHENTICATION.
  Users are required to be authenticated.

11.3.1.24 FIA_UAU.5

This requirement is enforced by the following security functions:

- SF.AUTHENTICATION
  FIA_UAU.5 specifies how the authentication mechanisms shall work.

11.3.1.25 FIA_UAU.6

This requirement is enforced by the following security functions:

- SF.AUTHENTICATION
  FIA_UAU.6 specifies when reauthentication may be triggered.

- SF.CMD_ACCESS
  FIA_UAU.6 specifies requirements for command access ACLs.

11.3.1.26 FIA_UID.2

This requirement is enforced by the following security functions:

- SF.AUTHENTICATION
  FIA_UID.1 specifies when the TOE shall require the users to identify themselves.

11.3.1.27 FIA_USB.1

This requirement is enforced by the following security functions:

- SF.DAC
  For the TOE to be able to perform DAC, it is required that user identity of subjects acting on behalf of

users have the correct user security attributes associated. This is part of the DAC functionality; user identity must be associated with all subjects acting on behalf of a user.

- SF.MAC
  Requirements defined in FIA_USB.1 ensure that the necessary security attributes for MAC functionality are associated with the subjects acting on behalf of the users.

11.3.1.28 FMT_MSA.1

This requirement is enforced by the following security functions:

- SF.DAC
  The TOE is required to apply DAC on the management functions for security attributes.

- SF.MAC
  The TOE is required to apply MAC on the management functions for security attributes.

- SF.COMMAND_ACCESS
  The SF provides management of administrators' command access. Command access is restricted by an administrator access level, as well as access to individual commands. Only Security Administrators are allowed to manage command ACLs.

11.3.1.29 FMT_MSA.3

This requirement is enforced by the following security functions:

- SF.DAC
  FMT_MSA.3 specifies how new objects and subjects shall be initialized with regards to security attributes relevant for DAC functionality.

- SF.MAC
  FMT_MSA.3 specifies how new objects and subjects shall be initialized with regards to security attributes relevant for MAC functionality.

11.3.1.30 FMT_MTD.1

This requirement is enforced by the following security functions:

- SF.ROLES
  The requirements describe how role belonging shall put restrictions on access to administrative tasks.

11.3.1.31 FMT_SMF.1

The requirement enforces the following security functions:

- SF.AUDIT
  The requirement defines the management functions for which execution must be logged.

11.3.1.32 FMT_SMR.1

This requirement is enforced by the following security functions:

- SF.ROLES
  Requirements defining the available roles.

11.3.1.33 FPT_FLS.1

This requirement is enforced by the following security functions:

- SF.SECURE_STATE_PRESERVATION
  The TOE is required to preserve a secure state in the occurrence of a failure.

11.3.1.34 FPT_RCV.1

- SF.AUDIT
  The security function ensures the TOE is shut down safely then the audit trail is full.

- SF.SECURE_STATE_RECOVERY
  The security function ensures the system can be restarted when sufficient storage space has been made available for the audit trail.

11.3.1.35 FPT_RCV.2

This requirement is enforced by the following security functions:

- SF.DB_SELF_TEST
  This security function covers the automatic and manual recovery functions required by FPT_RCV.2.

11.3.1.36 FPT_RCV.4

This requirement is enforced by the following security functions:

- SF.SECURE_STATE_RECOVERY
  This security function ensures that all SFs ends in a new secure state as required by FPT_RCV.4.

11.3.1.37 FPT_TDC.1

This requirement is enforced by the following security functions:

- SF.COMMUNICATION_SECURITY.
  During sending and reception of messages, the TOE must handle security attributes according to the requirements specified in the FPT_TDC.1.

- SF.LABEL_TRANSFORM.
  FPT_TDC.1 address requirements concerning the unambiguous representation of security labels and the possibility to convert to/from internal representation.

11.3.1.38 FPT_TST.1

This requirement is enforced by the following security functions:

- SF.DB_SELF_TEST.
  The requirements of FPT_TST.1 specify the features of the database self test.

- SF.VALIDATE.
  The TOE is required to be able to perform validation of the TSF data and executable code.

11.3.1.39 FRU_FLT.2

This requirement is enforced by the following security functions:

- SF.SECURE_STATE_RECOVERY.
  The TOE is able to recover from software faults.

11.3.1.40 FRU_PRS.1

This requirement is enforced by the following security functions:

- SF.PRIORITY.
  The TOE ensures that all TOE internal communication is assigned a priority based on a user selected precedence or . The TOE processes information based on its priority. The highest priority levels are processed in part by dedicated resources to prevent delays.

11.3.1.41 FTA_SSL.3

This requirement is enforced by the following security functions:

- SF.AUTO_LOGOUT
  The TOE is required to provide means for session termination after a period of user inactivity.

11.3.1.42 FTA_TSE.1

This requirement is enforced by the following security functions:

- SF.COMMUNICATION_SECURITY
  Communications security is enforced with the requirements for the TOE to be able to restrict access based on attributes defined in FTA_TSE.1.

- SF.LOCK
  FTA_TSE.1 requires the TOE to be able to deny session establishment based on the lock attribute.

- SF.SUBNET_RESTRICTION
  FTA_TSE.1 requires the TOE to be able to deny session establishment based on IP address, subnet address or hostname of the client initiating the connection.

11.4 PP rationale

Not applicable

12. CHANGE HISTORY

Public edition for XOmail 21.1.1.

End of changes