FFI RAPPORT

THE JOINT NO AND UK DEMONSTRATION OF INTEGRATED MMHS, PKI AND DIRECTORY SYSTEMS AT JWID 2003

EGGEN Anders, ANDREASSEN Morten, HVINDEN Øyvind, LÆGREID Helge

FFI/RAPPORT-2002/04655

FFIE/840/110

Approved
Kjeller 13. December 2002

Torleiv Maseng
Director of Research

THE JOINT NO AND UK DEMONSTRATION OF INTEGRATED MMHS, PKI AND DIRECTORY SYSTEMS AT JWID 2003

EGGEN Anders, ANDREASSEN Morten, HVINDEN Øyvind, LÆGREID Helge

FFI/RAPPORT-2002/04655

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
P O Box 25, NO-2027 Kjeller, Norway

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
N0-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER FFI/RAPPORT-2002/04655	2) SECURITY CLASSIFICATION UNCLASSIFIED	3) NUMBER OF PAGES 26
1a) PROJECT REFERENCE FFIE/840/110	2a) DECLASSIFICATION/DOWNGRADING SCHEDULE -	

4) TITLE

THE JOINT NO AND UK DEMONSTRATION OF INTEGRATED MMHS, PKI AND DIRECTORY SYSTEMS AT JWID 2003

5) NAMES OF AUTHOR(S) IN FULL (surname first)

EGGEN Anders, ANDREASSEN Morten, HVINDEN Øyvind, LÆGREID Helge

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) MMHS	a) MMHS
b) PKI	b) PKI
c) Directory	c) Katalogtjeneste
d) JWID	d) JWID
e) STANAG 4406	e) STANAG 4406

THESAURUS REFERENCE:

8) ABSTRACT

This report describes the joint NO and UK interoperability testing of integrated MMHS, PKI and Directory Systems conducted at JWID 2003. Joint Warrior Interoperability Programme (JWID) is a yearly event with the main site located at NATO SHAPE HQ. The role of JWID is to introduce new, evolving and low risk technologies that address capability areas within the Command, Control, Communications and Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance areas, or that offer potential solutions to interoperability issues. A formal Military Message Handling System (MMHS) is one of the most important components in a C2IS and is being widely implemented in NATO countries and in NATO. NATO has under NC3B defined a standard for formal Military Message Handling Systems (MMHS - STANAG 4406), together with solutions for application security services for MMHS. In order to make efficient use of these application security services (i.e. to handle Certificates and CRLs for digital signatures), the MMHS must be integrated with PKI and Directory Systems.

9) DATE 13. December 2002	AUTHORIZED BY This page only Torleiv Maseng	POSITION Director of Research

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

THE JOINT NO AND UK DEMONSTRATION OF INTEGRATED MMHS, PKI AND DIRECTORY SYSTEMS AT JWID 2003

1 BACKGROUND

Joint Warrior Interoperability Programme (JWID) is a yearly event with the main site located at NATO SHAPE HQ.

The role of JWID is to introduce new, evolving and low risk technologies that address capability areas within the Command, Control, Communications and Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance areas, or that offer potential solutions to interoperability issues.

A formal Military Message Handling System (MMHS) is one of the most important components in a C2IS and is being widely implemented in NATO countries and in NATO. NATO has under NC3B defined a standard for formal Military Message Handling Systems (MMHS - STANAG 4406), together with solutions for application security services for MMHS. The STANAG 4406 on MMHS contains a security annex (Annex B), which defines the protocol PCT (Protecting Content Type) to support the security services; Message Integrity, Authentication and Non-repudiation of Origin. The PCT protocol is based on parts of the IETF S/MIME protocol, which uses digital signatures to implement these services.

In order to have a complete secure MMHS using the mentioned application security services, the MMHS requires support for generation and revocation of certificates, a trust model for the certificates, a repository for i.a. certificates and addresses, and a way of exchanging certificates and certificate revocation lists (CRLs).

This joint test activity between Norway (NO) and United Kingdom (UK) was initiated in the spirit of the multi-lateral program ALICE (Allied Long Term Security Solution Inter-Connection Exercise), in which NO and UK attend. ALICE has as one of its goals to interconnect and test integrated national systems consisting of MMHS, PKI and Directory Systems, and NO and UK decided to try to demonstrate this concept at JWID 2002. The initiative was taken in January 2002 with the aim of attending JWID 2002 in May 2002.

The JWID 2002 test activity was based on the experience of testing the individual types of systems in other NATO programs or NATO Working Groups. In the NATO test program Message Security Demonstrator Programme (MSDP), STANAG 4406 with the security annex (Annex B) was tested, and the Ad-Hoc WG on Directory Systems had earlier on performed interoperability tests between national ACP-133 Directory Systems. However the participation nations had never before demonstrated interoperability based on integrated MMHS, Directory and PKI systems.

This report focuses on the Norwegian systems and experiences of the JWID 2002 testing. The report also includes some other MMHS test activities with other nations than UK.

2 ACRONYMS AND DEFINITIONS

MMHS	Military Message Handling System
MTA	Message Transfer Agent
MS	Message Store
UA	User Agent
PKI	Public Key Infrastructure
Directory System	A distributed repository of information based on the ITU X.500 and IETF LDAP standard.
CRL	Certificate Revocation List
MMHS-Client	The MMHS User Interface application, which may be separate from the MMHS server
MMHS-Server	MMHS component containing the parts of the User Agent, Message Transfer Agent (MTA) and the Message Store (MS).
RA	Registration Authority
CA	Certificate Authority
HUB	A centralized unit which function is to make information available to other systems or to connect other systems together.
DSA	Directory Server Agent
DUA	Directory User Agent
DISP	Directory Information Shadowing Protocol
LDAP	Light Directory Access Protocol

Certificate A certificate in PKI terms gives credibility to the binding of subject and a public Key

PCT Protecting Content Type (PCT) is a security content type defined in STANAG 4406 Ed.1 Annex B.

P1 P1 is the X.400 protocol used between the MTAs, and describes the “Envelope” of the message.

P772 P772 is the NATO military message content type for formal messaging defined in STANAG 4406 Ed.1.

ACP 133 ACP 133 is the CCEB standard for Directory Systems adopted by NATO

3 JWID MMHS, PKI AND DIRECTORY INTEROPERABILITY ARCHITECTURE

Figure 3.1 shows the systems architecture that was used in the joint NO and UK integrated MMHS, PKI and Directory systems test.

