thalesgroup.com

THALES

WHITEPAPER

Formal Messaging

INTRODUCTION

During the 1970s the need for standardized electronic messaging emerged as computers were interconnected. Personal computers became the dominant trend in network architecture and in 1982, Simple Mail Transfer Protocol (SMTP) with personal and private email accounts became the common Internet Standard for electronic mail transmission.

While sufficient for informal personal messaging, SMTP did not fulfil the requirements for formal messaging, in particular in military organisations. NATO therefore developed STANAG 4406 as the standard for formal messaging, having extensions for integrity and security features such as mandatory access control (e.g. digital signatures, security classification, user clearance). In addition, STANAG 4406 defines how to interoperate with the legacy ACP 127 messaging systems. In 2000, NATO ratified STANAG 4406. Today STANAG 4406 remains a relevant interface standard.

A formal messaging system differs from an ordinary email solution in many ways. Most notable is the support for organisational messaging. Messages are passed between organizational entities or roles within organisations rather than between persons.

A messaging system represents an organisation and its organisational processes and responsibilities.

WHY FORMAL MESSAGING

Organisations, military and public alike, all have to be compliant, transparent and accountable.

To achieve this, organisations have defined formal processes for approval, distribution and archiving of information.

A formal messaging service must support formal workflows, be fully automatic and provide required control functions to supervise the flow of information.

From a functional view, military and public organisations are very similar. A formal messaging system must perform according to a well-defined messaging policy. Such a policy will comprise several explicit parts. The most important are a security policy, a distribution policy, a release policy and an archiving policy. Each of these policies will be specific for each organisation and may change over time.

In addition, all users of the formal messaging system must have a defined role and authorisation. All information elements must have an associated information tag or label. The labels describes the information in terms of classification level, ownership, releasability, COI etc. Digital signatures strengthen the assurance of the policies.

Traditionally, military organisations have more detailed policies and rules for information tagging than public organisations.

REQUIREMENTS TO FORMAL MESSAGING SYSTEMS

All formal messaging systems have to comply with many requirements. Below is a selection of the most important.

BUSINESS PROCESS SUPPORT

A formal messaging system must be adapted to the work processes of an organisation, and replace error-prone manual operations with automated procedures. Unlike ordinary email solutions, messages are passed between organisations or departments rather than between individuals.

A trustworthy notification service is required. This service shall be able to notify the sender of successful delivery, and notify the sender if the receiver has not read a message within a specified time limit.

Another important quality of a formal messaging service is the ability to integrate with command and control systems and standard office tools.

AVAILABILITY

A formal messaging system must provide a messaging service with high availability. Access to the messaging service must be possible for the users independently of their physical location.

A formal messaging system has to be non-disruptive during software maintenance and reconfigurations.

The formal messaging system must remain available to the users to all times, even during Disaster recovery.

The messaging system supports running on a fully redundant infrastructure connected to a resilient infrastructure network.

INTEGRITY

A formal messaging system must ensure that the content of a message remains unaltered from the sender to the receiver. This requirement includes metadata associated with the message content.

Without proper use of digital signatures, it is hard to achieve message integrity, especially when messages pass across gateways and domains.

AUTHENTICATION

A formal messaging system must positively ascertain the identities of all messaging users and accurately represent these identities in service transactions.

The authenticity of all users is vitally important for both non-repudiation and access control mechanisms.

ACCESS CONTROL

A formal messaging system must enforce both Mandatory Access Control and Discretionary Access Control. All messaging users must have a defined set of rights and clearances. All messages, including attachments are labelled with security labels.

ACCOUNTABILITY AND NON-REPUDIATION

A formal messaging system must record all significant user actions on messages. Moreover, it must not be possible to change, hide or in any way deny the fact that a message has been sent or received.

SECURITY LABELLING

All messages must be marked with a security label. This label must represent the security policy and classification of the message. The authenticity of the security label is of high importance, as the security label affects both message flow and user access.

A formal messaging system has to be able to recognize and enforce the security policy of all connected messaging domains.

GUARANTEED TIMELY DELIVERY

A formal messaging service must guarantee timely delivery of all messages.

The messaging policy must contain time limits for each priority level. If a message is not read within the defined time limit, a formal messaging system must take appropriate action. Appropriate action can be to forward the message to an alternate destination or returning a non-delivery report to the originator.

