XOmail

Secure Military Message Handling System

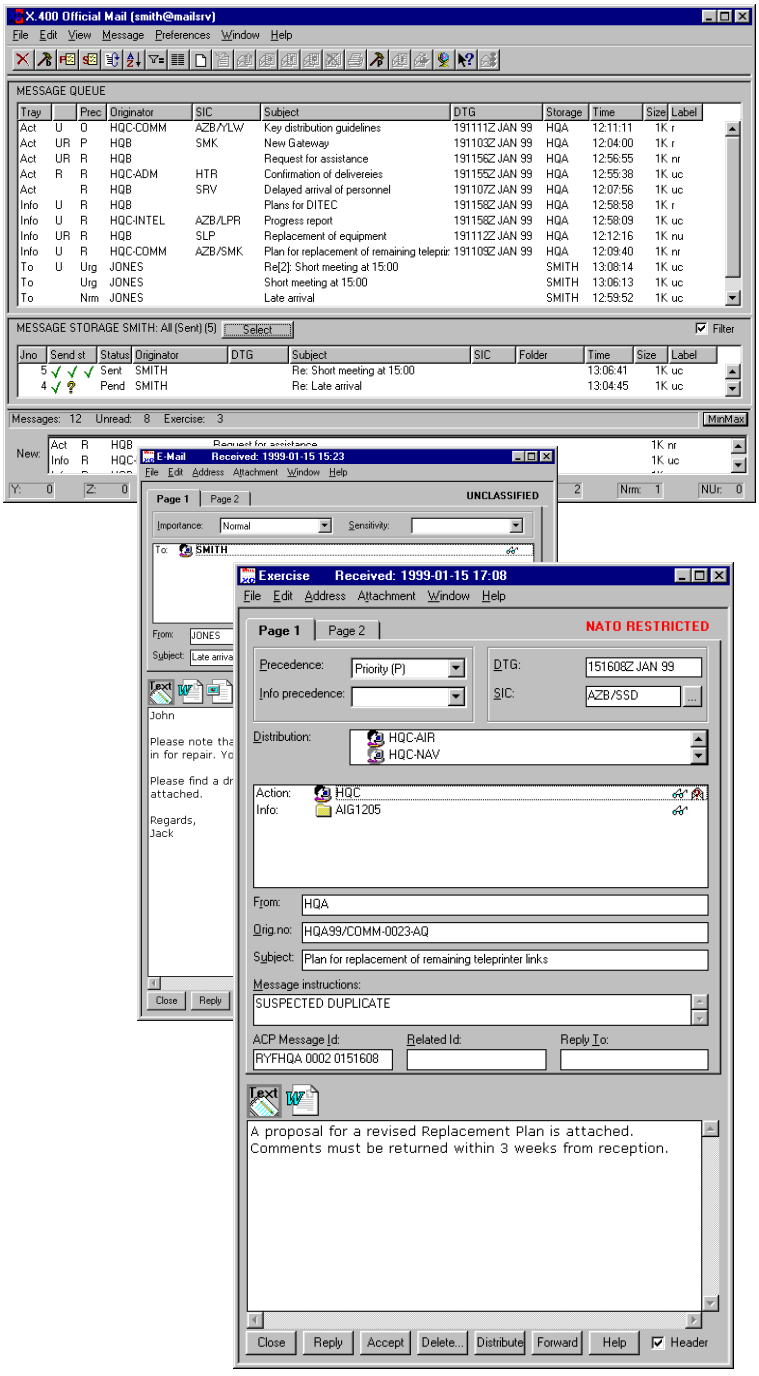
An advanced mail system tailored to messaging tasks in large, military organisations. Field proven and continuously improved since the first release in 1991.

Powerful functions are offered for "desk to desk" messaging, efficiently handling both *official messages* for the organisation and *personal messages* for the user.

NATO STANAG 4406 ("MMHS") is fully supported.

XOmail is designed as a Multi-Level Secure (MLS) system according to NATO Trusted Computer System Evaluation Criteria. It runs on both standard and secure platforms.

The MLS characteristics of the server are essential when used as a *Mail Server* and in dedicated *Mail Guard* applications.