The figure shows

- the Norwegian Domain with the NO strategic and tactical MMHS, Directory and PKI components
- the UK domain with the UK strategic MMHS, Directory and PKI components
- the Cooperative Zone which contains a MMHS HUB and a Directory HUB provided by the NC3A in order to ease the interconnection and information exchange between the national systems
- the US Domain with the DMS strategic MMHS system
- the Combined Endeavour Domain with the Swedish e-mail system

The orange boxes represent MMHS components, the blue boxes represent Directory Systems and the grey boxes represent PKI components. The protocols, STANAGs or information exchanged are shown on the arrows connecting the boxes.

The different systems and components used in the NO and UK domains are described in the related chapters. The US Domain and the Combined Endeavour Domain was not taking part in the integrated MMHS, Directory and PKI test. These domains are included in the figure for completeness.

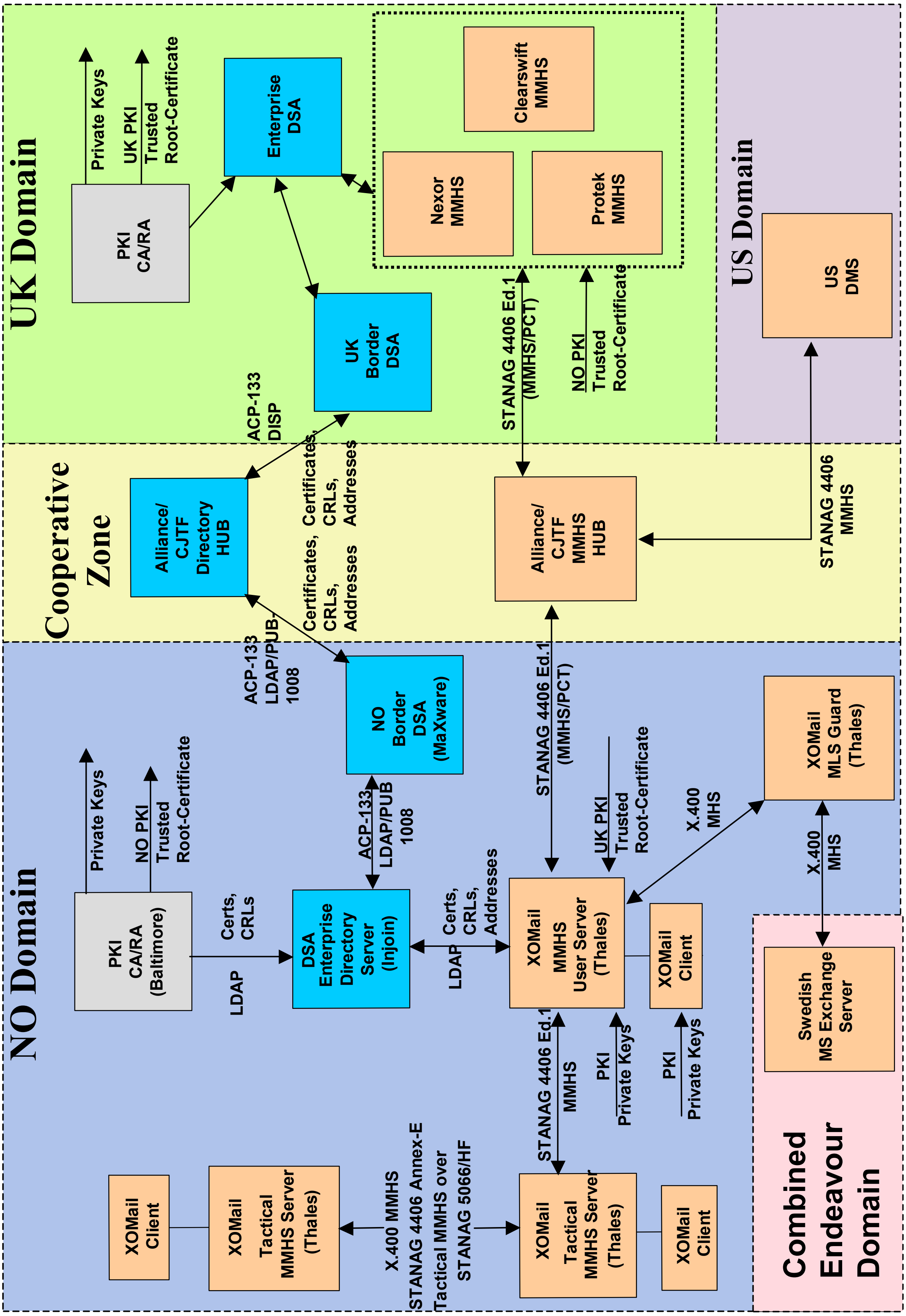

Figure 3.1 The integrated MMHS, PKI and Directory systems architecture

4 MMHS SYSTEMS AND STANDARDS

4.1 Introduction

This section describes the MMHS Systems and standards used in the integrated MMHS-Directory-PKI testing at JWID 2002. The rational for this integrated testing of MMHS, Directory and PKI, was that all of these systems are needed in order to have a complete, secure formal Messaging System. It is therefore important to integrate and test the systems operating together.

The MMHS part of the testing conducted at JWID 2002 was based on the last years MSDP trials in which both NO and UK participated. As in MSDP, the prime messaging focus in JWID 2002 was to test the security protocol content type in Annex B of STANAG 4406 (also called PCT – Protecting Content Type), the military P772 content and the message envelope P1.

The MMHS system was integrated with a Directory system and a PKI system which are required in order to create and issue crypto-keys and distribute certificates. The Directory part of the tests was based on earlier work in the NATO NC3B(SC/5)AHWG on Directory Systems. Both the X.500 DSP and DISP protocols and the (IETF) LDAP protocol have been tested in this group between the nations and the JWID 2002 Directory testing was based on these experiences. Little work has been done on PKI interoperability between the NATO nations. Because of this NO and UK had to agree on their own certificate and CRL profiles and a common trust model. The Directory and PKI systems are described chapters 5 and 6.

This report will focus on the Norwegian experiences and systems with less focus on the UK side. We will however for completeness, mention what types of systems used on the UK side.

4.2 Norwegian System

4.2.1 Strategic MMHS

The Norwegian MMHS system is developed by Thales Norway. The JWID 2002 systems configuration consisted of

- XOmail clients (version 9.6), which includes the user interface of the MMHS
- XOmail servers (version 9.6), which includes the UAs, MSs and MTAs
- XOmail MLS Guard for review and release of messages between the JWID 2002 secret segment and the Combined Endeavour unclassified segment

The operating systems used were Solaris 8.0 for the servers and Windows 2000 for the Clients.

The protocol between the Clients and the Servers over the LAN is a proprietary protocol developed by Thales. The protocol between the MTAs is the X.400 P1 and the content types used in the testing between the UAs were STANAG 4406 P772 and PCT (STANAG 4406 Annex B).