INTEROPERABILITY

A formal messaging system must provide automatic end-to-end interoperability.

A formal messaging system must have integrated interfaces or external gateways to ensure interoperability with old and new messaging systems.

The interoperability requirement also applies in cases where not all message processing systems have implemented digital signatures.

ARCHIVING

A formal messaging system must automatically archive messages to comply with archiving rules and regulations. Additionally, the system must be capable of archiving messages related to an operation or an exercise for later analysis.

CONFIDENTIALITY

A formal messaging system must protect NATO and nationally classified information from unauthorised disclosure.

The formal messaging system must only send classified messages over secured connections. Classified messages must only be delivered to authorised users.

Formal Messaging

XOmail

XOmail meets specific military and governmental requirements. An XOmail based solution provides essential functions such as archiving, battle log, acknowledgement, priority and security classification. Store and forward capabilities within XOmail provide reliable message flow, even across disruptive communication links.

XOmail is a flexible and scalable solution for Formal Messaging Systems allowing stepwise and incremental deployment. XOmail allows expanding the number of users and enabling of new interfaces, without the need for re-installing any software. The modular concept allows incremental modernisation of existing message infrastructures.

In XOmail, all Objects and Subjects have a set of security attributes and labels. The XOmail kernel enforces a security policy according to these attributes. A set of SPIFs (Securtity Policy Information Files) define the security policies to be enforces by XOmail. All XOmail products carry CC EAL 4 approval.

XOmail provides enhanced security services such as Integrity protection, Non-repudiation and Certificate based address validation when integrated with a PKI. XOmail easily integrates with any PKI that supports PKCS#11 and MS-CAPI.

XOmail ENTERPRISE

The XOmail Enterprise operates on virtualized platforms and integrates with third party components such as PKI systems, address directory systems and management tools common in state of the art datacentres. XOmail Enterprise provides Messaging-as-a-Service, including interfaces to other systems. XOmail Enterprise scales from 30 to over 100.000 XOmail Users and contains a number of optional interfaces that provide connectivity to systems external to the XOmail Domain.

ACP 145 INTERFACE

ACP 145 is the one and only agreed NATO standard for connecting messaging systems between nations, and between nations and international organisations. With this option, XOmail Enterprise provides separation between different security domains with different PKIs and allows automatic controlled message flow between them.

ACP 127 INTERFACE

With this option, XOmail Enterprise becomes interoperable with ACP 127 systems such as the NATO AIFS and national ACP 127 systems. The interface supports ACP 127 NATO SUPP-3(B) and ACP 127(G).

SMTP INTERFACE

This option enables XOmail Enterprise to interface with email systems. The SMTP interface allows integration of a wide range of SMTP-based messaging applications into a military messaging infrastructure, including Battle Force E-mail (BFEM).

XOmail CENTRAL ARCHIVE

Central Archive is an option in the XOmail Enterprise product. The Central Archive provides functionality for automatic archiving of all messages within a system. The archive provides long-term storage of messages and powerful mechanisms that allow authorised users to search for 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. A filtering mechanism can be used to identify messages that should be exempted from archiving.

XOmail CLIENTS

The XOmailWEB provides a messaging client accessed from a web browser. XOmailWEB provides basic functionality for message Drafters and Authorisers, and is the preferred application for most users.

The XOmail MS Client provides Traffic Operators and other advanced users with a modern user interface according to Microsoft user interface guidelines.

The XOmail Admin Client provides an application for configuration and management of the various XOmail products.

Formal Messaging

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 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. XOmail Broadcaster supports both Submarine and Surface broadcasting.

XOmail AFLOAT

XOmail Afloat is the Shipside of maritime messaging to be installed on surface vessels and submarines. The XOmail Afloat provides Broadcast reception, Ship-Shore transmission, Inter-Ship traffic and re-Broadcast capabilities.

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

NATION-WIDE FORMAL MESSAGING

XOmail provides formal messaging to military, governmental and non-governmental organisations. By establishing secure and reliable channels between all law enforcement and emergency services, XOmail can offer a much needed information exchange and alerting capability.

A nation-wide formal messaging system improve situation awareness, and ensures efficient distribution of actions across the national enterprise. This allows coordinated use of all national resources in peacetime, crisis, conflict and war. A nation-wide messaging system may contain one or more XOmail Domains.