Key benefits

- Delivered as a turn-key military mail system, or as a building block in Command and Control Information Systems or Management Information Systems
- Provides optimal efficiency and security in handling messages
- The user is in control at a glance - "merged view" of all messaging responsibilities
- Security gateways for controlled interconnection with external systems
- Interfaces allowing integration with existing systems (ACP127, NICS TARE, etc.)
- Windows® Clients
- Integration with Office tools

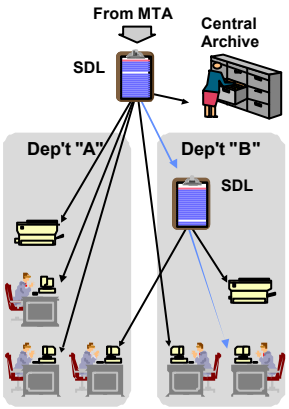
THALES

Messaging functions

Messaging functions are tailored to the needs of large organisations. The system differentiates strictly between official messages (to the organisation) and personal messages (to individual users). The user applications provide a complete environment for preparation and handling of incoming, outgoing, and stored messages with advanced “workgroup” services, such as *automatic local distribution, message co-ordination* and *message authorisation*.

Automatic distribution

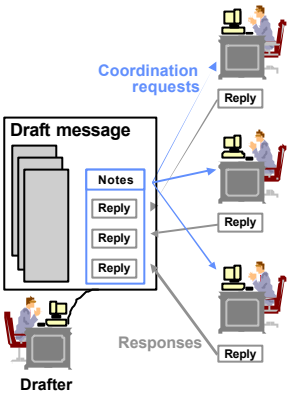
Messages are automatically distributed according to the pre-defined distribution profiles of the sending or receiving department.



The distribution is based on criteria such as SIC, Subject, Security Label and ADatP-3 MSGID.

Message co-ordination

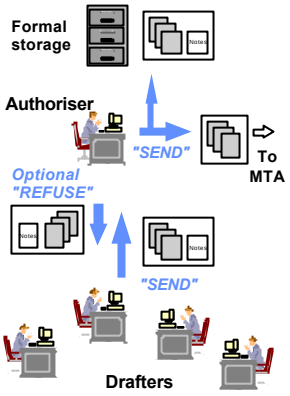
Messages can be distributed for comments before release.



Comments are added as a separate attachment and returned to the originator for final editing. The comments are stored locally, and automatically removed from the message before final transfer.

Message authorisation

Formal approval of official messages is provided by separate user roles of "drafters" and "authorisers".



The messages are routed via the authoriser(s) for release, or returned to the drafter with comments.

User interface

The Graphical User Interface (GUI) is configurable to cater for different users' needs. Some of the key features of the user interface are:

- Organisation modelling - Message storages may be configured in such a manner that it models the organisation. Every organizational unit can be defined as a “department storage”, handling all official messages. E-mail, draft and co-ordination messages are typically stored in private storages, owned by each individual user. Folders organize information within the storages.

- Merged view - The user is presented with a merged view of all incoming messages. This view may contain messages from different storages, depending upon the users’ responsibilities and security clearance.

- Status field - A status field shows the number of messages waiting per precedence (ACP121), the subject of the last message arrived, etc. The status field is updated in real-time, and can be displayed on screen while the user is working with other applications.

Security

Design and implementation has followed the NATO "Trusted Computer System Evaluation Criteria" ("Orange Book"), class B. Non-trusted applications operate under control of the security kernel ("Trusted Computing Base"). Individual channels are assigned security *label ranges* and *status* (e.g. MLS, System-High, and CMW). External cryptographic devices are recognized and utilized to ensure that classified messages are only transmitted on authorized channels. Logs, journals, and audit information are automatically generated and stored.

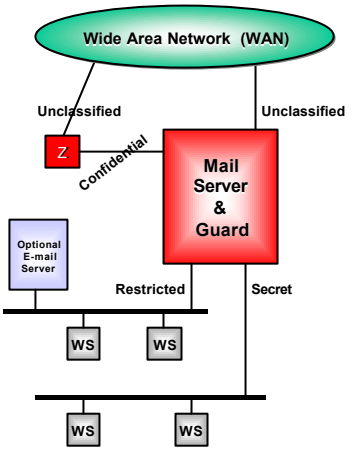
Security Services

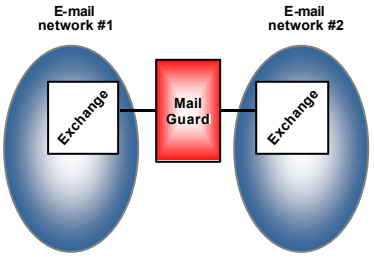
Security services are implemented according to STANAG 4406 V3. The security related algorithms can be replaced by user specified algorithms. The security services include signatures, encryption, content integrity check etc.