Figure 4.1 shows how the systems were integrated and how the information flows between the different components. The signing of the PCT messages was done at the XOmail client and the verification was done at the server, however signatures could also be generated at the XOmail server. The XOmail client and server also support signing and verification of the traffic between the client and the server.

The trusted root certificates from the UK PKI system were imported directly into the XOmail server in order to have a trusted path to validate the certificates of the signatures from the UK systems. The private keys generated at the Norwegian CA were imported into both the XOmail Client and the XOmail server for generation of signatures. The user certificates however, were exported to the Directory Server by UniCERT using LDAP and retrieved by UK from the Alliance Directory HUB (see figure 3.1). Likewise, the UK user certificates were retrieved from the Alliance Directory HUB and replicated into the Norwegian LDAP server. XOmail client/server could then get the UK certificates from the local Directory (using LDAP) when needed. The system was set up to automatically request the Directory for the certificates if they were not included in the messages.

In a live operational system, importing the same private signing keys into multiple systems (both server and client) is discouraged as this undermines the security of the system. Self generation of signature keys to increase security should also be considered.

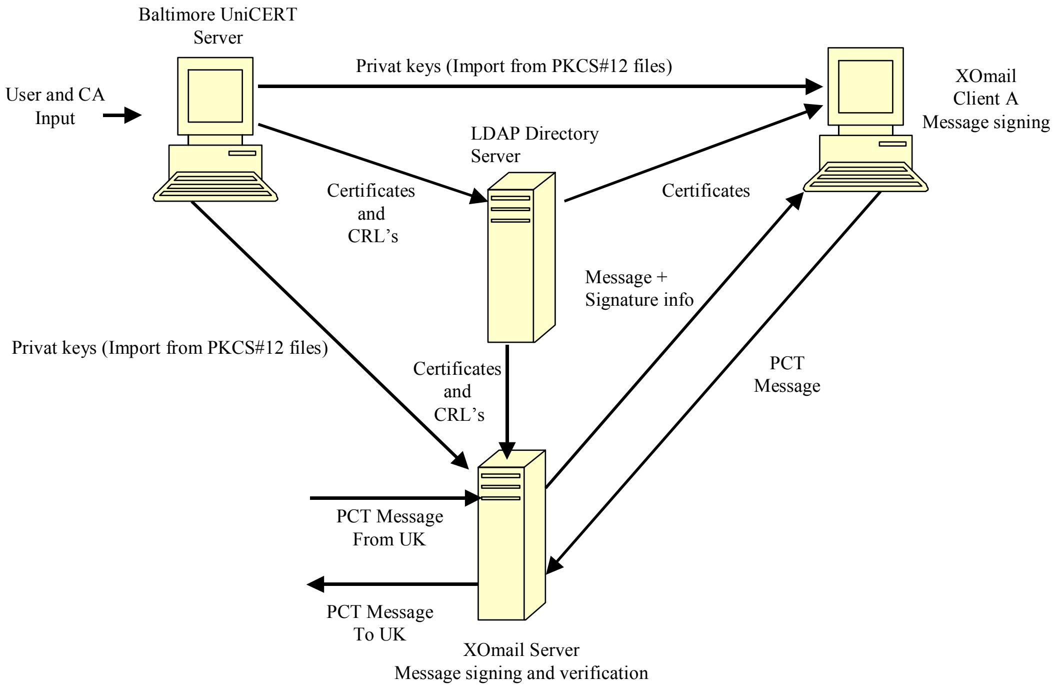

Figure 4.1 The Norwegian MMHS, PKI and Directory interoperation

4.2.2 Tactical MMHS

At JWID 2002 Norway demonstrated an implementation of STANAG 4406 Annex E (Tactical MMHS Protocol and Profile). STANAG 4406 Annex E was developed in order to meet the special communication requirements in the tactical environments (i.a. simplex/half duplex connections, radio silence, low data-rates, etc.). STANAG 4406 Annex E makes it possible for NATO to have a fully integrated tactical and strategic MMHS and replace the ACP 127 systems used for tactical formal messaging within NATO today. Figure 4.2 shows the interconnection of the tactical and strategic MMHS systems at JWID 2002.

STANAG 4406 Annex E allows for re-use of all the MMHS applications from the strategic system in the tactical system. The Thales XOmail Client is the same in both the strategic and the tactical domains. The messaging functionality of the strategic Thales XOmail server and the Thales TMS server is the same, but the tactical MMHS server (TMS) acts as a strategic tactical gateway with two interfaces. One interface running the tactical STANAG 4406 Annex E connectionless protocol stack over a low data-rate HF-modem channel and the other interface running the strategic STANAG 4406 Annex C protocols with full connection oriented OSI protocol stack over the high data-rate connection.

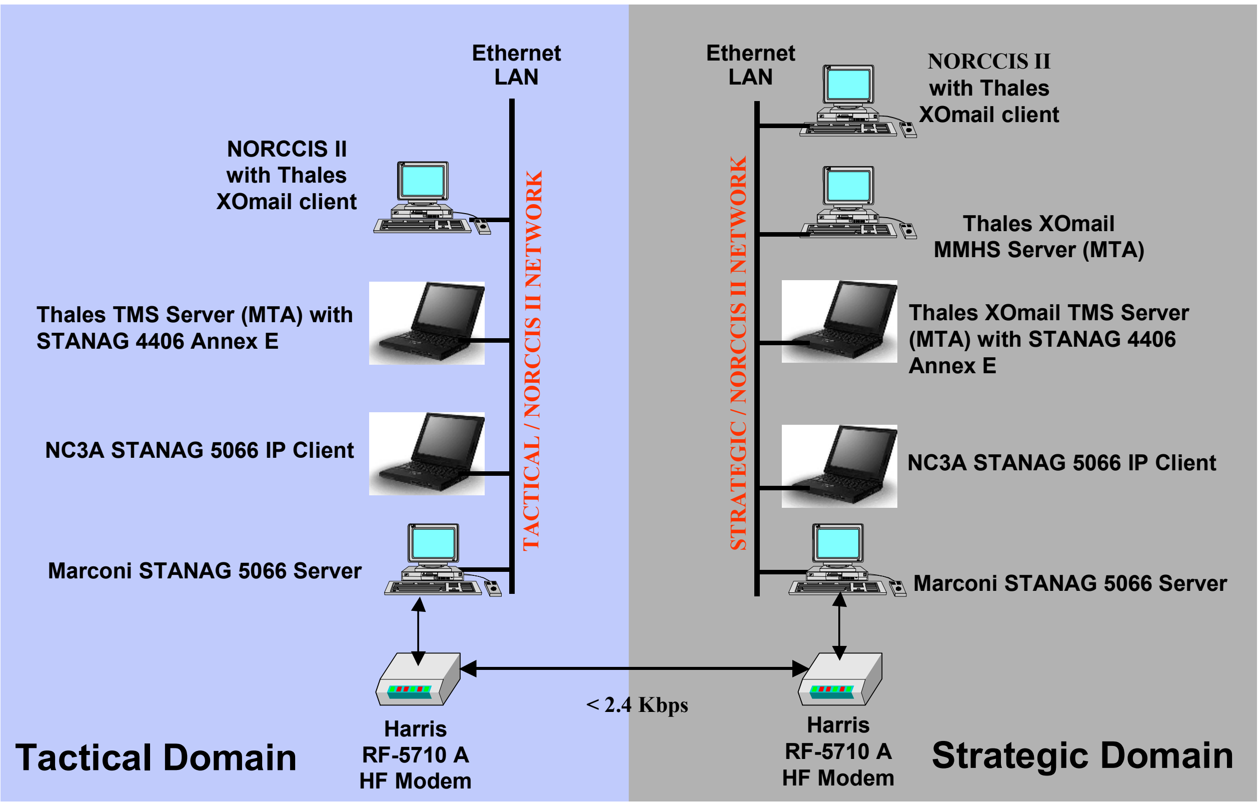
Ethernet LAN
NORCCIS II with Thales XOmail client
Thales TMS Server (MTA) with STANAG 4406 Annex E
NC3A STANAG 5066 IP Client
Marconi STANAG 5066 Server
TACTICAL / NORCCIS II NETWORK
Harris RF-5710 A HF Modem
Tactical Domain
< 2.4 Kbps
Ethernet LAN
NORCCIS II with Thales XOmail client
Thales XOmail MMHS Server (MTA)
Thales XOmail TMS Server (MTA) with STANAG 4406 Annex E
NC3A STANAG 5066 IP Client
Marconi STANAG 5066 Server
STRATEGIC / NORCCIS II NETWORK
Harris RF-5710 A HF Modem
Strategic Domain