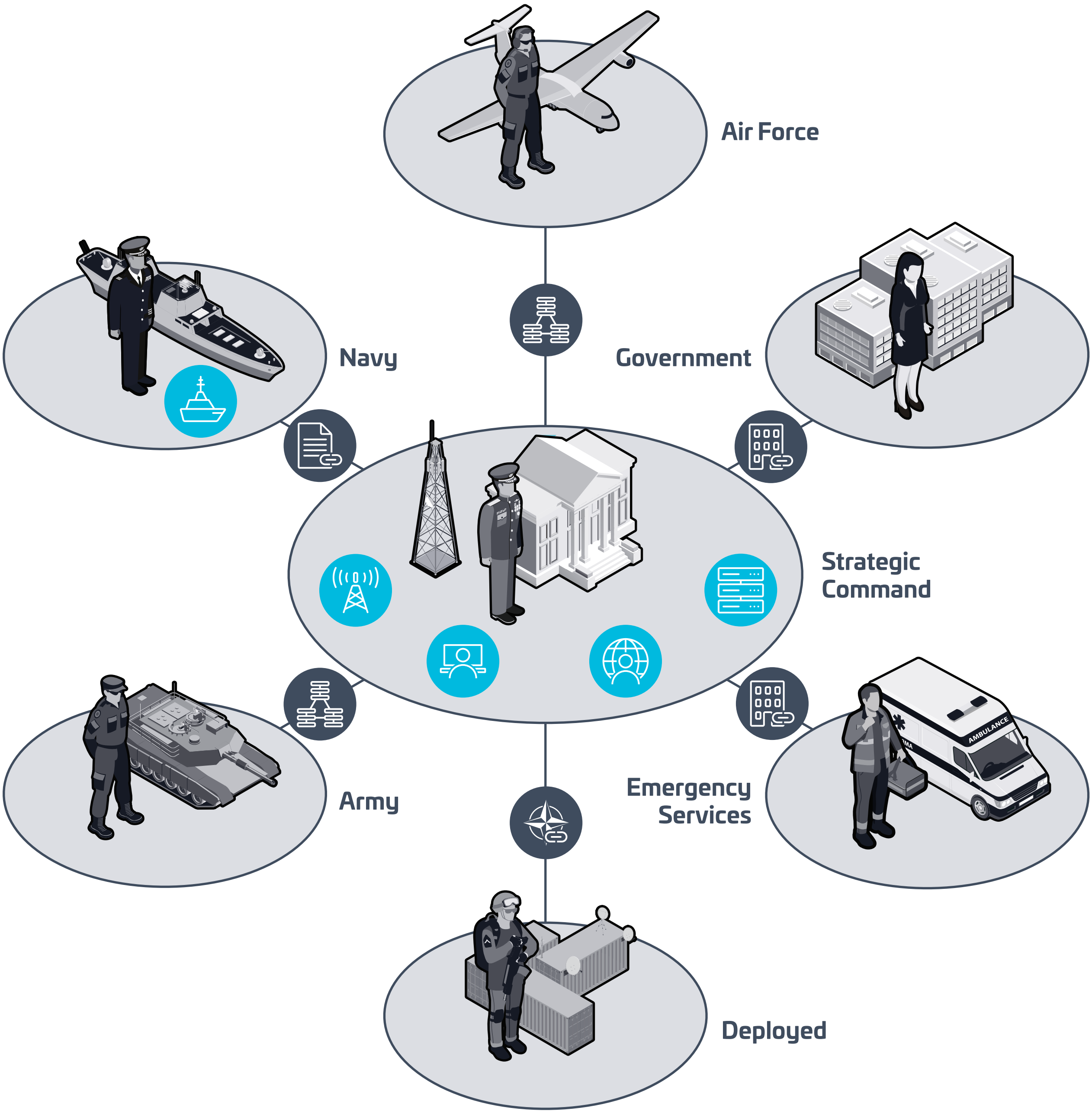
XOmail provides compliance and accountability to Governmental and Military organisations. The XOmail Central Archive provides long-term storage of messages and workflow records. Authorized operators can search and retrieve messages from the Central Archive.

By offering both a formal messaging service and a personal messaging service within the same product, XOmail assists nations in reducing the number of different messaging systems.