Security gateways

Utilizing its Multi-Level Security characteristics, XOmail is able to serve as a secure gateway between networks with different security characteristics. A typical configuration has one or more local segments at different levels, and both classified and non-classified external connections. The security gateway will ensure that security is under no circumstances compromised.

Manual inspection and re-labelling of messages ("Security Review & Release") from System-High domains are built-in to allow release of messages below the System-High level in a trusted manner. A trusted by-pass option can be used between domains operating with the same policy.





Mail Guards

A special *Mail Guard* mode utilizes the MLS characteristics to allow one- or two-way interconnection of E-mail networks that normally would not be allowed to interconnect.

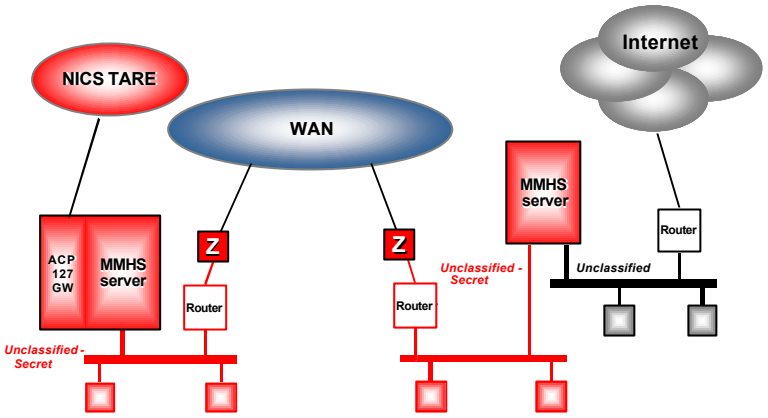
Messages with specific classifications can be allowed to pass, while all other messages are stopped. E.g. "xxxx RESTRICTED" can pass, while "yyyy RESTRICTED" can be stopped. Markings like "... RELEASEABLE TO ..." can also be part of the criteria.

Logs and Audits trails are maintained and can be inspected.

Networking

Servers are interconnected over LAN-based routers (IP) using e.g. an X.25 or ISDN sub-network. Optionally, X.25 or direct (point-to-point) interconnection is possible. User workstations may be connected over a LAN or serial line (RS-232) through modems or routers as appropriate.

Direct gateway functions to ACP127 based teleprinters and -networks enable smooth and gradual evolution of an existing network.



XOmail
TECHNICAL DATA

Baseline specifications
- NATO STANAG 4406 V3 (MMHS extensions to X.400)
- X.500
- ACP127
- NATO Trusted Computer System Evaluation Criteria (or similar)

Protocols & Interfaces
- X.400 P1, P2, P22
- PCT & P772 (STANAG 4406 version of P22)
- X.500 DAP/DSP/ DISP/DOP
- RFC 1006 & TCP/IP
- X.25 (option)
- CORBA

Application Program Interfaces
- Open Systems ("X/Open") MA and MS APIs (optional STANAG 4406 extensions)
- MAPI®

Operating systems
- Windows® NT/2000/95/98 (Client)
- Solaris® 7 / 8 (x86 & SPARC)
- Windows 2000 (not yet available)
- Trusted Solaris® 2.5.1
- AT&T Unix System V/MLS

(Other versions available on request)

Transit Switch Functions
- Powerful Queuing towards other systems
- Centralized or local Reject Positions
- Flexible routing

ACP127 Gateway
- Automatic address conversion
- Filtering based on address or traffic types
- NICS TARE EDC link level protocol
- Automatic generation of channel lists
- ACP127 security label interpretation and generation
- Automated ACP127 channel procedures
- Automatic message syntax checking
- Supports parallel channels for out-channel "message distribution"
- "Channel Check" generation, looping and supervision
- Format Line 2 NICS TARE AIG/XMT special function

On-line Operation and Maintenance
User-friendly Java-based Client for Local O&M functions handling:
- User and Department mailboxes
- System Units
  - Servers
  - Applications
  - Gateways
- Automatic functions
  - Distribution
  - Deletion strategies
  - Timeouts
- Performance Management
- Security Management

These functions and additional functions are available remotely using CORBA.

Tactical version (TMHS)
A tactical add-on product offers additional functions supporting mobility, radio integration and improved bandwidth utilization.

THALES

THALES COMMUNICATIONS AS
P.O. Box 22 Økern • NO-0508 Oslo • Norway • Tel: (+47) 22 63 83 00 • Telefax: (+47) 22 63 79 44
http://XOmail.com http://www.thalesgroup.no/ E-mail:mhs@thalesgroup.no