Figure 4.2 JWID 2002 – demo STANAG 4406 Ed.1 Annex E (MMHS) over STANAG 5066/HF

The tactical domain consisted of:

- an XOmail client,
- an XOmail TMS server,
- a STANAG 5066 IP client developed by NC3A, which provides an IP interface to a remote application in order to ease the access to the Marconi 5066 software.
- A Marconi STANAG 5066 Server
- A Harris RF-5710A modem

The strategic side of the configuration consisted of:

- an XOmail client,
- an XOmail MMHS server,
- an XOmail TMS server,
- a STANAG 5066 IP client developed by NC3A, which provides an IP interface to a remote application in order to ease the access to the Marconi 5066 software.
- A Marconi STANAG 5066 Server
- A Harris RF-5710A modem

The reason for using all of these PCs, were that the different applications and software run on different operating systems and we didn't have time to do any porting in the time available from before the demonstration. For the tactical MMHS there would normally be sufficient with two laptops at each side, one running the XOmail client and one running the XOmail server, NC3A IP client and Marconi 5066 server.

During the demonstration, formal messages were sent between users in the tactical and strategic domains without any problems. We put a limit on the message size to 2Mb (before compression) in order not to overload the limited capacity on the HF link. One issue that caused a problem was the lack of flow control (in this configuration) between the XOmail TMS server and the 5066 server. The problem was caused by the fact that the LAN between the XOmail server and the 5066 server is fast and the HF link is slow, causing overflow of buffers in the 5066 server. This problem will be solved in future configurations by using IETF ICMP *source quench* packets or TCP tunneling (with flow control) between the XOmail server and the 5066 server on each side (not end-to-end).

4.3 UK Systems

The three MMHS systems used by the UK in this JWID test was:

- Protek
- Clearswift
- Nexor

See chapter 7 for test results regarding interoperability with these systems.

4.4 Interoperability

4.4.1 The Norwegian MMHS – United Kingdom MMHS Connection

The MMHS systems were interconnected over the NATO secret TCP/IP WAN through a HUB at the NC3A. The MTAs were interconnected using the X.400 P1 protocol, which defines the transfer "envelope" of the message.

After some problems caused by IP routing, there were no protocol problems neither at the application layer nor at the lower layers and messages were exchanged in both directions

4.4.2 The Norwegian MMHS – Combined Endeavour e-mail Connection

The connection between the Norwegian JWID Messaging System and the Swedish Combined Endeavour e-mail system, was set up in order to demonstrate command and control interoperability among NATO and national systems in support of NATO CJTF and coalition operations (PfP represents tactical coalition). The NX-1020 crypto from Kongsberg was used to secure the connection between the NATO Secret High domain at JWID and the UNCLASSIFIED domain at Combined Endeavour. An MMHS MLS Guard from Thales with review and release function was used for releasing of messages from the Secret High domain to the Unclassified domain.

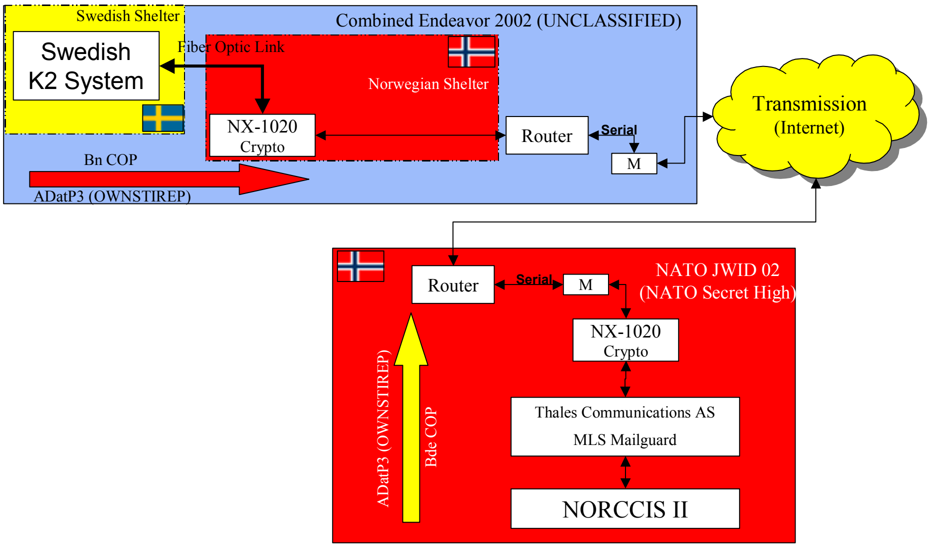

Figure 4.3 The JWID-Combined Endeavour Messaging Systems Configuration

This is the first time a connection between a secret NATO domain and an UNCLASSIFIED PfP domain is demonstrated in a NATO exercise (or at all of our knowledge).