XOmail Military Messaging provides messaging for strategic and tactical systems with required features for security, military workflow and priority handling. XOmail complies with STANAG 4406 with a full set of security labels.

XOmail provides formal messaging between organisational elements across security domains, and, optionally, personal messaging between users. XOmail ensures reliable and prioritized message flow, with guaranteed delivery. XOmail processes Flash messages separately with reserved resources. XOmail has a set of defined rules for processing of Flash messages. This enables high priority messages to be automatically processed and supervised.

Nation-wide messaging



Broadcaster

Afloat

Central Archive

Web client

MS client

Products

ACP 145

SMTP

ACP127

XOmail DCI

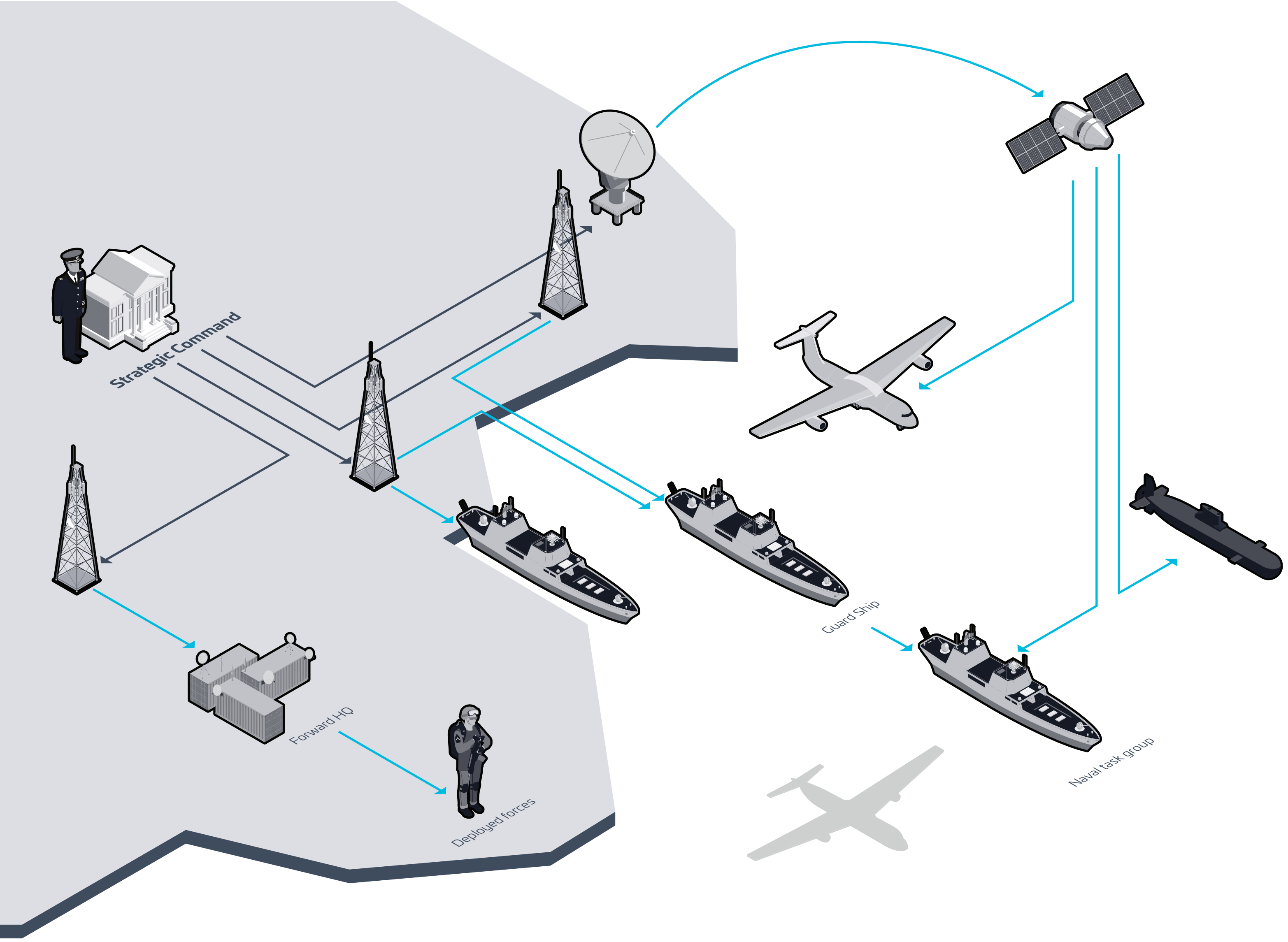
Interfaces

Formal Messaging

BEYOND LINE OF SIGHT

The belief in solving Beyond Line Of Sight communication purely through satellite communications is changing. Focus is now gradually shifting back towards HF, and many HF projects are emerging in Europe. New concepts for use of HF as an infrastructure element is in development, where HF and satellite communications together deliver the service.