4.4.3 The Norwegian MMHS – US DMS Connection

The US DMS system is interoperable with the Norwegian MMHS at a basic level when neither is using any of their messaging security services, which are incompatible. The US system may send out MMHS messages, which are not signed/encrypted when the messages are sent as unmarked from the client. The protocols used then are X.400 P1 and the MMHS P772 protocol. The Norwegian MMHS can receive these and will upon receipt stamp a security label based on the security definition of the X.400 connector to the US System, in this case it was generic Secret. The Norwegian MMHS can send messages without security elements such as a security label when a software switch is set, and then be interoperable with the US DMS. The X.400 P1 security label and other STANAG 4406 P1 extensions used by the Norwegian MMHS such as the Priority Level Qualifier must be stripped in order to communicate with the most common US DMS implementation, which is based on Microsoft Exchange even though these extensions may be ignored (i.e. they are not marked as critical). The same software switch, which strips the security label also strips the other P1 extensions. The demonstrated interoperability is rudimentary and was also subject to certain P772 fields being used by the US operator in order to show up as MMHS messages in the NO MMHS (e.g. message type) instead of as an e-mail. Interoperability at this level was first demonstrated between the NO MMHS and the US DMS type systems in a JWID demo by SHAPE Technical Centre (now NC3A) in cooperation with Thomson CSF Norway (now Thales) and Lockheed Martin/Loral Systems in July 1997.

5 PKI SYSTEMS AND STANDARDS

5.1 Introduction

This section describes the use of Public Key Infrastructure (PKI) for secure exchange of formal military messages according to STANAG 4406 between Norway and the UK. STANAG 4406 specifies use of digital signatures for securing the integrity and authenticity of messages. Use of digital signatures requires use of digital certificates with support from a PKI system. The PKI system handles life cycle management of the digital certificates. The digital certificates conform to the X.509 standard.

5.2 PKI Architecture

Both the Norwegian and the UK JWID messaging systems support the use of digital signatures and PKI for securing messages.

5.3 Norwegian System

The Norwegian PKI system for JWID 2002 was built using the following products from Baltimore Technologies

- UniCERT CA v.3.5.2
- UniCERT Advanced Publishing Module (ARM) v2.0.2

The PKI system was hierarchical with 2 CA levels. The root was an existing root CA used for test purposes at the Norwegian national security authority (NO NSA). NO NSA set up the sub CA especially for JWID 2002 and Thales then tailored the CA configuration to the MMHS system. The sub CA system also included RA functions and publication of certificates and CRL's to the directory using the ARM product.

The RA was used for key and certificate generation.,The generated keys and certificates were exported into password encrypted PKCS#12 files. The files were then imported into both MMHS servers and clients. A single signature key pair was issued per user. No key archive was used.

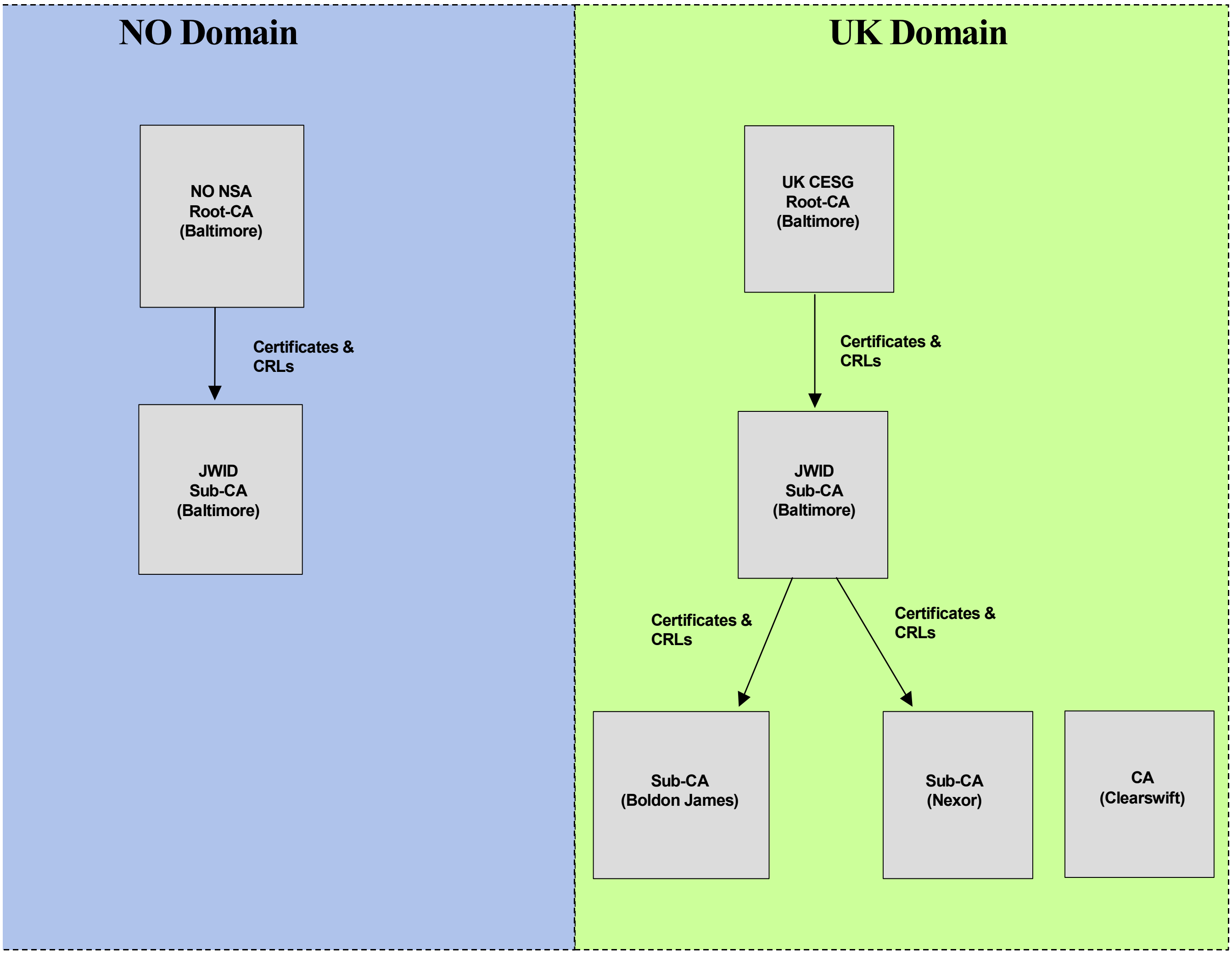

Figure 5.1 PKI CA-hierarchies

The APM was used for publishing both certificates and certificate revocation lists (CRL) into the directory system.The ARM was configured to publish CRLs into the directory container defined by the distinguished name of the sub CA, while the end user certificates were published as an attribute within each user object.

The certificate profile for JWID 2002 was based on the MSDP certificate profile with only minor changes that did not affect the testing.

The PKI system was designed specifically for demonstration purposes only, and the system does not meet all requirements for a production system, especially regarding private key management. In a live operational system, importing the same private signing keys into multiple systems (both server and client) is discouraged as this undermines the security of the system. Self generation of signature keys to increase security should also be considered.

5.4 UK Systems

The UK PKI system for JWID 2002 consisted of a 3 level CA hierarchy. The root CA was the test version of the CESG HSM root. A special sub CA for JWID was set up below the root. This CA then issued certificates to 2 of the participating UK MMHS systems (Protek and Nexor). In addition a third MMHS system was set up as its own self signed root CA (Clearswift). Further details on the UK PKI systems are not known.

5.5 Interoperability

The interoperability model between the PKI systems used multiple trust points. The UK root CA certificate was imported into the trusted certificate store in the Norwegian MMHS systems. This model allows the Norwegian MMHS system to process the certificate chain from a UK user certificate back to the trusted UK root certificate. The Norwegian root CA certificate was similarly installed in trusted certificate stores in the UK MMHS systems. Non-technical issues regarding the interoperability model were not considered (e.g. policy mapping).

The MMHS systems were configured to include the user certificate with the signed messages to ease the certificate path building at the recipient.
CRL information published into directory systems by the various PKI systems on both the Norwegian and UK side was replicated between the systems to allow revocation control of certificates on both sides. The Norwegian MMHS servers were able to locate and read the CRL's based on the naming of the issuing CA.

Messages signed in the UK system were successfully verified in the Norwegian system. Message signed in the UK system using a private key corresponding to a revoked certificate were successfully detected in the Norwegian system as an invalid signature due to certificate revocation. See the test result section for further details.

6 DIRECTORY SYSTEMS AND STANDARDS

6.1 Introduction

A Directory (DSA – Directory Service Agent) is often called a "Write-Once, Read-Many" database. It typically contains information that is static or at least not changed frequently, such as names, telephone-numbers, email-addresses, certificates, etc.

Directory systems are generally based on the ITU X.500 recommendations which stadarize protocols for client access to the directory (DAP), inter-directory communication (DISP/DSP) and directory content formats. In addition to the ITU/X.500 definitions, IETF has defined the LDAP-protocol (rfc 2251) that defines directory access over internet-protocols. While X.500 DAP/DISP is used to maintain the directory content, most clients use LDAP as access protocol to retrieve and modify information in the DSA. LDAP is implemented in many COTS products, including Microsoft Exchange and Netscape mail servers.

A directory schema, ACP 133, is also defined to support generally all attributes required to perform all kinds of military messaging. It is based on the standard X.500 schema, with addition of all directory-related definitions in X.400, + a number of classes and attributes defined in ACP 133 itself to support ACP127, etc., and to better fit into a military organizational structure with roles, more than individuals.

DISP is the X.500 protocol for directory replication. It defines setting up a Master- and a Target DSA and a starting-point in the Master from where all subordinate entries will be shadowed to the Target. Replication me be carried out "On Change" or time scheduled, initiated by the Source or the Target. DISP require both systems to have exactly the same Directory schema, as there is no transformation or filtering of the data being replicated.

The ACP133 directory schema, also recommend a directory-communication network based on X.500/DISP. It suggests each nation sets up a National Border-DSA (BDSA) through which all directory replication takes place to and from other nations and NATO. On the National side – behind the nation's BDSA – it is a National matter how replication is carried out and how information is being used nationally or what information to expose to the other nations.

In addition to DISP, the Norwegian Defence use the Meta-Directory product "Data Synchronization Engine" (DSE) from MaXware International AS to maintain the DSA(s) with updated information from databases, and other data-sources. In addition to performing the basic directory-replication, this product also is able to modify data on the fly to make sure the data is directly useable on the target side and also filter on which entries to be exported/imported to/from the Norwegian BDSA.

For JWID '02, directory replication was a critical functionality to be able to test the client products. It was important that email-addresses (smtp and X.400), certificates, and general contact information defined in one national end-systems, was available at the other side to use or just verify PKI-related attributes (Certificates, Revocation-lists), but also to gain access to more general directory-information.

6.2 Norwegian systems

For technical reasons, the Norwegian BDSA during JWID '02 was not a Directory, but actually a Microsoft Access database. This of cause made DISP impossible as replication protocol against other nations BDSAs, but as we used MaXware DSE, it did not cause any problems. The communication picture look exactly the same as it would even if a DSA had been used as BDSA.

Test objectives:

- synchronize contact information from the Norwegian NORCCIS II system (Exchange 5.5) into the NATO HUB (DCL)
- receive contact information from all the other countries via the NATO HUB and create usable email-addresses in the local Exchange GAL
- cross-synchronize MMHS attributes incl. UserCertificates, CA-Certificates and CRLs from a local InJoin DSA maintained by Baltimore PKI with the CJTF HUB (DCL)
- maintain a page on the Norwegian WEB-server with all contact information

The following picture show the configuration seen from the Norwegian side during JWID '02:

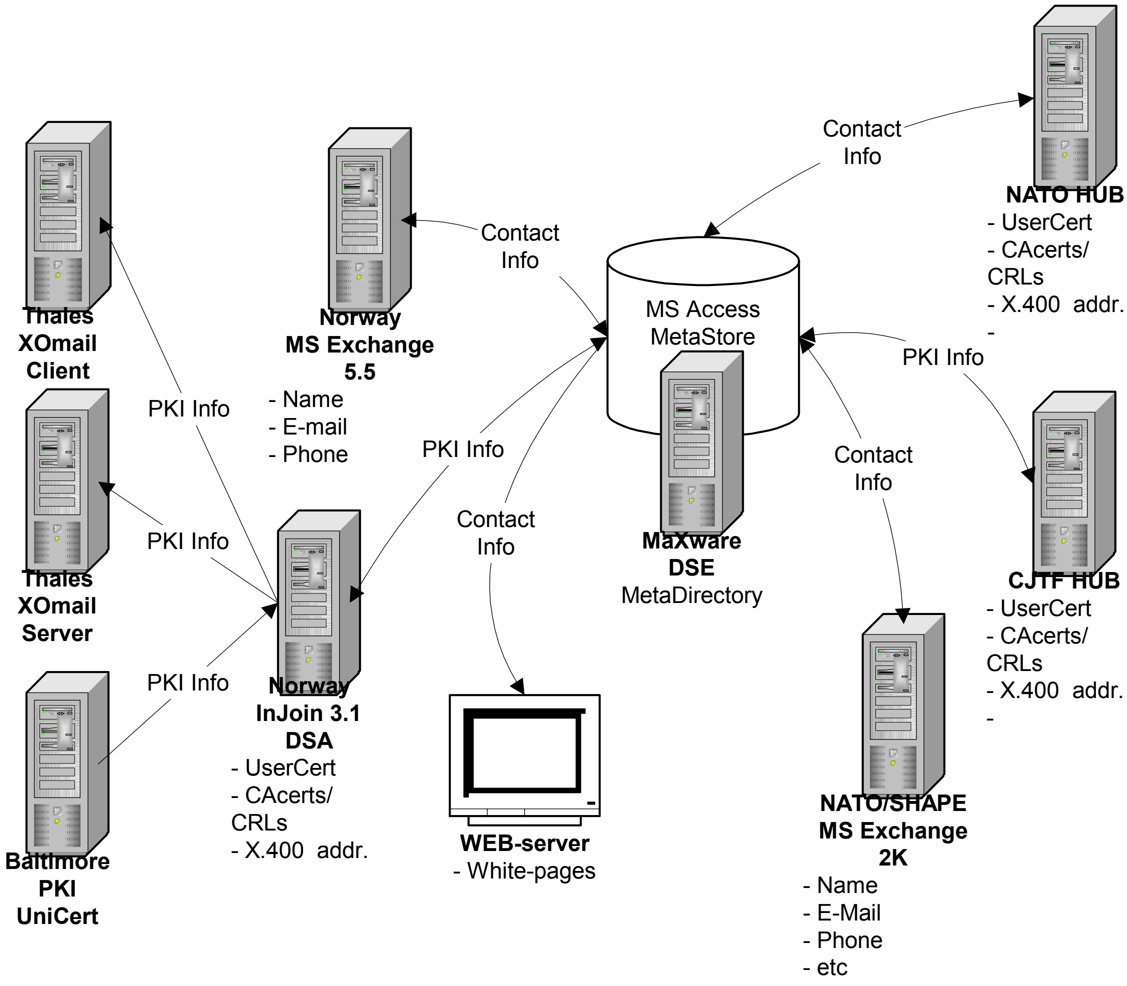

Figure 6.1 Directory connection overview

The following picture shows the attribute flow between the systems:

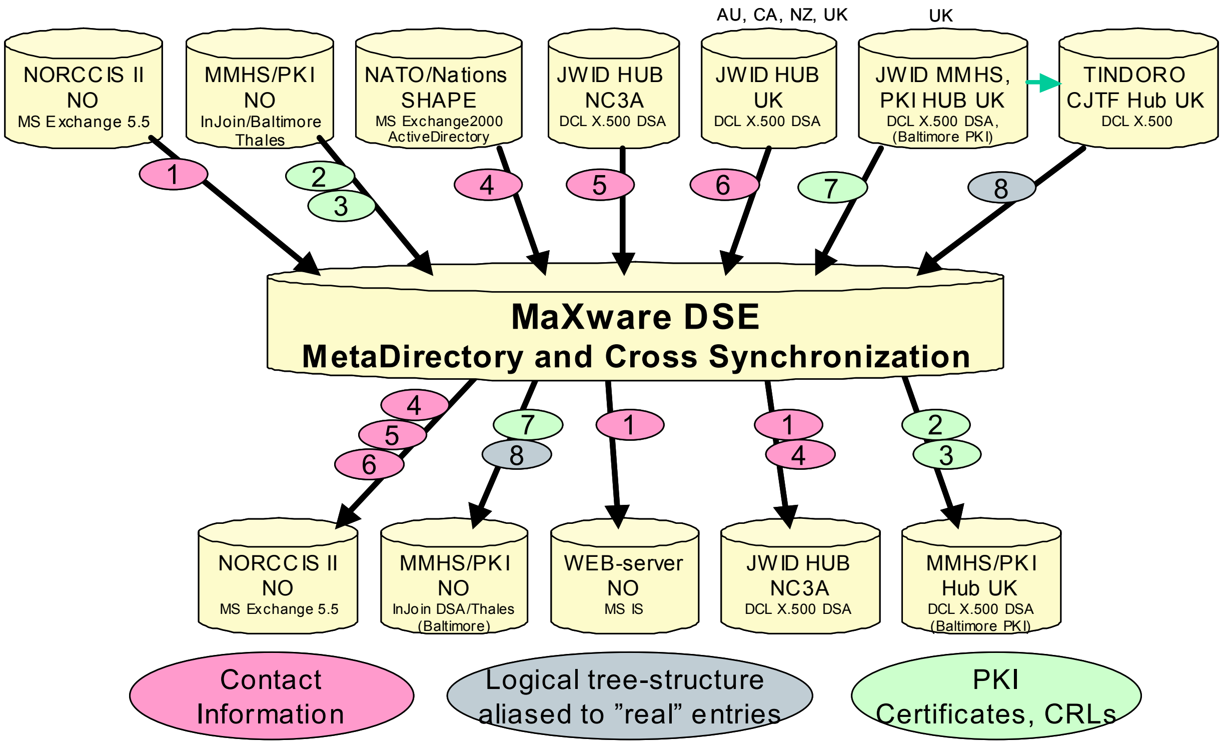
AU, CA, NZ, UK
UK
NORCCIS II NO MS Exchange 5.5
MMHS/PKI NO InJoin/Baltimore Thales
NATO/Nations SHAPE MS Exchange2000 ActiveDirectory
JWID HUB NC3A DCL X.500 DSA
JWID HUB UK DCL X.500 DSA
JWID MMHS, PKI HUB UK DCL X.500 DSA, (Baltimore PKI)
TINDORO CJTF Hub UK DCL X.500
1
2
3
4
5
6
7
8
MaXware DSE
MetaDirectory and Cross Synchronization
4
5
6
7
8
1
1
4
2
3
NORCCIS II NO MS Exchange 5.5
MMHS/PKI NO InJoin DSA/Thales (Baltimore)
WEB-server NO MS IS
JWID HUB NC3A DCL X.500 DSA
MMHS/PKI Hub UK DCL X.500 DSA (Baltimore PKI)
Contact Information
Logical tree-structure aliased to "real" entries
PKI Certificates, CRLs

Figure 6.2 Dataflow overview

7 TEST SCENARIOS

7.1 Preparations and pretesting

Prior to JWID, the XOmail client was extended to support import of private signature keys and user certificates, created by UniCERT. (Exported using the PKCS#12 standard) In addition, the Norwegian PKI hierarchy for JWID 2002 was defined. It included a root CA, a sub CA and users. All certificates issued during JWID 2002 were signed by the sub CA.