XOmail supports NATO BRASS and other Beyond Line Of Sight (BLOS) communication requirements. Deployed forces are supported with formal messaging over bandwidth-efficient protocols (PMUL and DMP) for use over HF, VHF and satellite channels. XOmail will automatically select the best available communications channel.



NAVAL MESSAGING

For communication with vessels and submarines, XOmail III offers two products. The shore-side XOmail Broadcaster is compliant with BRASS and BRASS EO message processing functionality. Vessels and other deployed assets will be equipped with XOmail Afloat.

Automated functions in XOmail hide some of complexity of the "old BRASS world" from the users. XOmail III will section long outgoing messages according to ACP 127, and reassemble received sectioned messages. This ensures a secure, easy and modern information exchange with ACP 127 legacy systems. XOmail is capable of signing a message on behalf of the ACP 127 user when needed.

XOmail provides an interoperable messaging service across numerous communication channels, creating seamless information flow between different systems, and between different units and nations. XOmail can interface and interoperate with both old and new systems, hiding the complexity of having to deal with several systems for the user.

Virtualized ENVIRONMENT

The on-going information technology revolution provides new opportunities for formal messaging, but also new threats to be met.

ENTERPRISE SOLUTION

The IT industry is promoting centralised solutions built around datacentres, promising reduced cost of ownership and simplified integration of services.

XOmail Enterprise can be installed on a datacentre as one of several applications. XOmail takes advantage of a virtualised environment and will provide Messaging as a Service. XOmail can utilize shared services provided by a data center. In particular, enterprise PKI, enterprise Directory services and enterprise management tools shared with other services provided in a Data Centre.

By interconnecting datacentres belonging to various national and international organisations, cross-domain message flow is simplified. This enables efficient collaboration between military forces, government, police forces, and emergency services when needed.

SECURE COLLABORATION

A formal messaging system enables information sharing, both within an organisation and between organisations. A well-defined information sharing policy is required to control information distribution. Elements of the sharing policy will be allowed classifications, communities of interest and need-to-know rights. A prerequisite for all sharing policies is that all information elements carry a set of labels.

A formal messaging system shall ensure a secure and seamless information exchange within a nation and with its partners and allies. Partners and allies may have slightly different security policies, therefore a formal messaging system shall be able to convert labelling information and verify digital signatures between the messaging domains. This enables controlled information flow across the security and organisational boundaries.

XOmail is able to exchange information across these boundaries and to interoperate with both old and new systems using different messaging technologies while hiding this complexity from the XOmail users.

NATIONS AND NATO

The XOmail Enterprise includes an ACP 145 interface for connecting messaging systems within a nation, between nations and between nations and NATO. ACP 145 bridges different PKIs, separating directory services between enterprises with different security policies, and still allowing automatic controlled flow of information.

INFORMAL MESSAGING SYSTEMS

The XOmail Enterprise has an SMTP interface allowing interconnection with e-mail systems running SMTP.

The XOmail SMTP interface supports digital signatures and mapping of security labels. If needed, incoming messages will be digitally signed and provided with default security label for correct processing in the XOmail Enterprise.

ABOUT THALES NORWAY

Thales Norway is a major supplier of security solutions to NATO and NATO Member Nations. For more than 25 years, Thales has been a contributor in field of secure message handling systems and various standardisation efforts lead by the coalition.

Thales has a long-term product improvement plan for the XOmail product family. Short term, our ambition is to extend the XOmail Enterprise into the Deployed forces segment. In the longer term, we will lift XOmail up and into "the Cloud". As always, it is our ambition to reduce the customer's cost of ownership with each and every future XOmail release.

THALES

Thales Norway AS
Langkaia 1, N-0150 Oslo, Norway
+47 22 63 83 00
XOmail@thales.no

> Thalesgroup.com <