A few weeks before JWID, we performed a few pretests with the three messaging systems set up in the UK:

- Protek
- Clearswift
- Nexor

The pretests were run over the Internet and included informal exchange of basic STANAG messages. The configuration of the UK systems was not completed at this stage, so we did not exchange PCT messages. However, we did complete most of the essential connection configuration and exchanged the certificates to be used later.

7.2 JWID tests

In addition to those systems mentioned above, a few messages were exchanged with a DMS and MUSE messaging systems. The table below summaries the protocol test results.

MMHS (Sender and receiver)	P772 (STANAG)	PCT	Certificate validation	Certificate revocation
XOmail -> Protek (UK)	OK	OK	OK	OK [1)]
XOmail <- Protek (UK)	OK	OK	OK	OK
XOmail -> Nexor (UK)	OK	OK	OK	
XOmail <- Nexor (UK)	Failed [2)]	OK	OK	
XOmail -> Clearswift (UK)	OK	OK	OK	
XOmail <- Clearswift (UK)	OK	OK	Failed [3)]	
XOmail -> DMS (US)	OK [4)]			
XOmail <- DMS (US)	OK [4)]			
XOmail -> MUSE (Fr)	OK [4)]			
XOmail <- MUSE (Fr)	OK [4)]			

NOTES

1. The Protek certificates used were suspended and not revoked by the Protek CA. This was done because a revocation would have affected the UK test scenario.
2. XOmail successfully decoded and verified PCT messages received from Nexor, However, the STANAG message encapsulated in the PCT protocol included some message extensions not supported by XOmail. Consequently, these messages were not delivered to the intended recipient.
3. XOmail does only allow self-signed CA certificates signed with at least a 1024bit DSA key to be imported as trusted. The Clearswift CA certificate used during JWID 2002 was signed with a 512 DSA key. Consequently, XOmail was not able to establish a valid certificate path to a trusted CA, for messages received from the Clearswift messaging system. No other issues were detected.
4. Test messages transmitted via a Nexor message server.

A set of basic STANAG and PCT tests were defined and distributed by UK prior to JWID 2002. The results described in the table above are based on a subset of these test and some additional informal tests. Consequently, an “OK” comment does not imply that there are no issues, only that none were discovered during JWID 2002. Since each of these messaging systems has been tested extensively earlier, during the MMHS Security Demonstrator Program (MSDP), we did not expect to encounter any major issues during JWID. The JWID tests confirmed this and demonstrated that these operational messaging systems are able to successfully exchange signed STANAG messages, using the PCT protocol. The XOmail –

Protek tests did also demonstrate that online certificate revocation using CRL's and directory services is supported.

8 SUMMARY

The JWID 2002 integrated MMHS, Directory and PKI testing between NO and UK was very successful and showed that it is possible to integrate systems on short notice and achieve interoperability across borders.

To summarise, we achieved:

- to integrate the MMHS, Directory and PKI systems on both sides
- to exchange signed PCT/P772/P1 messages and verify the signatures on both sides
- to revoke certificates with the consequence that the systems on both sides failed to verify the signatures
- to distribute certificate and certificate revocation lists automatically between the nations using the Directory replication HUB
- to exchange PKI certificates and establish trust anchors

With this exercise we demonstrated that by relative limited resources and on short notice it was possible for NO and UK to get an integrated MMHS, Directory and PKI system up and running. This shows that most of the technical solutions are available even though the procedural aspects may be a challenge in a real operational integrated system.

References

(1) NATO STANAG 4406 Ed.1 – Military Message Handling System (MMHS)
(2) NATO STANAG 4406 Annex E – Tactical MMHS Protocol and Profile Solution
(3) IETF S/MIME – Cryptographic Message Syntax (CMS), IETF RFC 3369
(4) ACP 133 - Common Directory Services and Procedures

DISTRIBUTION LIST

FFIE **Dato:** 13. desember 2002

RAPPORTTYPE (KRYSS AV) ☒ RAPP ☐ NOTAT ☐ RR	RAPPORT NR. 2002/04655	REFERANSE FFIE/840/110	RAPPORTENS DATO 13. desember 2002
RAPPORTENS BESKYTTELSESGRAD Unclassified		ANTALL TRYKTE UTSTEDT 41	ANTALL SIDER 26
RAPPORTENS TITTEL THE JOINT NO AND UK DEMONSTRATION OF INTEGRATED MMHS, PKI AND DIRECTORY SYSTEMS AT JWID 2003		FORFATTER(E) EGGEN Anders, ANDREASSEN Morten, HVINDEN Øyvind, LÆGREID Helge	
FORDELING GODKJENT AV FORSKNINGSSJEF Torleiv Maseng		FORDELING GODKJENT AV AVDELINGSSJEF: Johnny Bardal	

EKSTERN FORDELING

ANTALL	EKS NR	TIL
2		FLO/IKT
1		v/Øyvind Hvinden
1		v/Pål Granlund
1		v/Oddmund Korsveien
1		v/Per Anders Jørgensen
2		FO/I
1		v/Tor Einar Wivelstad
1		v/Per Trygve Gundersen
2		FO/S
1		v/Helge Lægreid
		Thales Communication
		Strindveien 1, 7030 Trondheim
1		v/Arve Olaussen
1		v/Bengt Kristiansen
1		v/Morten Andreassen
1		CESG
1		Attn: Chris Ensor
		P O Box 144
		Cheltenham, Gloucestershire
		GL52 5UE
		ENGLAND
1		QuinetQ Malvern
		Attn: William Ottaway
		St Andres Rd, Malvern
		Worcestershire WR14 3PS
		ENGLAND
1		UK MoD
		Attn: Toby Clark
		EC-CCII-FII2d
		Room 742
		Northumberland House
		Northumberland Avenue
		London WC2N 5BP
		ENGLAND

INTERN FORDELING

ANTALL	EKS NR	TIL
9		FFI-Bibl
1		FFI-ledelse
1		FFIE
1		FFISYS
1		FFIBM
1		FFIN
1		Anders Eggen
5		Restopplag til Biblioteket
		Elektronisk fordeling:
		Torleiv Maseng (TMa)
		Tor Gjertsen (TGj)
		Anton B Leere (ABL)
		Ole-Erik Hedenstad (OEH)
		Karsten Bråthen (KaB)
		FFI-veven

Benytt ny side om nødvendig.

EKSTERN FORDELING			INTERN FORDELING		
ANTALL	EKS NR	TIL	ANTALL	EKS NR	TIL
1		Defence Informations Systems Agency (DISA/API) (Attn: Principal Director Ronald J Dorman) 5275 Leesburg Pike Falls Church, VA 22041 USA			